SCIENCE & MILITARY

No 1 | Volume 9 | 2014

Dear readers,

You are just looking at the first issue of the journal Science & Military of this year. It has been published for nine years already. We are pleased to see that this scientific journal focused on military science has been successful for such a long time and is increasingly attracting more and more authors and readers.

We would like to continue in this way and offer our readers high-quality scientific articles that reflect current issues in the field of "Defense and Security". Conducting research, drawing scientific conclusions and writing specialized texts serve as presentation of authors as well as evaluation of institutions where the authors are employed. After all, scientific research results can be subject to discussion and validity assessment only if they are published and presented to a large number of experts and professionals.

The editorial board's long-term objective is still to include the journal Science & Military into the Scopus and Thomson Reuters databases. We realize the fact that we can reach this goal only by joint effort because international recognition of the journal does not depend only on work done by the editorial board and the chief editor. An internationally recognized journal means high-quality scientific articles that will appeal to specialists and spark discussions.

Dear readers, the current issue of the journal contains twelve new and undoubtedly interesting articles. Let me briefly introduce some of them:

The article written by Petr Františ titled „Experimental user interfaces to 3D visualization of C2 system" describes development of 3D visualization system that works with a Czech C2 system. The main focus of the article is on using motion tracking and augmented reality approaches to simplify the user interface of this visualization system.

The author Kazimierz Kowalski presents an article titled "Chosen issue of weapon systems exploitation research" in which he presents the complex technical weapon systems with standard natural ageing processes, degradation and random failures caused by human faults, overloading or destructive acting of surroundings.

The article written by Mykhailo H. Hrubel, Mariya B. Sokil, Roman A. Nanivskyi titled "Influence of characteristics of wheeled vehicle suspension on its road-holding along curved stretches of track" deals with a difficult issue of vehicle movement dynamics and specification of stabilization moments during its vertical and swiveling movement.

The article written by Martin Javurek, Michal Turčaník a Marcel Harakaľ titled "Artificial neural networks in cryptography" shows an overview of topologies of neural networks for use in cryptography. From the most known as is a Tree Parity Machine, through a Permutation Parity Machine to the use one of the most used ANN with Backpropagation algorithm as a Chaotic random numbers generator.

In article written by David Kusmič, Zbyněk Studený, Vojtěch Hrubý, Emil Svoboda titled "Material analysis of demaged 125 mm tank main gun type TK 2A46" are described procedures and methods used for material evaluation of materials applied for new damaged or wrecked tank main gun.

The authors Vlastimil Malý, Petr Hruza present the article titled "Modelling of task force structures", which describes a new approach to the planning process and a new possible way of selection of forces for international operations based on modular structures and units' capabilities required for particular operation. The article describes the options of original software application developed during the "STRUCTURE" project solution aiming as a support for staff officers in the preparatory phase of operational planning.

The article written by Radoslav Masnica, Jozef Štulrajter, Ivan Plichta titled "Common operational picture and a probabilistic model for recognition identification friendly or Foe – IFF" describes a probabilistic model of knowledge on the battlefield and Identification Friendly or Foe – IFF and current overview of the situation for the commander and offers an introduction to the understanding of the relationship between information and their impact on the results of the fight.

The authors Sergiy Orel, Oleksiy Ivaschenko in article titled "Through ecological risk assessment" addressed the question of management by ecological safety of troops through assessment of ecological risk is considered in the article. As the model of risk assessment was used scheme, proposed by the United States Agency of Environmental Protection (USEPA).

The article titled "Quality value analysis from customers' point of view" written by Iveta Kmecová, Robert Zeman, Daniel Kučerka, Monika Kučerková deals with the importance of marketing and its great influence on running a business successfully. The article presents some results of the research focused on judging the process of providing quality value in business field.

The author Josef Požár wrote the article titled "Modelling of the investigation of cybercrime". The article deals with selected aspects of computer crime with stress on some ways of forensic investigation of this phenomenon. Some typical ways of committing computer crime with regard to investigative situations are described here. In conclusion, the author refers to possible education of the police officers about computer crime.

Dear readers, I do believe that you will continue reading our journal Science & Military and that in this year you will also have a chance to go through a lot of inspiring articles that will spark discussions with other universities, scientific and research institutions and specialists.

Assoc. Prof. Eng. Marcel HARAKAĽ, PhD.
Chairman of the editorial board

Reviewers:

Lt. Col. Eng. Vladimír **ANDRASSY**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Eng. Július **BARÁTH**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Assoc. Prof. RNDr. Vanda **BOŠTÍKOVÁ**, Ph.D.	University of Defence Brno (CZ)
Assoc. Prof. RNDr. Ľubomír **DEDERA**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Assoc. Prof. Eng. Jaroslav **DOČKAL**, CSc.	University of Defence Brno (CZ)
Lt. Col. Eng. Radek **DOSKOČIL**, Ph.D.	University of Defence Brno (CZ)
Assoc. Prof. Eng. Mária **DZÚROVÁ**, PhD.	University of Economics in Bratislava (SK)
Eng. Viera **FRIANOVÁ**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Eng. Jozef **GALANDA**, PhD.	Technical University of Košice (SK)
Assoc. Prof. Eng. Marcel **HARAKAĽ**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Assoc. Prof. Eng. Ondrej **HÍREŠ**, CSc.	Alexander Dubček University of Trenčín (SK)
Assoc. Prof. Eng. Ladislav **HOFREITER**, CSc.	University of Žilina (SK)
Assoc. Prof. Eng. Olena **KONOVALOVA**, PhD.	National Aviation University Kiev (UA)
Eng. Ivan **KOPECKÝ**, PhD.	Alexander Dubček University of Trenčín (SK)
Assoc. Prof. Eng. Mariana **KUFFOVÁ**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Eng. Milota **KUSTROVÁ**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Prof. Eng. Miroslav **LÍŠKA**, CSc.	Armed Forces Academy Liptovský Mikuláš (SK)
Assoc. Prof. Eng. Peter **LISÝ**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Prof. Eng. Stanislav **MARCHEVSKÝ**, CSc.	Technical University of Košice (SK)
Prof. Eng. Pavel **NEČAS**, PhD.	EDA Brussels POC (BE)
Assoc. Prof. Eng. Miroslav **ŠKOLNÍK**, PhD.	Armed Forces Academy Liptovský Mikuláš (SK)
Assoc. Prof. Eng. Vladimír **VRÁB**, CSc.	University of Defence Brno (CZ)

EXPERIMENTAL USER INTERFACES TO 3D VISUALIZATION OF C2 SYSTEM

Petr FRANTIŠ

Abstract: The article describes development of 3D visualization system that works with a Czech C2 system. It briefly describes the history of the Czech C2 system development and the current state in this area in the world. Various projects that contributed on development of the tactical data 3D visualization from the C2 systems are mentioned as the main contributors to development of the new visualization system. The main focus of the article is on using motion tracking and augmented reality approaches to simplify the user interface of this visualization system. The experimental application of motion tracked command post is described in detail and the results of this experiment are concluded, also the results of testing the augmented reality devices in two test scenarios are concluded as well.

Keywords: Command and Control. C2. Visualization. Augmented reality. Motion tracking.

1 INTRODUCTION

One of the generally accepted definition of Command and Control (C2) system dates back to 1986. C2 is a system of systems that can be characterized by high degree of complexity, distributed environment focused on distribution of decision making process over the agents, high demand on reliability and inevitable human machine interface implemented to support communication between operator and system [1] C2 system can be seen in many domains such as traffic control, manufacturing system, nuclear system, military system, etc. Military C2 (MC2) system is C2 system that operates in the real time battlefield domain with the main goal to achieve operational and information superiority. [2]

MC2 system research activities began in 1970 and from that moment battlefield information was strictly connected to geographical position information. Thus the main MC2 interface was born as a battlefield real time picture with related geo information. Interface was called common operational picture (COP) and its name is still in use. COP is usually composed of visualized military information (SW solution) and physical interface to control this environment (both HW and SW solution).

Visualized military information is divided into:

- Friendly position information (blue forces);
- Enemy position information (red forces);
- Unit tactical data information;
- Geo data (raster, vector and satellite imagery).

From the visualization point of view the military information is visualized on the map resources. Physical interface is composed of:

- Visualization system (LCD, projector);
- Input devices (keyboard, mouse, trackball).

The most important demands on COP are:

- Credibility of visualized information;
- Accuracy of visualized information;
- Natural and understandable visualization;
- Easy and user-friendly interface;
- Ability to work in field conditions.

1.1 Current state of MC2 system

First MC2 system has been implemented in 1995 in the US Army. This system was capable to gather all battlefield data from sensors and to visualize it in 2D map resources. The progress of technology and mainly the growth of computer power enabled to develop application that was capable visualize friendly units in 3D terrain in 2008. [3] That was the first attempt to visualize COP in 3D (Figure 1). The system was implemented in the US Forces under the code name Force XXI Battle Command Brigade and Below (FBCB2).

FBCB2 3D solution has these shortcomings:

- Friendly and enemy units are visualized as a symbol (not 3D objects);
- Not exactly expresses the area covered by unit (only connected to a point, not to the area of operation);
- Unit tactical data is not visualized (combat efficiency, movement velocity, fuel capacity, ammunition capacity, etc.);
- Human machine interface is slow and old fashioned (keyboards, LCDs).

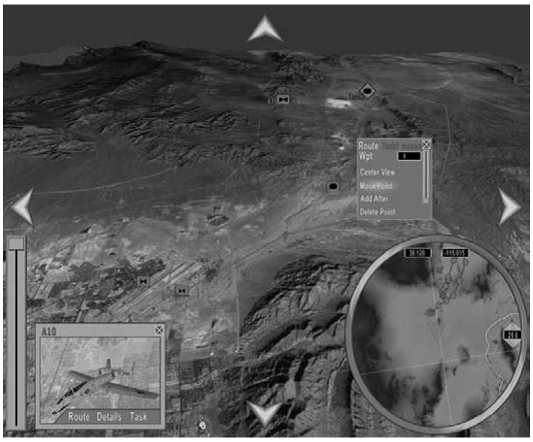


Fig. 1 Blue and red forces mapped on the 3D terrain - COP

In 2007, The Defense department of the Czech Republic accepted a new research project called:

”Virtual reality devices in ground forces tactical command and control system (GFTCCS)”. The project concentrates on increasing commander situational awareness at a tactical and operational level in three dimensional (3D) terrain visualization.

This project is based on integration of virtual reality devices into command and control process.

The main project goal was a demonstration of a new presentation layer of GFTCCS with virtual reality devices. A global architecture of GFTCCS was designed in 1999 and its presentation abilities were obsolete. The commander could get information about battlefield in 2 dimensions (2D) only. The terrain spatial data were available but they were not used to visualize the battlefield in 3D. Communication between the commander and GFTCCS was supported only by a mouse or keyboard. A resolution of visualized battlefield was given by output devices abilities - CRT or LCD monitors. The old presentation layer offers common features of Geographic Information Systems (GIS) such as zoom in, zoom out or movement of actual position over a map.

The main ability of GFTCCS is to show a position of friendly forces as it can be seen on the picture bellow.

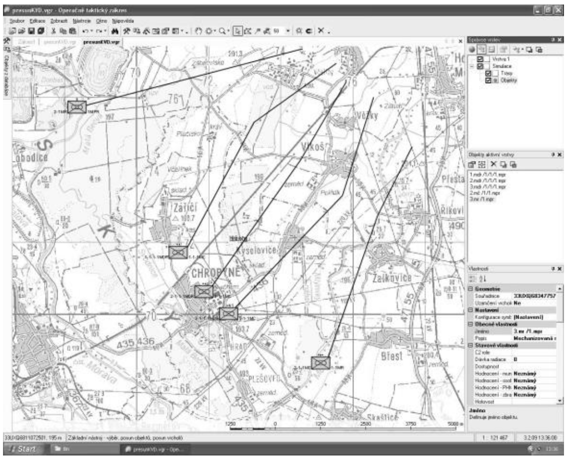


Fig. 2 Old presentation layer of GFTCCS

The new presentation layer comes out from experience with virtual reality devices in the modeling and simulation world. It was based on project with code name “Virtual” (2008-2009) that implemented a new presentation layer for Czech GFTCCS system that is capable to visualize friendly units as a 3D object in virtual terrain. The virtual terrain is fully automatically generated from geo data resources without any operator involvement and visualized unit covers by its volume the unit controlled area.

This new presentation layer was tested by commanders and the visualization part was positively accepted.

The new 3D visualization system could display 3D terrain based on digital geographic data and 3D units in forms of tactical symbols in App6a format but it was not able to display any other tactical graphic – the tactical overlays from GFTCCS system.

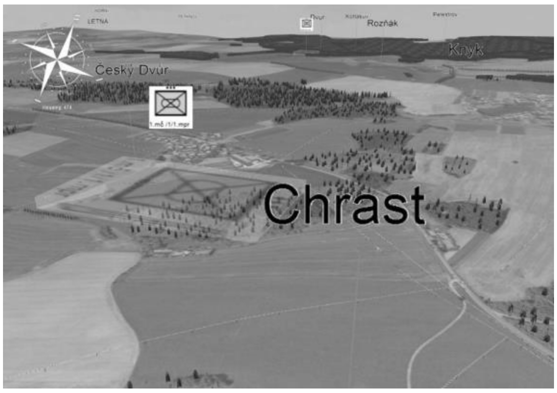


Fig. 3 GFTCCS 3D Visualization system

Project with code name “Visual”, started in 2010 and ending in 2012, enhances the 3D visualization capability mainly in the field of tactical data visualization in 3D. The 3D visualization methodology of tactical overlays (tactical lines, areas, directions and points) has been designed and implemented. It uses a non-official standard for tactical overlays exchange in C2 system – the NVG (NATO Vector Graphics). The NVG standard is composed from two parts:

- NVG data format;
- NVG service.

The NVG service is based on web-service standard and is implemented in the GFTCCS system and provides tactical overlays graphical data in NVG data format. The overlay in NVG format is converted using a special service on the side of 3D visualization system into 3D representation.

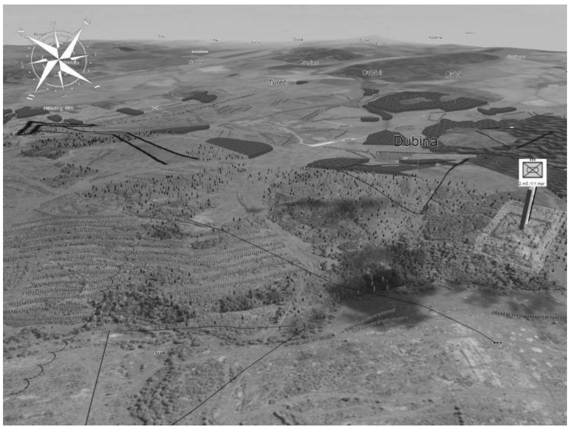


Fig. 4 Shows the tactical overlays visualized in 3D

2 EXPERIMENTAL USER INTERFACE

The traditional user interface consists of computer mouse and keyboard. This type of user interface is satisfactory in the desktop configuration – monitor or multi-monitor systems, but for the projection systems it does not give the commander a freedom of move. The commander must voicecommand the operator of the system to move the view in the 3D environment. So an idea of using the body movement and hand gestures was introduced. As a body motion sensor was tested the Microsoft Kinect sensor.

2.1 Using the Kinect sensor

Microsoft Kinect sensor was chosen to control COP as a low cost device. Originally it was developed only for Xbox game console, but currently Kinect can be used on the PC platform. This devices is composed of two infra cameras and one standard camera that enables the drivers to measure distance between important points in the tracked area. The exact position of appropriate joints of user (or two users) standing in front of it can be solved by Kinect API and customized SW application.

The Kinect device was implemented into GFTCCS solution. The commander can stand in front of sensor and his movements are tracked by the Kinect device. The tracked body movements and gestures are used to control the COP visualization veral. The Kinect is a wireless device so the commander does not need any other attached motion tracking sensors.

Not only was the Kinect device employed into veral architecture. The Figure 5 shows the complete COP visualization architecture solution. Commander and his staff (usually 5 persons) wear glasses that are synchronized with 3D stereoscopic projector projecting the visualized imagine on a standard projection screen (active stereoscopic projection is used). The Kinect device is placed under the projection screen. The projector can placed either on the floor or mounted on the ceiling. The ceiling projection mounting allows more room for the commander but floor projector placement is easier for fast deployment. This configuration was designed and tested for easy deployment in standard military field tents. The active stereoscopic projection enables better depth sensing of the visualized terrain and is very appreciated by the commanders and staff.

2.2 Utilization of augmented reality

The visualization using stereoscopic projection allows better depth sensing for the user that controls the camera position in the virtual environment. But works in the way that user controls the virtual camera in the virtual environment and “fly with it”. On the contrary a lot of commanders is used to work with the traditional sand tables and want to walk around this virtual terrain as they can around the sand table. This experience is able to give them the augmented reality solution only.

The augmented reality solution can work in two ways:

- Using the motion tracker;
- Using the pattern recognition.

Both solutions require wearing see-through glasses that are connected with a personal visualization computer. As a personal visualization computer can be used any tablet or embedded computer such as Fit-PC2 or similar.

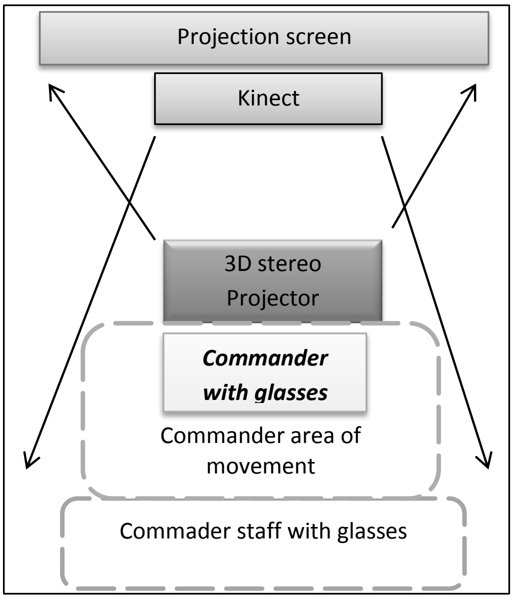


Fig. 5 Basic scheme of Commander post equipped with the Kinect sensor

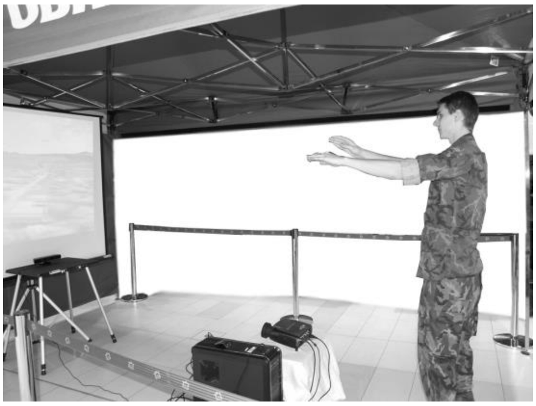


Fig. 5 Motion tracked commander post demonstration

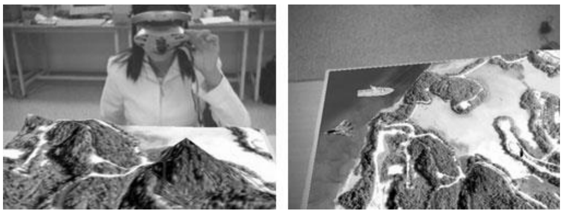


Fig. 6 Virtual sand table example

2.2.1 Augmented reality with motion tracking

The most important thing in the virtual sand table solution is the tracking of user's head. The head position and orientation information determines position and orientation of virtual camera in the virtual environment. To obtain such data a motion tracking platforms should be used. The motion tracking can be either optical – using several calibrated cameras and reflexive points on the user's glasses or hybrid using optical and inertial sensors. These motion tracking platforms guarantee precision values and stability of position and information data but as a drawback they are expensive and require precise installation and calibration so they are not designed for the field conditions.

2.2.2 Augmented reality using pattern recognition

The position and orientation information about the user's head can be also obtained by using pattern recognition algorithms. The augmented reality glasses must be equipped with a camera that records user's point of view. A special library for pattern recognition analyses frames capture from the camera and looks for the defined pattern. From the recognized pattern the parameters such as user's relative position and orientation can be obtained and these data are used to render the virtual sand map accordingly. Unlike the solution with motion tracking platform in pattern recognition the camera must see the whole pattern so the freedom of movement is limited and it is not possible for example to come closer to the part of virtual sand table that is too distant from the pattern position because the pattern recognition library would lost the position and orientation information. The advantage is that this solution does not require any complicated hardware just the piece of paper with printed pattern that is placed on the virtual sand table place.

3 CONCLUSION

We have already done couple of experiments with low cost visualization solutions. We have tested the Kinect sensor and its usability to control the visualization system of MC2 in simulated field condition. We revealed that:

- Kinect solution works perfectly in dark environment (battlefield tents);
- Commander staff must be located in the specified areas (usually on the sides) to not cross the line of sight from the Kinect device to the tracked commander;
- Commanders were able to better understand the vital information from the battlefield;
- Control of visualization was more intuitive and thus faster;
- The overall solution was easy to deploy and ready to use in very short interval – less than 10 minutes.

The augmented reality based virtual sand table was tested in the laboratory conditions only. The tests revealed that the idea is correct but there are many technical difficulties that degrade the quality of the solution. As the crucial factor based on our tests is the precision of position and orientation sensing during fast movements of the user.

References

[1] BUILDER, C. H., BANKES, S. C., NORDIN, R.: *Command Concepts: A theory derived from the practice of command and control.* Santa Monica : RAND, 1999. ISBN 0-8330-2450-7.

[2] TOLK, A., KUNDE, D.: Decision Support System – Technical Prerequisites and Military Requirements. In *C2 Research and Technology Symposium.* Monterey, 2000.

[3] FBCB2. CG2 C3D Demonstration Application Employed in U.S. Army AAEF Exercise Tests Real-Time 3D Visualization of on - the - Move C4ISR Data from FBCB2 VMF Messages. Retrieved June 10, 2008. Available at: http://www.cg2.com/Press.html.

Maj. Eng. Petr FRANTIŠ, Ph.D.
University of Defence
Kounicova 65
612 00 Brno
Czech Republic
E-mail: petr.frantis@unob.cz

CHOSEN ISSUE OF WEAPON SYSTEMS EXPLOITATION RESEARCH

Kazimierz KOWALSKI

Abstract: Complex technical weapon systems meet with standard natural ageing processes, degradation and random failures caused by human faults, overloading or destructive acting of surroundings. Knowledge of a first period of utilization phase of technical objects, called infant mortality or “burn-in”, is significant from point of view of confidence in performing an intended function of these objects. Models of infant mortality of crucial functional systems of main battlefield tanks were presented.

Keywords: Weapon system. Maintenance. Operational availability.

1 INTRODUCTION

Availability of complex technical objects is a fundamental feature of their operational quality. Availability is typically measured by function or availability index which variability are observed in the usage time or mileage of these objects. Particular importance of the availability is observed for objects which are used continuously and objects which perform significant role in national defence. Weapon systems are such special objects which are usually used in two different operating environments (times): a peace time or a war time. Weapon systems, in a peace time, usually operate in the “garrison” environment in which there are stored or operated and supported (O&S) for training. During the period of armed conflicts (a war) weapon systems should be characterized by high operational availability and low damageability. Due to the rapidly changing requirements, set by today's armed conflicts, quite often, new weapon systems are placed directly after the production phase to operational theatre. Therefore, it is important that new objects should achieve a low damageability, caused by infant mortality, in the shortest time after entering into service. These requires the elimination of errors and defects already in the production phase. That is way knowledge of the so-called manufacturing errors is a key issue for the operational availability of newly introduced weapon systems into service.

2 OPERATIONAL FAILURES OF TECHNICAL OBJECTS

Failures of technical objects are defined as events resulting in the loss of ability to perform the intended functions. The appearance of a failure dependents on inside factors of the objects, O&S environment, O&S staff as well as the pre O&S and O&S periods. The literature bath-tube curve [1, 2, 3] illustrates the course of the hazard rate function during the infant mortality "running-in", useful life and were-out periods.

In the case of modern, technologically advanced technical objects, a hazard rate function is often limited to two specific intervals (Fig. 1 b, d, f [3]). Most typical are cases where there are no an infant mortality period (2b) or an were-out failure period (2f). Low, initial level of the intensity of failures may be the result of diligence in the design and high-quality of manufacture.

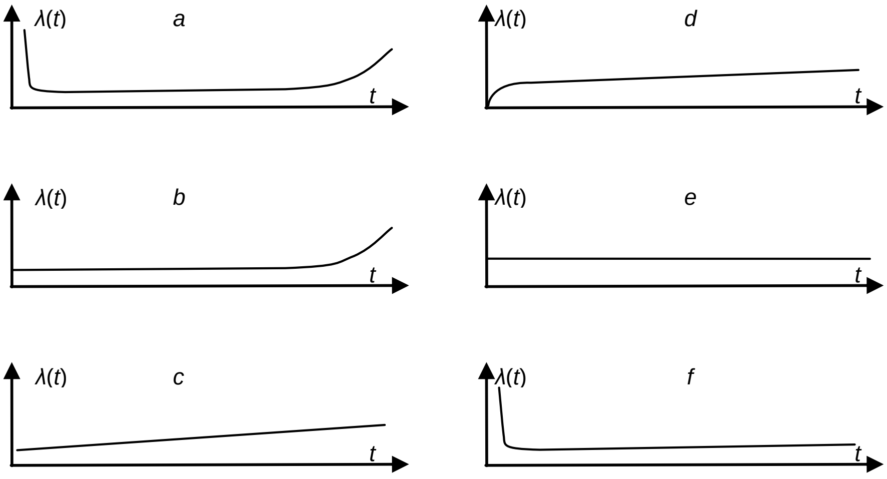


Fig. 1 Failure patterns of technical objects

Analysis of weapon systems O&S phases indicates to two main phases when the elements of these systems operate in peace and war time. Requirements for weapon systems in these periods of times are subjected into different criteria. Objects entered into O&S phases during the war are quickly sent to use positions and there are required to act safely and with high efficiency. Adjust the object to the O&S phases conditions is not advisable and achieving a long lifetime is limited in performing combat tasks (Fig. 1 b, c, e). Therefore, it is expected that these objects reach the lowest reliability state in a short time. On the other hand, in peacetime weapon systems are mainly used for training and provide a defensive reserve. Under these conditions the most important criteria should be the operating cost. This corresponds to the course of hazard rate function as shown in Figure 1f. The longer period of "entering" of the object into O&S phases is not profitable from a technical point of view, however it may refers to bit cheaper objects.

3 CHARACTERISTICS OF RESEARCH OBJECT AND ITS EXPLOITATION SYSTEM

The objects of the study were high-speed tracked vehicles, PT-91 tanks (Tab. 1), operated in a military armored unit with increased intensity of training. Exploitation of tanks proceeded according to the annual exploitation plan, which details their use and maintenance (including storage).

Tanks were used only for the training. The training included fire training (about 60 % of total time of training) and tactical training (about 40 % of total time of training). Access to a training range from a stopping place of tanks was carried out independently by the tanks that took part in the training.

Tab. 1 Core technical – maintenance data of PT-91 "Hard" tank

No.	Performance	Unit measure	Value
1	Weight of tank	kg	45300
2	Unit pressure	MPa	0.08
3	Maximum velocity	km/h	60
4	Maximum engine power with 2000 r.p.m.	kW	625
5	Maximum engine torque with 1300-1400 r.p.m	Nm	3100 ± 100
6	Gun calibre	mm	125
7	Fuel consumption	l/100km	420-450
8	Driving range (unsurfaced road)	km	460-600

Maintenance of tanks was performed as planned preventive maintenance in accordance with the following rules:

- Routine maintenance (in day of usage): an inspection before usage, an inspection during usage, an inspection after usage;
- Technical maintenance No 1, every 1600-1800 km mileage;
- Technical maintenance No 2, every 3300-3500 km mileage;
- Special maintenance for the tank preparation to water obstacles crossing, operation in summer or winter time, storage;
- Annual maintenance - once a year regardless of the mileage;
- Maintenance as a part of so-called "Technical days".

Routine maintenance was carried out by the direct users of tanks (the crew), but the rest type of maintenance were carried out by specialized technical structure (repair companies and repair platoons) in cooperation with the direct users (operators).The processes of tanks exploitation are illustrated graphically in Figure 2. The utilization (1) was carried out as a fire and tactical training. Preventive maintenance, according to the warranty, (2) was carried out as the mentioned above maintenance rules. Corrective maintenance (3) was carried out under warranty (after accepting the complaint by the manufacturer) or the own maintenance units (in the case of non-accepting of the complaint by the manufacturer). After performing corrective maintenance (replacement, adjustment, repair) tanks were directed to the diagnosis (4), and then to a stopping place (5) or directly to the utilization (1).

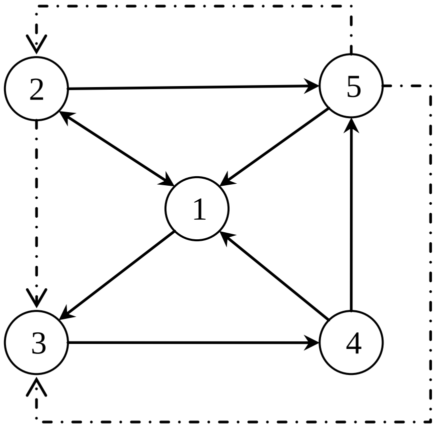


Fig. 2 Tanks exploitation processes
1 – utilization, 2 – preventive maintenance, 3 – corrective maintenance, 4 – diagnostics, 5 – awaiting for utilization (maintenance).

<table>
<tr><td colspan="4">TOTAL AMOUNT OF VEHICLES IN A MILITARY UNIT</td></tr>
<tr><td>RESERVE OF VEHICLE FOR WARTIME</td><td colspan="3">VEHICLES IN EXPLOITATION IN PEACE TIME</td></tr>
<tr><td colspan="3">VEHICLES IN STORAGE</td><td>VEHICLES IN USAGE</td></tr>
<tr><td colspan="2">LONG TERM STORAGE</td><td>SHORT TERM STORAGE</td><td>UTILIZATION</td></tr>
</table>

Fig. 3 The pattern of military vehicles' allocation into exploitation groups

The tanks exploitation system (and other military vehicles) is characterized by the allocation of a particular item of the vehicle to the one of the two exploitation groups: the group of vehicles in storage or the group of vehicles in usage (Fig. 3). Due to the fact that the tanks were operated under manufacturer's warranty, all of them were assigned to the group of vehicles in usage.

The total planed lifetime for the PT-91 tank amounts 38000 km or 30 years in service. However, the total lifetime for the power engine of the tank amounts 2400 mth.

4 RESEARCH OF WEAPON SYSTEMS INSTALATION

Analysis of the running-in stage of the weapon system into operation performed on the example of PT-91 tank. Operational information collected from the period of 3 years and 2 months in a garrison for the 144 tanks. For research purposes objects were decomposed to functional systems, subsystems and components. During the observation period (1174 days) tanks were failed by a total of 510 times with the mean time to repair (MTTR) of 27 days. Variability of failures ranged between 1 and 14 fails, with the mean number of failures more than 3 failures per one tank. Failures were reported as a warranty. About 364 complaints were recognized as a legitimate. That is, it can be concluded that approximately 71 % of the failures were derived from early production phase, and the others had different roots than the production errors [4].

The Table 2 depicts the main characteristics of failure: number of failures, Mean Mileage Between Failures (MMBF) and Mean Time To Repair (MTTR) of individual functional systems and subsystems. Data analysis was performed using the Weibull++ (ReliaSoft), adjusting to revised operational data from the Weibull shape parameters α and scale parameters β. The degree of matching of the distribution assess the correlation coefficient ρ with the lowest value of 0.93.

Tab. 2 Characteristics of tanks failure

Code of the system	The name of the system	The failure number	MMBF [km]	MTTR [day]	Distribution parameters W(α, β)		Correlation coefficient
					α	β	ρ
10	Chassis	25	84.4	24.0	0.82	151.76	0.98
11	Engine	97	48.9	25.1	0.87	103.43	0.99
12	Power transmission	27	25.0	29.7	1.06	60.45	0.97
13	Control system	21	113.5	20.9	1.20	232.11	0.99
14	Electrical system	69	151.6	28.4	0.92	140.56	0.93
20	Armament	69	161.1	26.9	0.63	117.21	0.98
21	Fire Control System (SKO)	59	91.4	29.5	0.58	119.52	0.97
23	DRAWA	42	74.7	28.7	0.93	102.73	0.98
24	Control system, electrical system	31	156.9	24.1	0.64	108.38	0.95
30	Communications	56	126.7	27.4	0.64	115.54	0.96
40	Special Systems	14	41.9	18.4	0.95	237.85	0.97

Analysis of the results of statistical data processing of field data (Tab. 2) shows that for 6 out of 11 functional subsystems a shape parameter α of the Weibull distribution has a value far less than 1 (α <0.92). This means decreasing failure intensity which is characteristic for the warranty period [1]. Failure of the origin of production are in the initial phase of operation gradually removed, hence the appearance of further operating life is becoming less likely. The decreasing failure rates of these six subsystems are corresponded with the Weibull shape parameter α within the range 0.58 - 0.87. In the case of five other subsystems: power transmission, control system, electrical system, DRAWA and special systems emerging failures are random (α = 0.92-1.20), resulting from human errors or unforeseen environment impacts. Their contribution in total number of failure (173 number of failures stand 34 % of total failures) is in line with the number of failures not recognized under warranty.

Figure 4 and 5 depict some examples of features characterizing the reliability of the extreme values of the shape parameter Weibull distribution. Figure 4 and 5 depict the failure intensity function curve and the reliability curve, respectively, for the subsystem 12-power transmission, with nearly constant failure intensity. Figure 6 and 7 depicts similar plots for the subsystem 21-Fire Control System (SKO) with decreasing failure intensity function. This indicates that the main factors causing the unusable state of objects are phenomena that occur during the production process.

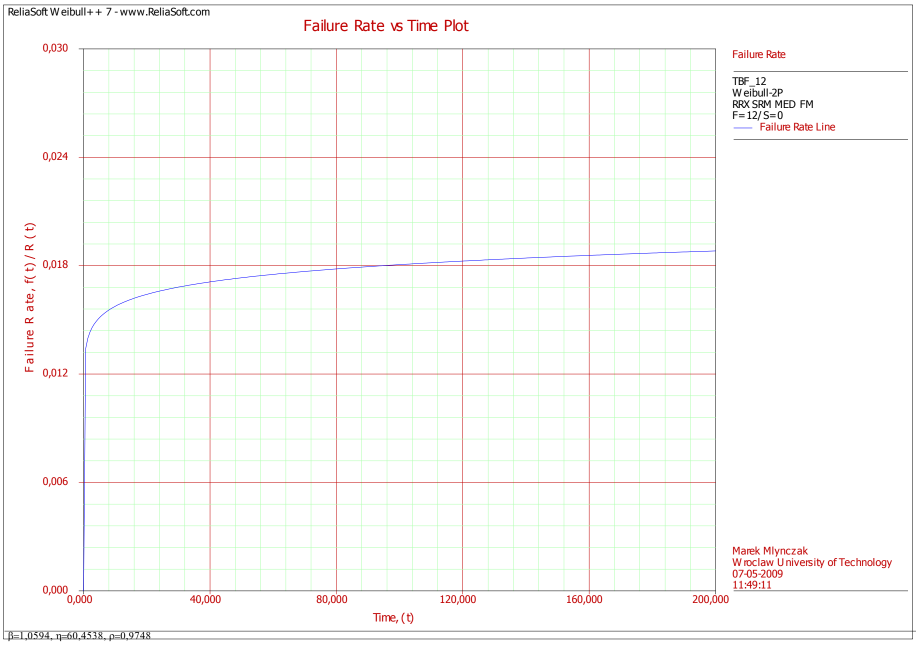


Fig. 4 Function of failure rate (nearly constant) for the 12-th subsystem – power transmission system [4]

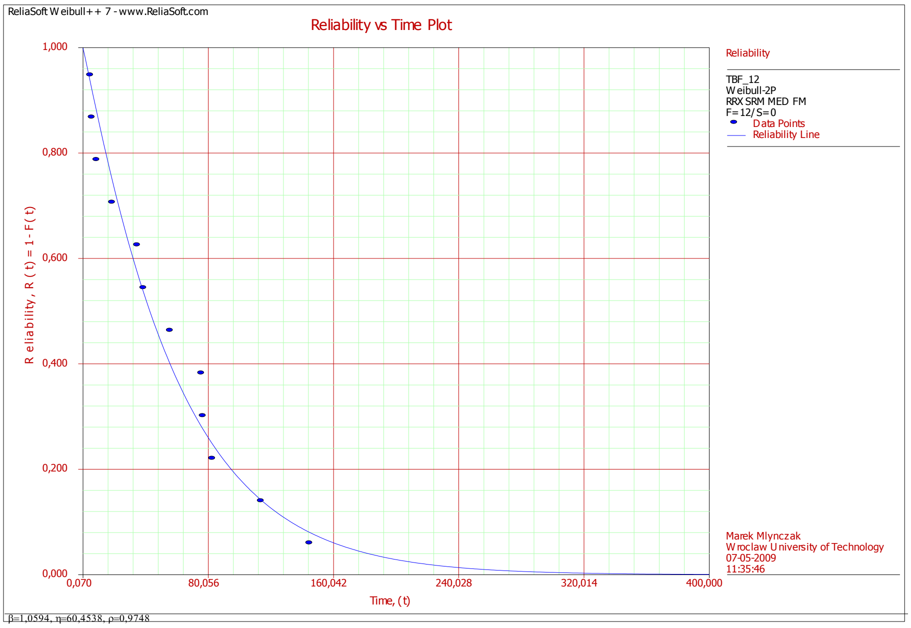


Fig. 5 Function of reliability for the 12-th subsystem – power transmission system [4]

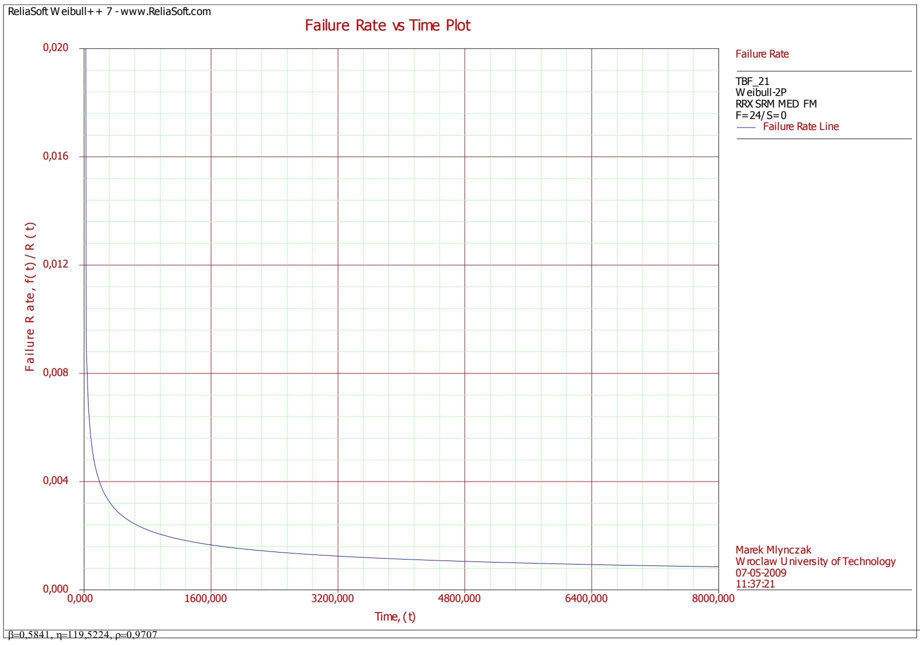


Fig. 6 Function of failure rate (decreasing) for the 21-st subsystem – fire control system [4]

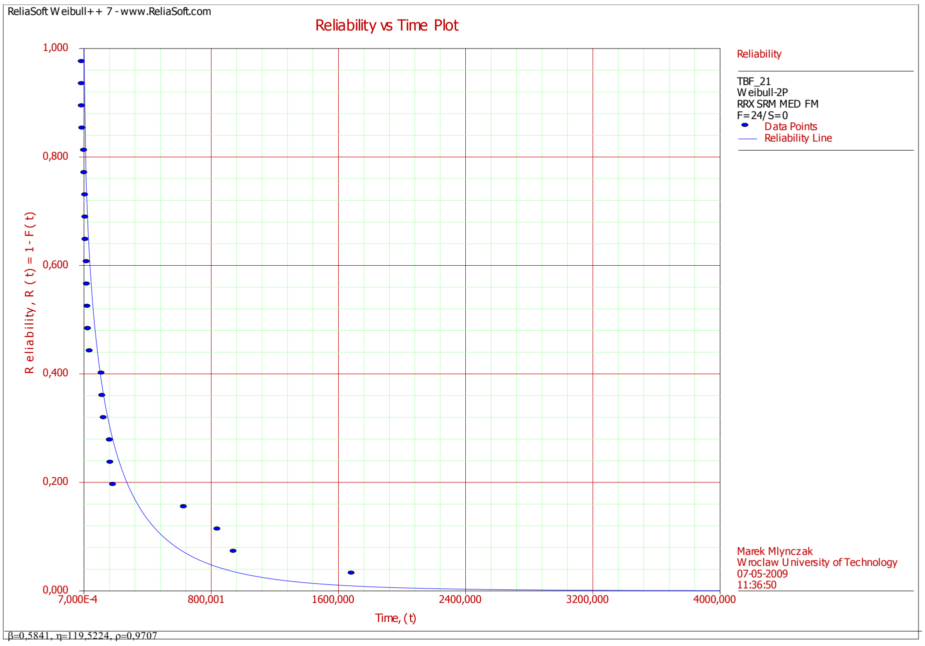


Fig. 7 Function of reliability for the 21-st subsystem – fire control system [4]

5 CONCLUSION

When usage of complex technical weapon systems are considered one should be aware of idea of a weapon system, its life cycle and related costs, its availability and a running-in stage of a weapon system.

The running-in stage last usually over long periods of time and after that the weapon system reaches steady state. In the case of PT-91 tank, the burn-in time lasted about two years for the whole system. The research findings show that some of the subsystems are not related with the infant mortality phase. Analysis of failures recorded during the first 3 years (10 % of the assumed durability of the object) shows that the availability is high at 0.98, and the so-called „damage warranty“ were considered and disposed of by the manufacturer. The performed analysis shows that the theoretical models of safety are fully justified in modeling the operation of complex weapons systems like tanks.

Logistics and administration dominate space of warfare, and neither is easy to defend. In the past these activities took place so far behind the lines that they were reasonably secure. Such is no longer the case which brings into serious question any form of warfare that requires huge logistics and administrative buildup.

In many cases, operational availability cannot be controlled by the manufacturer due to variation in location, resources and other factors that are the sole province of the end user of the product

References

[1] BENTLEY, J. P.: *Introduction to Reliability and Quality Engineering.* Edinburgh Gate, Harlow : Addison-Wesley Longman Ltd., 1999.

[2] BLISCHKE, W., MURTHY, D. N. P.: *Reliability. Modeling, Prediction, and Optimization.* New York : John Wiley & Sons, Inc., 2000.

[3] MOUBRAY, J.: *RCM - an Introduction.* 1st International Society of Automotive Engineers: JA1011 - Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes: Warrendale, Pennsylvania, USA : SAE Publications, Aladon, 2000.

[4] KOWALSKI, K., MLYNCZAK, M.: *Issue of Availability of Weapon Systems in early operation phase.* Motrol, 2009, No 6, p. 105-112.

Col. Eng. Kazimierz KOWALSKI, PhD.
Logistics Department of The General Tadeusz
Kosciuszko Military Academy of Land Forces
Czajkowskiego str. 109
51-150 Wroclaw
Poland
E-mail: k.kowalski@wso.wroc.pl

INFLUENCE OF CHARACTERISTICS OF WHEELED VEHICLE SUSPENSION ON ITS ROAD-HOLDING ALONG CURVED STRETCHES OF TRACK

Mykhailo H. HRUBEL, Mariya B. SOKIL, Roman A. NANIVSKYI

Abstract: It's investigated the influence of the parameters that characterize the renewing force of nonlinear elastic suspension of wheeled vehicles on transverse-angular oscillations of a body and road-holding of vehicle along curved stretches of track. Obtained: the transverse-angular oscillation frequency of a body and critical value of stable motion speed as the function of the oscillation amplitude and the parameters that describe the gravity centre position of a body and renewing force.

Keywords: Transverse-angular oscillations. Amplitude. Frequency. Vehicle suspension. Road-holding.

1 THE RELEVANCE AND OVERVIEW OF THE MAIN RESULTS

Tasks of comfort [1, 2] and stability [3, 4] are some of the most important for the dynamics of wheeled vehicles during its moving along the stretches of track and over rough terrain.

The relevance of these tasks is increasing due to improvement operating characteristics of vehicles. It is primarily about driving speed and use of the vehicle suspension with strongly pronounced nonlinear connection between the deformation of the spring, torsion or pneumatic shock-absorbers and renewing force which acts from its side on a body [5].

The suspension, for which at small shock-absorber deformations the renewing force takes small values and at large ones it is rapidly growing, can provide as proper comfort people and goods transportation, so little driver fatigue. However, theoretical research of the dynamics of vehicles with the indicated characteristic of suspension and moreover with the road-holding haven't found appropriate coverage in the literature. Only in some studies [4-6], in a varying degree, the given problems are considered and only for simplified physical and the corresponding mathematical models of process.

The main reason for such simplified approach to the solution of the given type of tasks is the lack of mathematical apparatus of construction of solutions to nonlinear differential equations describing the vehicle body oscillations and taking into account: a) the curvature and roughness of the stretches of track, and b) nonlinear elastic qualities of the suspension. At the same time, only on the basis of theoretical studies of the dynamics and road-holding of the vehicles on condition of mathematical physical model adequateness can be proposed ways to modernize existing or develop new and more advanced suspensions. Therefore, the question of influence of parameters of nonlinear elastic characteristic of wheeled vehicle suspension on the transverse-angular oscillations and road-holding of wheeled vehicles, that is the subject of this work, is relevant.

2 PROBLEM FORMULATION

To investigate the road-holding of a vehicle along a curved stretch of track will be considered:

1. A vehicle moves with constant velocity V ;
2. The radius of curvature of the road is constant and equal to ρ ;
3. Oscillations of the vehicle (more precisely of its body) occur only in the vertical plane, which is perpendicular to the velocity vector (longitudinal-angular oscillations of vehicle are not considered);
4. Elastic characteristics of wheels are unaccounted;
5. The gravity center of a body in a static position of the vehicle is in the plane, which is parallel to the plane of its symmetry, and its static position is determined by the parameters a and H (or l_1 and β_1).

In this case, as the estimated physical model of wheeled vehicle dynamics can be adopted a system of two bodies: body-rear axle, which interact with each other through suspension. For given physical model the relative position of the vehicle (in the moving frame of reference YOZ) is uniquely determined by the gravity center position of a body (point C) and its rotational angle φ around axis, which passes through the gravity center and is perpendicular to the plane of relative motion (see Fig. 1).

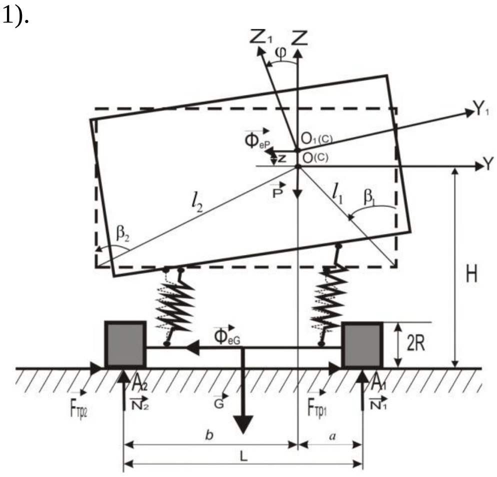


Fig. 1 The physical model of wheeled vehicle dynamics and the distribution of forces

The following external forces act on the specified system of two bodies: body weight - $\vec{P}$ and rear axle weight $-\vec{G}$; road reactions (normal forces $\vec{N}_1, \vec{N}_2$ and friction forces $F_{1mp.}$ and $F_{2mp.}$).

A body is in a complex movement, so the main vectors of portable inertial forces of a body $\vec{\Phi}_{eP}$ and the rear axle $\vec{\Phi}_{eG}$, which caused by road curvature, are directed from the center of road curvature, and their values are equal to $\Phi_{eP} = \frac{P}{g}\frac{V^2}{\rho}$, $\Phi_{eG} = \frac{G}{g}\frac{V^2}{\rho}$. All shown above allows to represent the kinetostatic equations of mechanical system of a body - the rear axle as:

$$-(N_1 + N_2) + P + G - \Phi_r = 0,$$
$$F_{1mp.} + F_{2mp.} - \Phi_{eP} - \Phi_{eG} = 0,$$
$$-N_2 L + G\frac{L}{2} + Pa + \Phi_{eP}(H + z) + \Phi_{eG}R - \Phi_r a + M_A^{\phi} = 0, \tag{1}$$

where friction forces $F_{1mp.}$ and $F_{2mp.}$ are determined in accordance with relations $F_{1mp.} = kN_1$, $F_{2mp.} = kN_2$ ($k -$ *friction coefficient*), M_A^{Φ} – principal moment of inertia forces of a body relative motion relative to the contact point of the right wheel and the road (point A); Φ_{rP} – principal vector of inertia forces of a body in its relative motion; z – vertical component of the displacement of mass center of a body.

Remarks:

1. Here and below it is considered that the radius of the road curvature along its width does not change;
2. The horizontal component of relative motion of mass center of a body is much less than the vertical one and it is unaccounted in the kinetostatic equations.

Task consists in determination of the vehicle velocity magnitude $V = V_{\kappa p}$ at which occurs the loss of dynamic stability of wheeled vehicles movement ($N_2 = 0$).

3 METHODS OF SOLUTION

The obtained kinetostatic equations (1) allow to determine the critical velocity value $\tilde{V}_{\hat{e}\eth}$ at which occurs the loss of motion stability without exclusive of transverse-angular oscillations of a body: $\tilde{V}_{\kappa p} = \sqrt{\frac{\rho g}{HP + RG}\left(P(L-a) + G\frac{L}{2}\right)}$.This value for the case where the symmetry axis of a body passes through the gravity center is transformed to the form: $\tilde{V}_{\kappa p} = \sqrt{\frac{\rho g L}{2(HP + RG)}(P + G)}$. However, as show the experimental studies the given values of “static” critical velocity of motion is much too high. Refined value of the critical velocity of the vehicle on a curved stretch of track, as follows from (1), directly relating to the determination of the moment of inertia forces of a body relative to contact point of a wheel and the road and the main vector of inertia forces of relative motion. Differential equations of relative motion of a body are the basis for its determination. Relative motion of a body is plane-parallel. Thus, the body position in relative motion is uniquely determined by the position of mass center (point O) and rotational angle φ of a body around the axis that passes through the mass center of a body and is perpendicular to the plane of relative motion. The determining factors of relative motion of a body are weight characteristics of suspension (internal factors) and external factors (curvatures of the road).The latest ones, in the case of single roughnesses, we can consider using the initial conditions for the differential equation of transverse-angular oscillations. The foregoing differential equation, under the condition that the elastic characteristics of shock absorbers satisfy the nonlinear law and with sufficient accuracy they can be described by the relation

$$F = c\Delta^{\nu+1}, \tag{2}$$

can be reduced to the form:

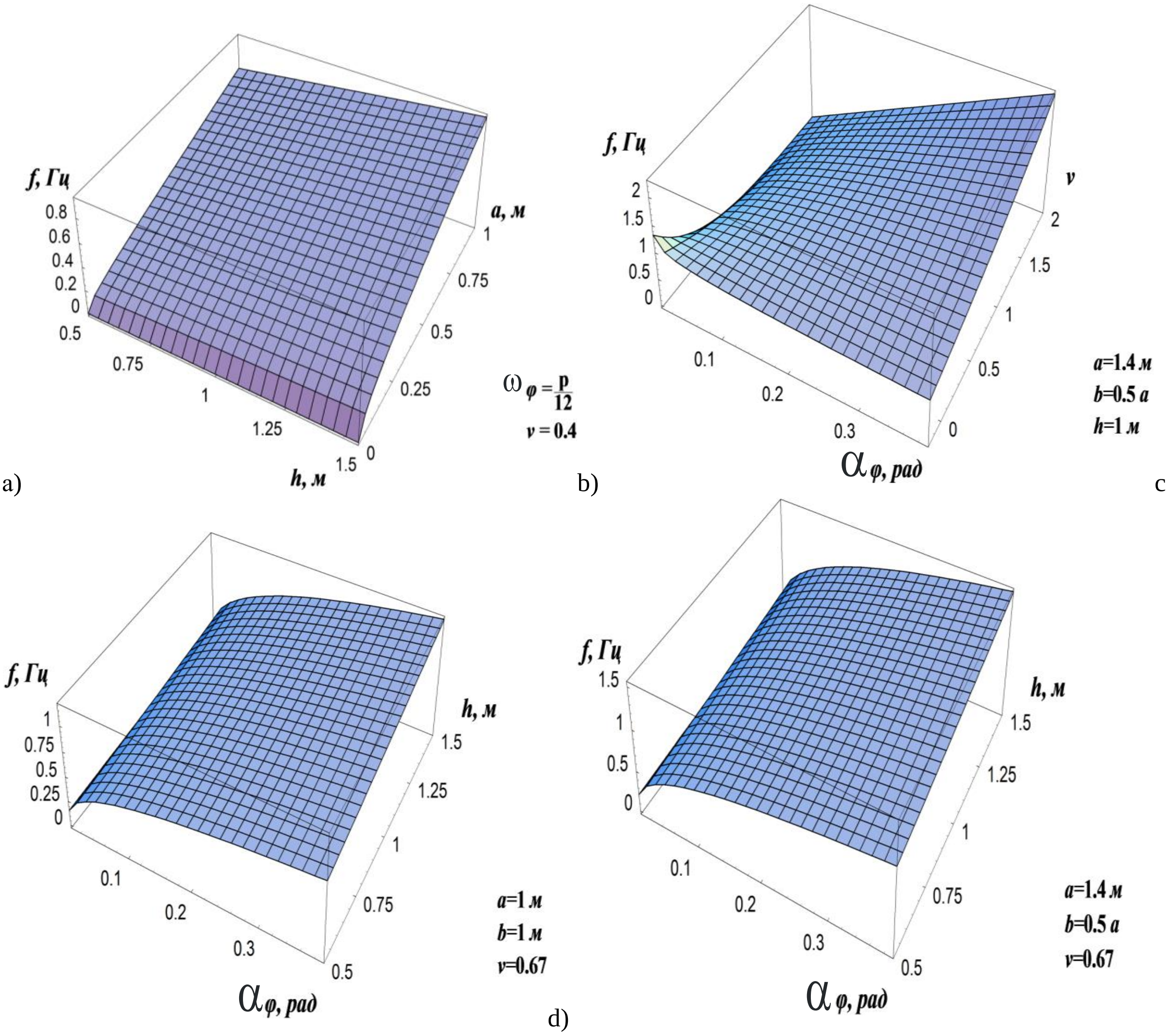
$$I_{\tilde{N}}\ddot{\varphi} + \tilde{n}\varphi^{\nu+1}\begin{bmatrix} l_1^{\nu+2}\sin\beta_1(\sin\beta_1 + \cos\beta_1) + \\ + l_2^{\nu+2}\sin\beta_2(\sin\beta_2 + \cos\beta_2) \end{bmatrix} = 0 .\tag{3}$$

In the relations (2), (3) F – force value of the elastic shock absorber, Δ – its deformation, c, ν – constants, moreover $\nu + 1 = (2m+1)/(2n+1)$, ($m, n = 0,1,2,\ldots$), I_C – inertia moment of a body relative to mass center, $l_1, l_2, \beta_1, \beta_2$ –parameters that define the mass center position. It is easy to make sure that in this case the law of variation in time of the angle of body deviation from the static position is described by the periodic Ateb-functions [8] as:

$$\varphi = a_\varphi ca(\nu + 1, 1, \omega_\varphi(a_\varphi)t + \vartheta),$$
$$\omega_\varphi(a_\varphi) = \sqrt{\frac{c\Xi}{I_C}\frac{\nu+2}{2}}a_\varphi^{\frac{\nu}{2}}, \tag{4}$$

where a_φ and ϑ – the amplitude and initial phase respectively, $\omega_\varphi(a_\varphi)$ – oscillation frequency, and $\Xi = \begin{bmatrix} l_1^{\nu+2}\sin\beta_1(\sin\beta_1 + \cos\beta_1) + \\ + l_2^{\nu+2}\sin\beta_2(\sin\beta_2 + \cos\beta_2) \end{bmatrix}$.

Asemphasized above, the value of parameters a_{φ} and ϑ is determined by the initial conditions (including instant disturbance) and this problem may be the subject of the separate consideration. Figure 2 shows the dependence of the transverse-angular oscillation frequency $f_{\varphi} = \omega_{\varphi}/(2\Pi)$ on some parameters, describing nonlinear elastic characteristics of the suspension components and placement of mass center of a body, $\Pi = \sqrt{\pi}\Gamma\left(\frac{1}{\nu+2}\right)\Gamma^{-1}\left(\frac{1}{2}+\frac{1}{\nu+2}\right)$–half-cycle of used functions.



a) b) c

d)

Fig. 2 The dependence of the body oscillation frequency on the parameters defining the position of the gravity center - a); the amplitude and non-linearity parameter ν – b); the amplitude the parameters defining the position of mass center – c), d)

The obtained dependence (4) describes not only the transverse-angular oscillations of a body around the gravity center, but also is the base for determining the main moment of its inertia forces relative to contact point of a wheel and the road. The main moment of inertia forces of a body relative to the specified above contact point is determined according to the formula:

$$M_{A}^{\phi} = I_{A}\frac{d^{2}\varphi}{dt^{2}}, \qquad (5)$$

where I_A–inertia moment of a body relative to the axis that passes through the contact point of a wheels and the road and is perpendicular to the plane of relative motion, $\frac{d^{2}\varphi}{dt^{2}} = \varepsilon$–angular acceleration of a body. Should be noted that in the planar motion the value of the rotating angle of the body, in contrast to the inertia moment, does not depend on the choice of the pole [9]. The value of the last one relative to the axis that passes through the point A can be determined by the Huygens-Steiner theorem [9]:

$$I_A = I_C + \frac{P}{g}(a+H)^2, \qquad (6)$$

where a –parameter describing the displacement of the gravity center of a body from the plane of vehicle symmetry ($a = l_1 \sin \beta_1$, see Fig. 1).

Angular acceleration ε, based on the relation (4), is equal:

$$\varepsilon = -\frac{2a_\varphi}{\nu+2}\omega_\varphi^2(a_\varphi)ca^{\nu+1}(\nu+1,1,\omega_\varphi(a_\varphi)t+\vartheta). \quad (7)$$

Shown above totality allows to determine the dependence of the inertia forces moment on the position of mass center of a body (a and H parameters), amplitude of its transverse-angular oscillations (a_φ) and parameters, describing nonlinear elastic characteristics of the suspension (ν and c parameters):

$$M_A^\phi = \left(I_C + \frac{P}{g}(a+H)^2\right)\frac{2a_\varphi}{\nu+2}\omega_\varphi^2(a_\varphi)ca^{\nu+1}(\nu+1,1,\omega_\varphi(a_\varphi)t+\vartheta). \quad (8)$$

Considering the properties of periodic Ateb-functions [9], without much difficulty we find the maximum value of the inertia forces moment of a body:

$$\overline{M}_A^\phi = \left(I_C + \frac{P}{g}(a+H)^2\right)c\Xi a_\varphi^{\nu+1}. \qquad (9)$$

Substituting in the relation (1) in place of M_A^ϕ its maximum value $\overline{M}_A^\phi$, we obtain the velocity critical value at which occurs loss of stability of transverse-angular oscillations of the wheeled vehicles

$$V_{кр} = \sqrt{\frac{\rho g}{HP}\left(P(L-a)+G\frac{L}{2}\right)-\left(I_C+\frac{P}{g}(a+H)^2\right)c\Xi a_\varphi^{\nu+1}}. \quad (10)$$

Taking Δ_{cm} as one of the parameters describing the elastic characteristic of the suspension, the wheeled vehicle stability condition transforms to the form

$$V_{кр} < \sqrt{\frac{\rho g}{HP}\left(P(L-a)+G\frac{L}{2}\right)-\left(I_C+\frac{P}{g}(a+H)^2\right)P\Xi\left(\frac{a_\varphi}{\Delta_{cm}}\right)^{\nu+1}}. \quad (11)$$

Fig. 3 presents the dependence of the critical velocity of the wheeled vehicles on the amplitude of transverse-angular oscillations, parameters describing the nonlinear elastic characteristics of the suspension and the position of the mass center of a body.

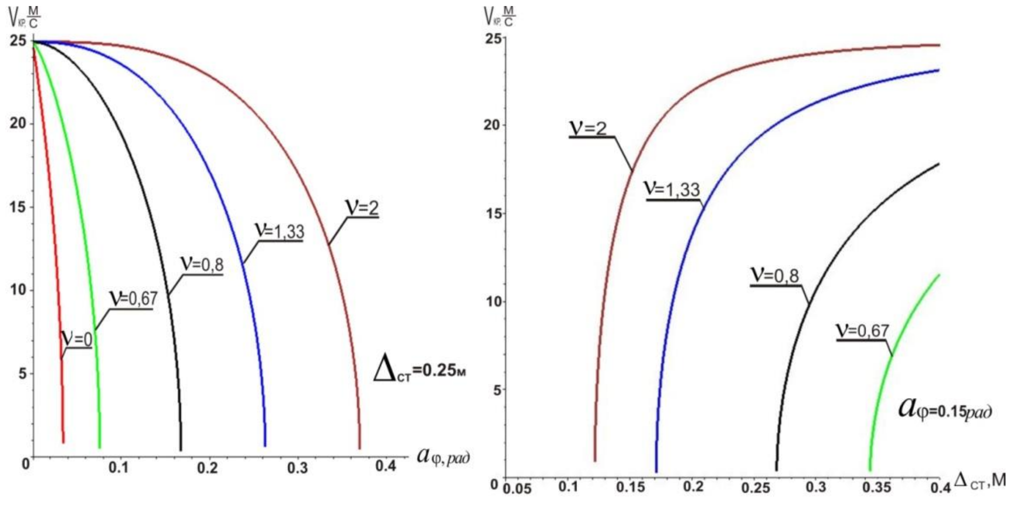


Fig. 3 The dependence of the critical velocity of the wheeled vehicles on the amplitude of transverse-angular oscillations and parameters characterizing the suspension

4 CONCLUSIONS

1. The frequency of transverse-angular oscillations with the growth of oscillation amplitude a_φ and the nonlinearity parameter ν increases (for the linear case $\nu = 0$ does not depend on amplitude);
2. The velocity critical value of the stable motion of wheeled vehicles along curved stretches of track obtained without taking into account the transverse-angular oscillations of a body, is much too high.
3. The transverse-angular oscillations of a body greatly reduce the velocity critical value of stable motion.
4. For the value of parameter $\nu > 0$ of the elastic characteristic of the wheeled vehicle suspension

the velocity critical value of stable motion is higher for smaller transverse-angular oscillation amplitudes.

At the same time the relations obtained above (primarily formula (4), (10) and (11)) can serve as a basis for determining the characteristics of the suspension, proceeding from the conditions of comfort and stability.

References

[1] ROTHENBERG, R.: *Vehicle suspension*. Moscow : Mechanic Engineering, 1972. 392 p.

[2] RAYMPEL, Y.: *Vehicle chassis: Suspension components.* Translated from German by A. Karnukhina, edited by G. Gridasova. Moscow : Mechanic Engineering, 1988. 288 p.

[3] LITVINOV, A.: *Vehicle handling and road-holding*. Moscow : Mechanic Engineering, 1971. 416 p.

[4] BOZHKOVA, L.: Effect of the transverse forced oscillations on the rollover of car during passing the obstacles. In L. Bozhkova, V. Riabov, G. Noritsyna: *Transportation Business of Russia.* 2009. № 03. p. 65-73.

[5] KUZIO, I.: Influence of suspension parameters on nonlinear oscillations of vehicles. In I. Kuzio, B. Sokil, V. Paliukh: Reporter of Lviv Polytechnic National University *"Dynamics, durability and designing of machines and devices"*. Lviv : 2007. № 588. p. 49-52.

[6] SOKIL, B.: Own vertical body vibrations of the vehicle with account of nonlinear characteristics of elastic suspension. In R. Nanivskyi, M. Hrubel: *Scientific production magazine Avtoshliakhovyk.* Kyiv : 2013. № 5 (235). p. 15-18.

[7] KILCHEVSKIY, N.*: Course of Theoretical Mechanics.* II. volume. Moscow : Science, 1977. 544 p.

[8] SENIK, P.: Inversion of incomplete Beta-function. In P. Senik: *Ukrainian Mathematical Journal*. Kyiv : 1969. 21, № 3. p. 325-333.

[9] KRAVETS, I.: Influence of suspension design on the road-holding of wheeled terrain vehicles. In I. Kravets, B. Melnyk*: Interdisciplinary research in science and education*. 2011. №1. Available at: www.es.rae.ru/msno/153-500 (23/11/2913)/

Assoc. Prof. Mykhailo H. HRUBEL, CSc.
Mariya B. SOKIL, CSc.
Roman A. NANIVSKYI
Army Academy named after Hetman P. Sahaidachnyi
Hvardiyska Str. 32
79012 Lviv
Ukraine
E-mail: m.g.grybel@gmail.com
sokil_b_i@ukr.net
roman_nani@ukr.net

ARTIFICIAL NEURAL NETWORKS IN CRYPTOGRAPHY

Martin JAVUREK, Michal TURČANÍK, Marcel HARAKAĽ

Abstract: The use of artificial neural networks (ANN) in cryptography brings many benefits for encrypting messages. Therefore, this article shows an overview of topologies of neural networks for use in cryptography. From the most known as is a Tree Parity Machine, through a Permutation Parity Machine to the use one of the most used ANN with Backpropagation algorithm as a Chaotic random numbers generator. Next, the article describes the learning methods used for the training TPM, such as Hebb's learning rule and Anti-Hebb's learning rule, Backpropagation and Genetic algorithm. Finally, it describes the basic attacks on the ANN such as a Simple Attack, a Geometric Attack, a Majority Attack and a Genetic Attack.

Keywords: TPM. PPM. ANN. Chua's circuit. Hebb's learning rule. Anti-Hebb's learning rule. Backpropagation Genetic algorithm. Simple Attack. Geometric Attack. Majority Attack. Genetic Attack.

1 INTRODUCTION

The main goal of this article is to present an overview of the use of Artificial Neural Networks (ANN) in cryptography, their use and short description of used neural networks. Main topologies of neural networks, such as the most used type the Tree Parity Machine (TPM), next the Permutation Parity Machine (PPM) and the artificial neural network with backpropagation algorithm as the Chaotic Random Numbers Generator will be presented. Next the article will be devoted to basic learning algorithms as are Hebb`s rule and Anti-Hebb`s rule used in the TPM, Backpropagation algorithm and Genetic algorithm for training of ANN. The most common attacks on neural networks will be summarized in the last section such as the Simple Attack, the Geometric Attack, the Majority Attack and the Genetic Attack.

2 TOPOLOGIES OF NEURAL NETWORKS FOR CRYPTOGRAPHY

Different types of neural networks are used in cryptography. For example, the Tree Parity Machine (TPM) that is a special type of a multilayer feed forward neural network, then the Permutation Parity Machine (PPM) that is a variant of the Tree Parity Machine but also the artificial neural network to generate random numbers.

2.1 Tree Parity Machine

The Tree Parity Machine (TPM) is the most common neural network topology for neural cryptography. It consists of $K\times N$ input neurons, K hidden neurons and one output neuron o [1], [2], [4]. The basis of the neural cryptography uses two identical artificial neural networks (ANN) which are able to synchronize after mutual learning. At the beginning each TPM has generated random values of weights (w_{kj}) which are secret. The learning process consists of generating random inputs, same for both TPMs, then computing outputs from the each TPM and their mutual comparing [1], [2], [3], [9].

The TPM (Fig. 1) consists of input bits x, weight vectors w (w is the value of synaptic weight) and the output bit o. Further the TPM consists of the K hidden neurons and the N inputs to the each hidden neuron. Values of synaptic weights w are generated as random discrete values L. So w_{kj} can take numbers from $–L, -L+1, \ldots, L$ [1], [2], [3]. There are assumed that the K, N, L and w are secret for the attacker who is trying to catch the encrypted communication from the public channel. Next assume is that the K, N and L has to be same for both TPMs which are in the synchronization process.

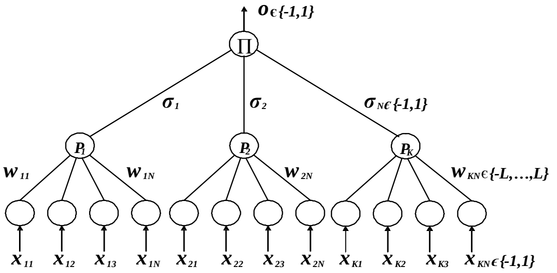


Fig. 1 The architecture of TPM with K=3 (hidden neurons P), N=4 (inputs into the each neuron), w (values of synapse weights), x (outputs bits), σ (output bits from neurons) and o (the output bit) where Π is the mathematical operation of multiplication (14).

2.2 Permutation Parity Machine

The Permutation Parity Machine (PPM) is a binary variant of the TPM. It consists of one input layer, one hidden layer, and one output layer. Number of neurons in the output layer consists of number of neurons K in the hidden layer. Each hidden neuron has N input neurons, for which it is true that x_{ij} are binary [5]:

$$x_{ij} \in \{0,1\} \qquad (1)$$

Weights between input and hidden neurons are binary too, and their definition is:

$$w_{ij} \in \{0,1\} \tag{2}$$

The output value of each hidden neuron is calculated as a sum of all exclusive disjunctions (XOR) of input neurons and these weights:

$$\sigma_i = \theta_N \left(\sum_{j=1}^{N} w_{ij} \oplus x_{ij} \right) \tag{3}$$

where ⊕ represents the operation XOR and $\boldsymbol{\theta_N}$ is a threshold function, which returns values 0 or 1:

$$\theta_N(x) = \begin{cases} 0 \quad if\ x \le N/2 \\ 1 \quad if\ x > N/2 \end{cases} \tag{4}$$

The output of PPM with two or more hidden neurons can be computed as the XOR of the values produced by hidden neurons [5]:

$$o = \bigoplus_{i=1}^{K} \sigma_i \tag{5}$$

According to the work of Luis F. Seonane and Andreas Ruttor [5] the PPM is not secure enough for any cryptographic application.

2.3 Chaotic generator of random numbers

Generators of the random numbers are often used in cryptography. Chaotic generators have recently been applied in cryptography. A chaotic system is aperiodic and sensitive to initial conditions, system parameters and the topological transitivity. One of the most known chaotic generator is a Chua`s circuit (Fig. 2) [6].

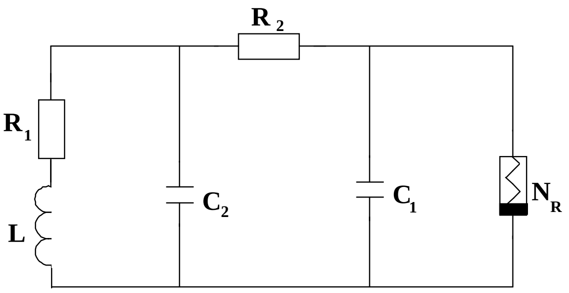


Fig. 2 The chaotic Chua`s circuit

The Chua`s circuit has a simple structure and it consists of two capacitors ($C_1$, $C_2$), an inductor ($L$), two linear resistors ($R_1$, $R_2$) and a non-linear resistor also called the Chua`s diode (N_R). One of the possible implementation of the chaotic Chua's circuit in the ANN is shown in Fig. 3. It is based on the backpropagation algorithm [6].

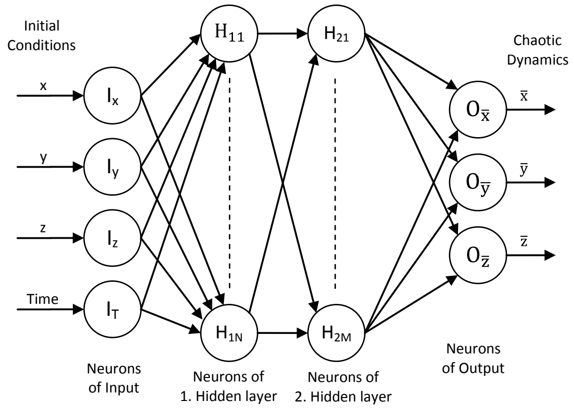


Fig. 3 The block diagram of trained ANN model

The cryptography based on the ANN chaotic generator (Fig. 4.) [6] consists of the Control Unit which gives initial conditions into the chaotic generator. The Generator generates chaotic dynamics with using initial conditions and chaotic dynamics encrypt the plain text into the cipher text. Chaotic dynamics is a sequence of random numbers generated by the chaotic generator.

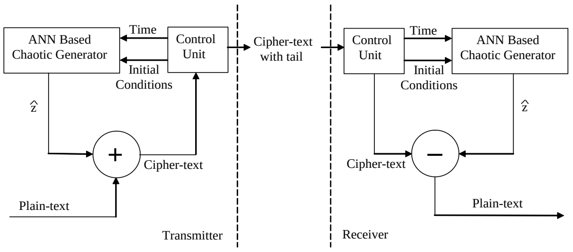


Fig. 4 The block diagram of ANN based chaotic crypto-system

This message is sent to the receiver where the Control Unit removes initial conditions. These initial conditions are sent to the chaotic generator and it generates chaotic dynamics which it is able to decrypt the cipher text again and get the plain text.

3 METHODS OF LEARNING NEURAL NETWORKS

For synchronization of the tree parity machine, there are compared outputs ***o*** both TPMs and on their base, they learn until they are not synchronized. The most used learning rules for TPMs are Hebb`s learning rule (15), Anti-Hebb`s learning rule (16), and the Random walk algorithm (17).

3.1 Hebb`s learning rule

Hebb`s learning rule is based on adaptation weights of mutual interaction of the input and the output signal. If two neurons are connected with single value of the synaptic weight and they are activated simultaneously the value of weight is increased. And the value of weight is reduced if they are activated separately. The following formula describes Hebb`s learning:

$$w_{ij} = x_i x_j \qquad (6)$$

where $\boldsymbol{w_{ij}}$ is weight between neurons ***i*** and ***j***, $\boldsymbol{x_i}$ is neuron input ***i*** and $\boldsymbol{x_j}$ is neuron input $\boldsymbol{x_i}$.

Another formula describing Hebb`s learning rule is:

$$w_{ij} = \sum_{k=1}^{n} x_i^k x_j^k \qquad (7)$$

where $\boldsymbol{w_{ij}}$ is weight between neurons ***i*** and ***j***, ***n*** is numbers of neuron input, and $\boldsymbol{x_{ik}}$ is $\boldsymbol{k^{th}}$ input to the neuron ***i*** and $\boldsymbol{x_{jk}}$ is $\boldsymbol{k^{th}}$ input to the neuron ***j***.

Hebb's Rule is generalized as:

$$\Delta w_i = \eta x_i y \qquad (8)$$

the change in the $\boldsymbol{i^{th}}$ synaptic weight $\boldsymbol{w_i}$ is equal to a learning rate ***η*** (positive constant ***η*** ∈***(0, 1)***) times the $\boldsymbol{i^{th}}$ input $\boldsymbol{x_i}$ times the postsynaptic response ***y*** for the linear neuron:

$$y = \sum_j w_j x_j \qquad (9)$$

where $\boldsymbol{w_j}$ is the weight of $\boldsymbol{j^{th}}$ neuron and $\boldsymbol{x_j}$ is the input of $\boldsymbol{j^{th}}$ neuron.

In TPM where inputs are binary [2], [4], [9]:

$$x_{ij} \in \{-1,1\} \qquad (10)$$

and weights between inputs and ***K*** hidden neurons have values:

$$w_{ij} \in \left\{ -L, -L+1, \dots \;\; , L \right\} \qquad (11)$$

the output value of each hidden neuron is equal to the sign of the sum of all multiples of inputs and their weight values [1], [2], [4], [9]:

$$\sigma = \operatorname{sgn}\left(\sum_{j=1}^{N} w_{ij} x_{ij} \right) \qquad (12)$$

where ***sgn*** is a simple function that returns values ***-1***, ***0*** or ***1*** [1], [2]:

$$\operatorname{sgn}(x) = \begin{cases} -1 & if\ x < 0 \\ 0 & if\ x = 0 \\ 1 & if\ x > 0 \end{cases} \qquad (13)$$

The input of neural network is calculated as a multiplication of all input values created with hidden neurons (14) and where the output from the TPM is binary [2], [4].

$$o = \prod_{i=1}^{K} \sigma_i \qquad (14)$$

During synchronization between two TPMs there are compared values of both TPM outputs and two situations can occur. Both outputs ***o*** are different and then it is again generated the random input vector ***x*** and new output is computed or both outputs are same and then one of learning rules is applied (15), (16), (17) [1], [2], [3], [9].

Hebb`s learning rule (15), both neural networks are learning from each other:

$$w_i^+ = w_i + \sigma_i x_i \theta(\sigma_i o)\theta(o^A o^B) \qquad (15)$$

where θ is excitation threshold.

Anti-Hebb`s learning rule (16), both neural networks learn with opposite as their own outputs:

$$w_i^+ = w_i - \sigma_i x_i \theta(\sigma_i o)\theta(o^A o^B) \qquad (16)$$

Random walk (17), the set value of the output is not important for synchronization as long as it is the same for all participating neural networks [2], [3], [9].

$$w_i^+ = w_i + x_i \theta(\sigma_i o)\theta(o^A o^B) \qquad (17)$$

3.2 Anti-Hebb`s learning ng rule

Anti-Hebb`s learning rule is inverse toward Hebb`s learning rule. Hebb`s learning rule increases value of the weight if neurons are activating synchronously unlike Anti-Hebb`s learning rule where value of the weight is reduced if neurons are activating synchronously.

Anti-Hebb`s learning rule is generalized as:

$$\Delta w_i = \eta(x_i y - w_i y^2) \qquad (18)$$

where the change in the $\boldsymbol{i^{th}}$ synaptic weight $\boldsymbol{w_i}$ is equal to a learning rate ***η*** times the $\boldsymbol{i^{th}}$ input $\boldsymbol{x_i}$ times the postsynaptic response ***y*** for the linear neuron (19) minus the $\boldsymbol{i^{th}}$ weight times squared of the response ***y*** :

$$y = \sum_j w_j x_j \qquad (19)$$

where the $\boldsymbol{w_j}$ is weight of the $\boldsymbol{j^{th}}$ neuron and the $\boldsymbol{x_j}$ is input of the $\boldsymbol{j^{th}}$ neuron.

3.3 Backpropagation

One of the most used ANN is the feedforward network with the backpropagation algorithm (or also the backpropagation of errors) [7]. Elements or nodes of the feedforward neural network are arranged into different layers: the input, the middle or also the hidden and the output. The output from the feedforward neural network with the backpropagation algorithm is computed using a procedure known as the forward pass [8]:

- The input layer propagates a particular input vector's components entering to the each node in the middle layer.
- Middle layer nodes compute output values, which become inputs to the nodes of the output layer.
- The output layer nodes compute the network output for the particular input vector.

The forward pass produces an output vector for a given input vector based on the current state of the network weights. The weights are adjusted to reduce the error by propagating the output error backward through the network. This process is known as the backward pass [8]:

- Compute the error values for the each node in the output layer. This can be computed because the desired output for the each node is known.
- Compute the error for the middle layer nodes. This is done by attributing a portion of the error at each output layer node to the middle layer node, which feed that output node. The amount of error due to the each middle layer node depends on the size of the weight assigned to the connection between the two nodes.
- Adjust the weight values to improve network performance using the Delta rule.
- Compute the overall error to test network performance.

The training set is repeatedly presented to the network and the weight values are adjusted until the overall error is below a predetermined tolerance. Since the Delta rule follows the path of greatest decent along the error surface, local minima can impede training [8].

3.4 Genetic algorithm for training

Backpropagation has some disadvantages. First is the scaling problem. Backpropagation works well on the simple training problems. However, as the problem complexity increases, the performance of backpropagation falls off rapidly. Second drawback is that to compute a gradient requires differentiability. Therefore backpropagation cannot handle discontinuous optimally criteria or discontinuous node transfer functions. This precludes its use on some common node types and simple optimality criteria [14].

Genetic algorithms should not have problem with scaling as backpropagation. One reason for this is that they generally improve the current best candidate monotonically. They do this by keeping the current best individual as part of their population while they search for better candidates. Secondly, genetic algorithms are generally not bothered by local minima. The mutation and crossover operators can step from a valley across a hill to an even lower valley with no more difficulty than descending directly into a valley [14].

Genetic algorithms are algorithms for optimization and learning based loosely on several features of biological evolution. It requires five components [14]:

1. A way of encoding solutions to the problem on chromosomes. The weights (and biases) in the neural network are encoded as a list of real numbers.
2. An evaluation function that returns a rating for each chromosome given to it. Assign the weights on the chromosome to the links in a network of a given architecture, run the network over the training set of examples, and return the sum of the squares of the errors.
3. A way of initializing the population of chromosomes. The weights of the initial members of the population are chosen at random with a probability distribution. This is different from the initial probability distribution of the weights usually used in backpropagation, which is uniform distribution between -1 and 1.
4. Operators that may be applied to parents when they reproduce to alter their genetic composition. Included might be mutation, crossover (i.e. recombination of genetic material), and domain-specific operators.
5. Parameter settings for the algorithm, the operators and so forth. There are a number of parameters whose values can greatly influence the performance of the algorithm.

Given these five components a genetic algorithm operates according to the following steps [14]:

1. The population is initialized. The result of the initialization is a set of chromosomes.
2. Each member of the population is evaluated. Evaluations may be normalized and important thing is to preserve relative ranking of evaluations.
3. The population undergoes reproduction until a stopping criterion is met. Reproduction consists of a number of iterations. One or more parents are chosen to reproduce. Selection is stochastic, but the parents with the highest evaluations are favored in the selection. Then the operators are applied to the parents to produce children. And at the end, the children are evaluated and

inserted into the population. In some version of the genetic algorithm, the entire population is replaced in each cycle of reproduction. In others, only subsets of the population are replaced.

4 ATTACKS ON NEURAL CRYPTOGRAPHY

Safety of the neural exchange protocol is based on the fact that two ANN (*A*, *B*) communicating with each other are synchronized faster than the third network (*E*) which is trained only to capture the input and outputs from the synchronizing ANN from the public channel. The attacker does not know the topology of the ANN and what output values are in the each hidden neuron so that the most of attacks are based only on estimate status of hidden neurons [12, 13].

4.1 Simple attack

The attacker ANN *E* has the same structure as *A* and *B*. Then *E* starts with random initial weights and trains with the same inputs transmitted between *A* and *B* over the public channel. After that *E* learns the mutual output bit $o^{A/B}$ between *A* and *B* and applies the same learning rule by replacing o^E with $o^{A/B}$ [2], [10]:

$$w_k^E = w_k^E - o^A x_k \theta(\sigma_k^E o^{A/B})(o^A o^B) \qquad (20)$$

4.2 Geometric attack

A geometric attack can outperform the simple attack because, in addition to applying the same learning process, *E* can exploit o^E and the local fields of its hidden units, h_1^E, h_2^E, ..., h_k^E. When $o^{A/B}$ is equal to o^E, *E* applies only the same learning rule used by *A* and *B* but if $o^{A/B}$ is not equal to o^E, then *E* tries to correct its internal representation h_1^E, h_2^E, ..., h_k^E. The lower the absolute value of $|h_i^E|$, the higher the probability that $o^{A/B}$ is not equal to o^E and this probability is known as the maximum error prediction ε_i^p. Therefore, *E* will modify the hidden neurons with minimum $|h_i^E|$ before applying the learning rule [2], [10], [11].

4.3 Majority attack

The majority attack is similar to the geometric attack. However, *E* can increase the probability to predict the internal representation of any of the partners' TPM. The majority attack is also called a cooperative attack because *M* TPMs (*M* is number of cooperating TPMs) are working in a cooperating group rather than as individuals. Instead of using only one TPM, the attacker starts with *M* TPMs with random weight vectors to achieve a zero overlap between them. If o^A is not equal to o^B, weights are not updated but for o^A is equal to o^B, the attacker must update its own TPM. Then it calculates the output bit of all its attacking ANNs. If the ***m**^th^* output bit of attacking ANN $\boldsymbol{o^{E,m}}$ is not equal to $\boldsymbol{o^A}$, then the geometric attack is applied individually for every $\boldsymbol{m^{th}}$ ANN and no update will occur before cooperating with other ANNs. Next, ***E*** searches for the common internal representation among the ***M*** TPMs and updates their weights according to this majority vote. In order to avoid the expected high correlation between the ***M*** TPMs, the majority attack and the geometric attack are applied alternately in even and odd steps, respectively [11].

4.4 Genetic attack

In the genetic attack, the attacker starts with only one TPM but is permitted to use ***M*** TPMs. Because the most challenging issue in the mutual learning process is to predict the internal representation of either TPM$^{\boldsymbol{A}}$ or TPM$^{\boldsymbol{B}}$, the genetic attack directly deals with this difficulty. For a specific value of $\boldsymbol{o^{A/B}}$, there are $\boldsymbol{2^{K-1}}$ different internal representations to reproduce this value. The genetic attack handles all these possibilities in a parallel fashion. The genetic attack proceeds as follows [9], [11]:

- If $\boldsymbol{o^A = o^B}$ and ***E*** has at most $\boldsymbol{M/2^{K-1}}$ TPMs, $\boldsymbol{2^{K-1}}$ TPMs are generated and each updates its weights based on one of the possible internal representations. This step is known in genetic algorithms as the mutation step.
- If E has more than M/2K−1 TPMs, the mutation step will be essentially an overhead due to the exponential storage needed. Therefore, the attacker must discard some of the TPMs to avoid exponential storage increase. As a genetic algorithm, the discarding procedure is based on removing the TPMs with the least fittest function. The algorithm uses two variables ***U*** and ***V*** as the fitting functions. The variable ***U*** represents the number of correct prediction of $\boldsymbol{o^A}$ in the last ***V*** training steps.

5 PLUSES AND MINUSES OF NEURAL NETWORKS IN CRYPTOGRAPHY

Advantages of using neural networks in cryptography are mainly lower processing power compared with the RSA algorithm, because neural network cryptography is not based on number theory. It is more difficult to break the cipher because the cryptography based on the TPM expects faster synchronization than attacker's network. The main reason is that two TPMs cooperate together during synchronization process. However, attacker's network does not cooperate with them. ANNs can be software based or hardware based. If ANNs are hardware based they can be analog or digital.

Disadvantages are mainly the time needed to synchronize. The ANN needs time for learning so it cannot start encrypting immediately. For ANNs with a large number of neurons and synapses there is needed high processing time for the training of ANN. ANN architecture is different from universal microprocessor architecture so the network must be emulated or special processors or FPGA must be used.

6 CONCLUSION

In the article the most used topologies of neural networks in cryptography are presented. It follows that the most used topology is still the Tree Parity Machine. The experiment [5] has found out that the Permutation Parity Machine is not suitable for using in cryptography. In the future it is suitable to focus on TPMs and develop their security against the attack. We have presented the use of artificial neural network as a random numbers generator for encrypting and decrypting what appear as a perspective area in the neural network cryptography. In the article the most used learning rules for TPM and also one of the most used learning process in the artificial neural network, the Backpropagation algorithm and Genetic algorithm for training have been shortly introduced. Traditional methods of cryptography are tested to attempt to break the cipher and either the neural cryptography is no exception. In the article, also the most known possible attacks on the artificial neural networks are mentioned.

References

[1] KANTER, I., KINZEL, W.: The Theory of Neural Networks and Cryptography. In *Quantum Computers and Computing*. V. 5, No1, pp. 130-140. 2005.

[2] RUTTOR, A., KINZEL, W., KANTER, I.: Dynamics of Neural Cryptography. In *Physical review.* E 75, 056104, Statistical, nonlinear, and soft matter physics, 2007. ISSN 1539-3755.

[3] SANTHANALAKSHMI, S., SANGEETA, K., PATRA, G. K.: Design of Stream Cipher for Text Encryption using Soft Computing based Techniques. In *IJCSNS International Journal of Computer Science and Network Security*. Vol.12, No.12, pp. 149-152. 2012.

[4] KINZEL, W., KANTE, I.: Neural Cryptography. In *9th International Conference on Neural Information Processing, Singapor.*, pp. 1351 – 1354, vol. 3, 2002.

[5] SEOANE, L. F., RUTTOR, A.: Successful Attack on Permutation-parity-machine-based Neural Cryptography. In *Phys. Rev.* E 85, 025101(R). 2012.

[6] DALKIRAN, I., DANISMAN, K.: Artificial Neural Network Based Chaotic Generator for Cryptology. In *Turk J Elec Eng & Comp Sci*. Vol. 18, No.2, pp. 225-240. 2010.

[7] VOLNA, E., KOTYRBA, M., KOCIAN, V., JANOSEK, M.: Cryptography Based on Neural Network. In *26th EUROPEAN Conference on Modelling and Simulation*. Koblenz, Germany, DOI: http://dx.doi.org/10.7148/2012-0386-0391.2012.

[8] SHIHAB, K.: A Backpropagation Neural Network for Computer Network Security. In *Journal of Computer Science*. Volume 2, Issue 9, pp. 710-715. 2006.

[9] RUTTOR, A., KINZEL, W., NACH, R., KANTER, I.: Genetic Attack on Neural Cryptography. In *Phys. Rev.* E 73.036121. 2006.

[10] ALLAM, A. M., ABBAS, H. M.: On the Improvement of Neural Cryptography Using Erroneous Transmitted Information with Error Prediction. In *IEEE Transactions on Neural Networks.* Volume 21, Issue 12, pp. 1915 – 1924. 2010.

[11] PRABAKARAN, N., VIVEKANANDAN, P.: A New Security on Neural Cryptography with Queries. In *Int. J. of Advanced Networking and Applications*. Volume 02, Issue 01, pp. 437-444. 2010.

[12] STOIANOV, N.: One Approach of Using Key-Dependent S-BOXes in AES. In *MCSS 2011*, CCIS 149, Springer-Verlag Berlin Heidelberg, 2011, pp. 317–323, ISBN 978-3-642-21512-4.

[13] NIEMEC M. N., STOIANOV, N.: Testing basic security features of symmetric block ciphers. In *Bulgarian Cryptography Days – BulCrypt 2012*. Proceedings, Sofia, 2012, pp. 37-48, ISBN 978-954-2946-22-9.

[14] MONTANA D. J., DAVIS L.: Training Feedforward Neural Networks Using Genetic Algorithms. In *Proceedings of the International Joint Conference on Artificial Intelligence*. San Francisco, 1989, pp. 762-767.

Eng. Martin JAVUREK
Eng. Michal TURČANÍK, PhD.
Assoc. Prof. Eng. Marcel HARAKAĽ, PhD.
Armed Forces Academy
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: martin.javurek@aos.sk
michal.turcanik@aos.sk
marcel.harakal@aos.sk

MATERIAL ANALYSIS OF DEMAGED 125 MM TANK MAIN GUN TYPE TK 2A46

David KUSMIČ, Zbyněk STUDENÝ,Vojtěch HRUBÝ, Emil SVOBODA

Abstract: In this paper are described procedures and methods used for material evaluation of materials applied for new damaged or wrecked tank main gun. Following approaches and devices were used for the main tank gun material analysis: sampling and samples preparation of the main tank gun core material, chemical composition analysis (for spectral analysis was the LECO SA – 2000 device used), microstructure evaluation (using the Neophot 32 light microscope, with digital camera Color View IIIμ Olympus device under magnification of 50x and 500x), material purity evaluation (due to the chemical composition of the steel was the inspection on the presence of oxides, sulphides, nitrides and silicates focused), assessment of the surface fracture, testing the mechanical properties - including the tensile tests (using the Zwick Z 100 testing machine), Charpy impact tests (instrumented impact tester Zwick RKP 450 IWI), fractographic analysis of the fracture surfaces of testing rods and hardness testing (Vickers HV_{30}). The obtained values of material characteristics and microstructure evaluation were compared to the standard material values.

Keywords: Tank main gun. Material analysis. Microstructure. Mechanical properties. Fracture.

1 INTRODUCTION

The Ministry of Defence – the Section of Logistics, Army of the Czech Republic specified the requirements for material analysis of damaged 125 mm tank main gun Type TK 2A46. The material analysis was performed on tank main gun fragments. The technical documentation or drawings were no longer available, just the expert opinion was provided by the Czech Police for consultation. These reports, however, did not refer to any evaluation problem of material characteristics. The paper describes the procedures and technics used for the material characteristics verification of material which was applied for production of damaged 125 mm tank main gun Type TK 2A46.

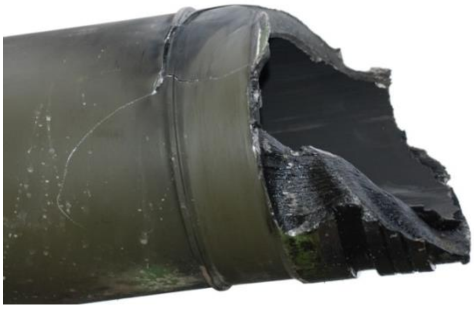


Fig. 1 The braking detail of main tank gun

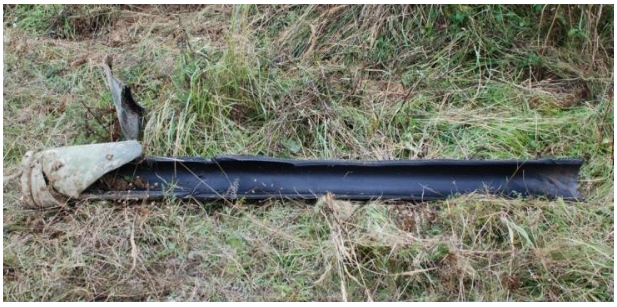


Fig. 2 The main tank gun fragments after destruction

Tab. 1 Chemical composition of analysed and associated steels

Marking (standard)	Element [wt%]								
	C	Mn	Si	P	S	Cr	Ni	Mo	Cu
Measured	0.42	0.37	0.26	0.007	0.008	1.07	3.01	0.57	0.12
CSN 4216540	0.30 0.40	0.50 0.80	0.15 0.40	0.035	0.035	0.70 1.10	2.75 3.25	0.25 0.40	-
The general requirement for the chemical composition	0.30 0.40	0.60 0.80	max. 0.40	max. 0.011	max. 0.011	1.00 2.00	1.50 3.00	0.20 0.30	-

2 SAMPLING AND SAMPLE PREPARATION OF THE TANK MAIN GUN MATERIAL

Fragments and parts of the 125 mm damaged main tank gun which were separated after destruction are presented in Fig. 1 and 2 and were delivered for the material analysis.

For the material evaluation and testing were the samples taken from the fragments of damaged main tank gun. The samples were taken after photographic documentation.To avoid thermal or mechanical effects on the analysed part of main tank gun the sampling was carried out by machining. It´s necessary to note the fragments and fracture area of the main tank gun, which were available for the analysis showed corrosion attack on the fractured surface areas. Of course this surface could not be used for fractographic analysis at all.

3 MATERIAL ANALYSIS

3.1 Chemical composition evaluation

Chemical composition evaluation of the main tank gun material composition consisted of spectral analysis using the LECO SA – 2000 spectrometer device, using the GDOES/Bulk methode. To the calibration procedure the CKD standards 180A ÷ 189A were used. For the values of chemical composition (in wt %) see in Tab. 1. The average values of two measurements on several places of the main tank gun are shown in Tab. 1.

The won chemical composition is close to the CSN 4216540 steel with relatively small variation of content of Mn and a significantly lower amount of basic impurities and elements like P and S. The chemical composition and marked CSN 4216540 does not match precisely the any steel specified according to CSN, ASTM, DIN, EN, or ISO standard, but it is equivalent only to the GOST 4543-71steel. This 16 540 steel is in general for artillery barrels required. The evident higher content of Mo in the evaluated steel causes higher level of mechanical properties, it will be discused later.

3.2 Purity evaluation

The purity evaluation was according to the CSN ISO 4967 standard performed.

For the purity evaluation were the Charpy impact test samples used, for greater evaluation area.

The samples were prepared in a direction parallel to the longitudinal axis of the main tank gun. Considering the chemical composition of the steel, a test for the presence of oxide (D), sulphides (A), nitrides (B) and silicates (C) was carried out.

Purity evaluation was performed on polished surfaces of samples at a magnification of 100x, displaying the sample surface area of 0.50 mm^2 using the ocular according to the method B (Chapter 5.2.2 of the Standard).

There was found a predominant content of fine globular oxides (D), corresponding to both - the fine and coarsed inclusions (with size of 8÷13 μm) indexed by number 0.5 up to 1.

The ratio of sulphides (A) with size greater than 3 μm was at a minimum value of tested Samples found, as well as the ratio of silicates (C). Inclusions of B-type (nitrides) and DS-type (individual globular inclusions) were not indicated. Locally were sulfide inclusions of enormous size detected, total length of two inclusions was of 77 μm (see Fig. 3).

The evaluation was carried out according to paragraph 6.2 of the Standard, for the results see Tab. 2.

It is clear that the local accumulation of enormous sized inclusions can the crack nucleation and propagation cause. But it is not clear that this fact was the reason of the main tank gun destruction.

Tab. 2 Purity evaluation

Evaluation	Type of inclusion				
	A	B	C	D	DS
The maximal index number i	1	-	1	1	-
Results	A 1s	-	C 1e	D 1e	-

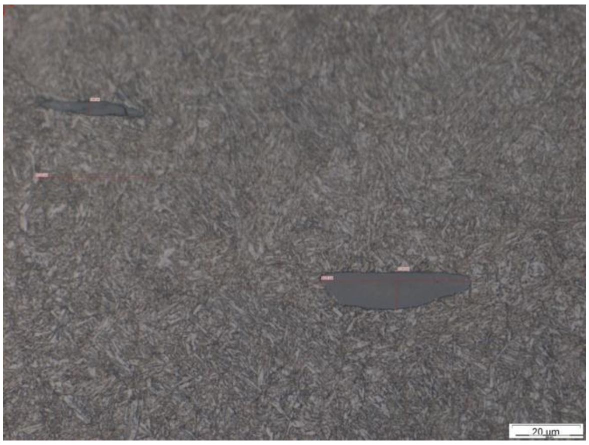


Fig. 3 Sulfide inclusions of enormous size

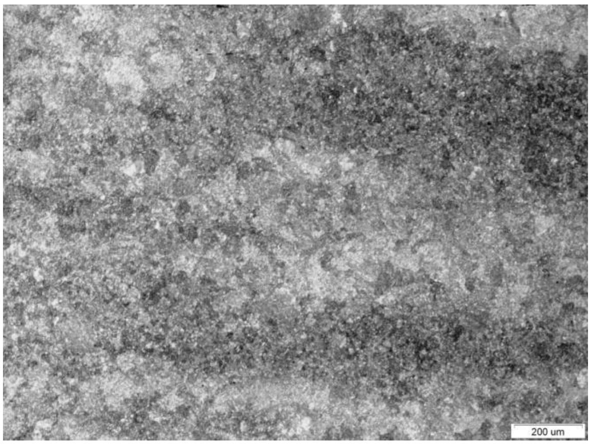


Fig. 4 Line microstructure

3.3 Microstructure evaluation

The microstructure evaluation was used for the heat treatment procedures verification. For microstructure evaluation were the Charpy impacttest samples used (see Fig. 4 and 5). The samples marked as No 1. and 2. were taken from the wrecked parts of the main tank gun in direction parallel to the longitudinal longer axis and samples marked as No 3. and 4. in perpendicular direction to the longitudinal axis.

The microstructure was documented using the Neophot 32 light microscope devide with digital camera Olympus Colour View III under magnification of 50x and 500x.

During the microstructure evaluation was the line microstructure documented (see Fig. 4). Using the microhardness tests $HV_{0.01}$ in perpendicular direction were differences of microharness values detected, in the range of 423 up to 552 $HV_{0.01}$. The line microstructure can in general affect the direction of crack propagation, but it is not likely to cause the crack nucleation. From the analysis of the structureof all samples is evident that it consists of homogeneous, tempered martensite, and corresponds to the desired state.

4 TESTING THE MECHANICAL PROPERTIES

According to the principles of sampling, samples were taken from damaged main tank gun segments for the tensile and impact tests.
Folowing samples and tests were prepared:

- Flat test rods for the tensile tests with orientation parallel to the longitudinal axis;
- For the impact tests two samples with orientation parallel to the longitudinal axis and two samples in perpendicular direction to the longitudinal axis (see Tab. 3).

4.1 Tensile tests

For tensile tests of the dimensions listed in Tab. 3 were two flat samples prepared. Sample No. 2 - prepared from the wrecked parts of the main tank gun in direction parallel to the longitudinal axis and sample No 4. in perpendicular direction to the longitudinal axis (see Tab. 3).

Tensile tests were performed using the Z100 tensile testing device. For the results of tensile tests see Fig. 7 and Tab. 4.

The tensile test results shows that the heat treatment was carried out to reach very high mechanical properties, which leads to decreasing deformation characteristics, values of toughness and fracture toughness as well. (see Tab. 4).

4.2 Charpy impact test

Charpy impact tests were performed using the pendulum impact tester Zwick type RKP 450 IWI device. The samples No 1. and 2. were from the wrecked parts of the main tank gun prepared in direction parallel to the longitudinal longer axis and samples No 3. and 4. in perpendicular direction To the longitudinal axis. Samples dimensions are marked in Tab. 5. The won values obtained during the bend impact test are shown in Tab. 6. The results of Charpy impact tests are shown in Fig. 8 and 9.

The results of the bending impact test were compared to the fractographic analysis of the fracture surfaces of tested rods. Fracture areas of samples 1, 2, 3 and 4 are shown in Fig. 10 ÷ 13.

The evaluated fracture surfaces of the samples after impact bending test shows that the breaking occurred as half developed cup-and-cone fracture, caused by thermal treatment processed to achieve higher values of strength characteristics, whichgenerally causes the toughness decreasing. This fact is evident for samples 3 and 4 (see Fig. 12 and 13).

Fracture surfaces, shown in Fig. 11, 12. and 13, are very inhomogeneous, which is associated to the line microstructure as a result of manifacturing and to the locally exclusion of impurities, as mentioned in Chapter 3.2.

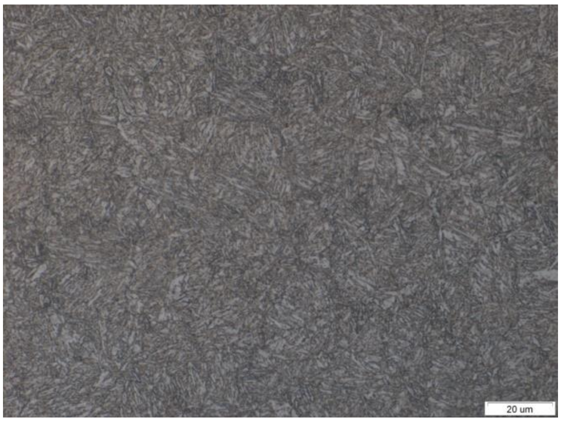


Fig. 5 Microstructure for Charpy impact test parallel to the longitudinal axis of the main tank gun (sample No 1.)

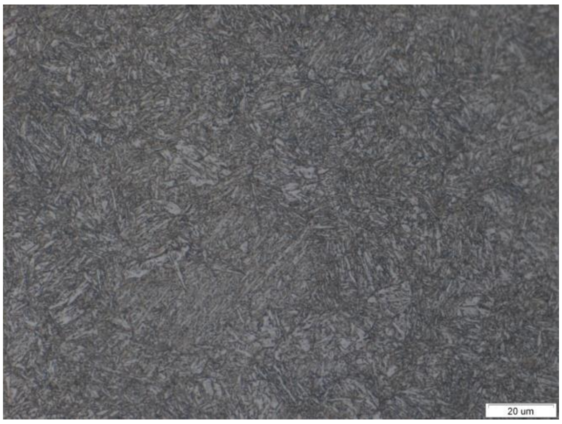


Fig. 6 Microstructure for Charpy impact test perpendicular to the longitudinal axis of the main tank gun (sample No 1.)

Tab. 3 Dimensions of test rods

Sample	a_0 [mm]	b_0 [mm]	S_0 [mm]	L_0 [mm]
2	4.9	13.8	68.2	50.0
4	3.8	13.8	52.1	50.0

Tab. 4 Results of tensile tests

Sample	L_0 [mm]	S_0 [mm^2]	$Rp_{0,2}$ [MPa]	Rm [MPa]	A5 [%]	Z [%]
2	50.0	68.2	1185	1489	2.26	-
4	50.0	52.1	1283	1340	3.60	33.74
ø	50.00	-	1234	1414.5	2.93	33.74
±	0.00	-	49	74.5	0.67	-
Desired values	-	-	900 - 1150	-	-	min. 20

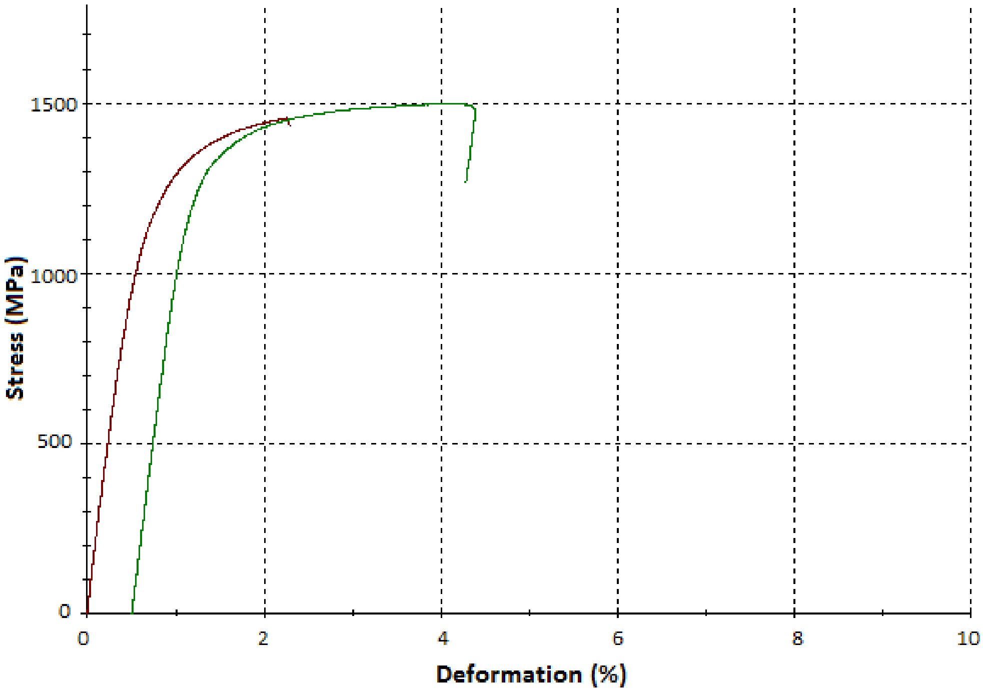


Fig. 7 Record of the tensile test

Tab. 5 Sample dimensions for the bend impact test

Sample	a_0 [mm]	b_0 [mm]	L [mm]	$a_0 - v_{notch}$ [mm]	Notch angle [°]
1	9.98	10.0	55	7.50	45
2	9.97	10.0	55	7.50	45
3	10.0	10.0	55	7.47	45
4	10.0	9.96	55	7.46	45

Tab. 6 Results of Charpy impact tests

Sample	Parameters				
	F_{max} [N]	S_m [mm]	W_m [J]	W_t [J]	ak [J/cm^2]
1	30116.7	1.17	18.80	27.93	37.3
2	30103.7	1.11	19.12	27.63	36.9
3	28805.3	1.08	14.19	21.34	28.6
4	28193.1	0.93	13.86	19.68	26.3

F_{max} - the maximum measured value of power; S_m - size deflection at maximum force;
W_m - the work done to attain maximum power;W_t - total impact energy minus the friction;
ak - the work done to attain maximum power.

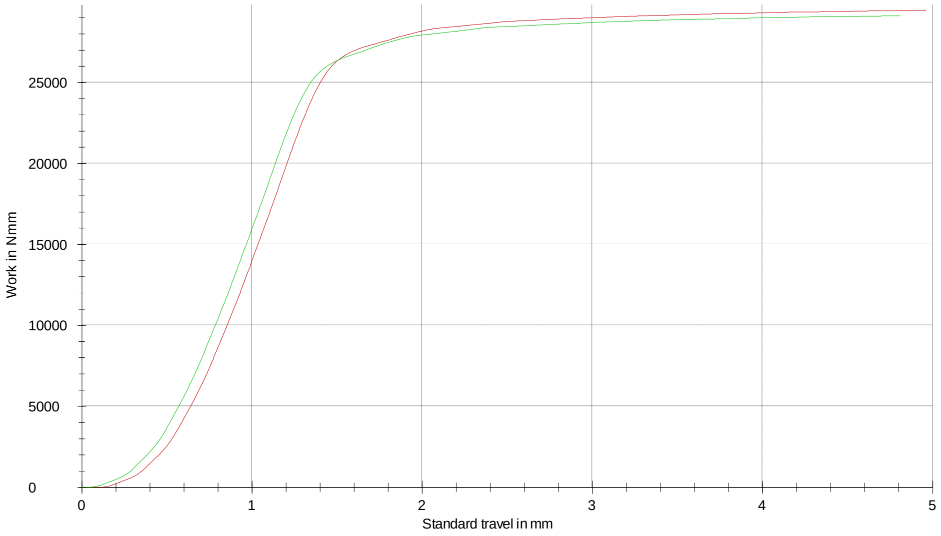


Fig. 8 Record of the bend impact test – work standard track depandence

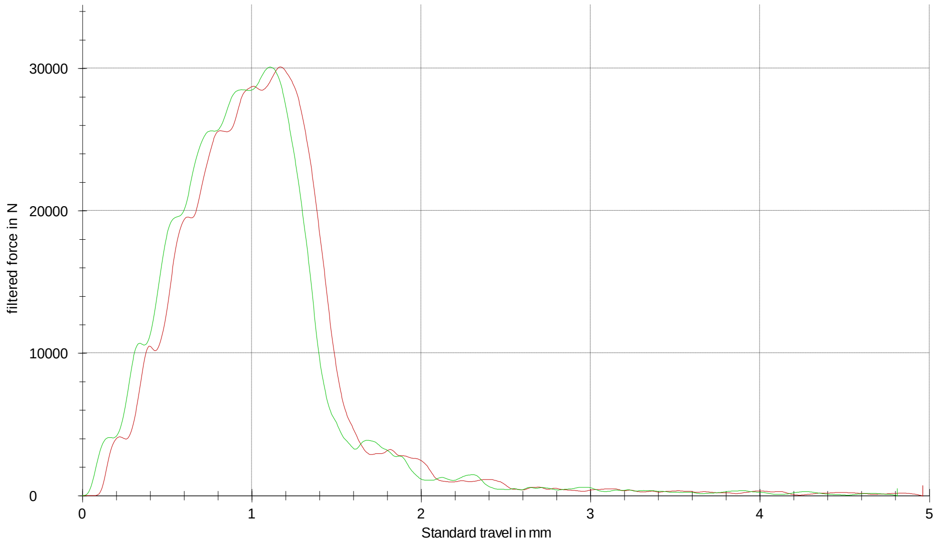


Fig. 9 Record of the bend impact test – filtered power-standard track dependence

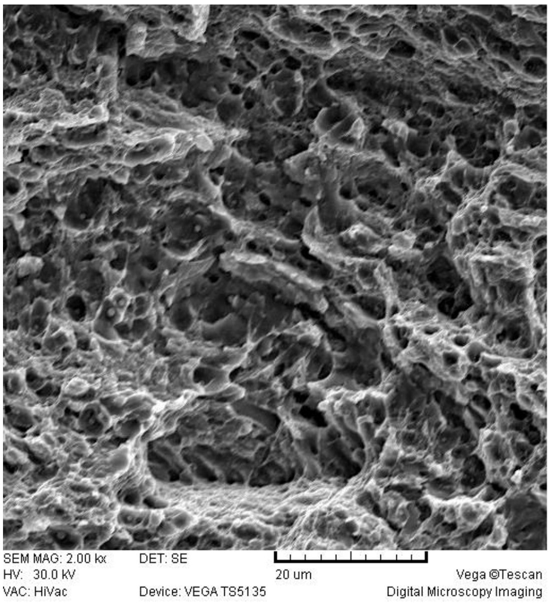


Fig. 10 Sample No. 1

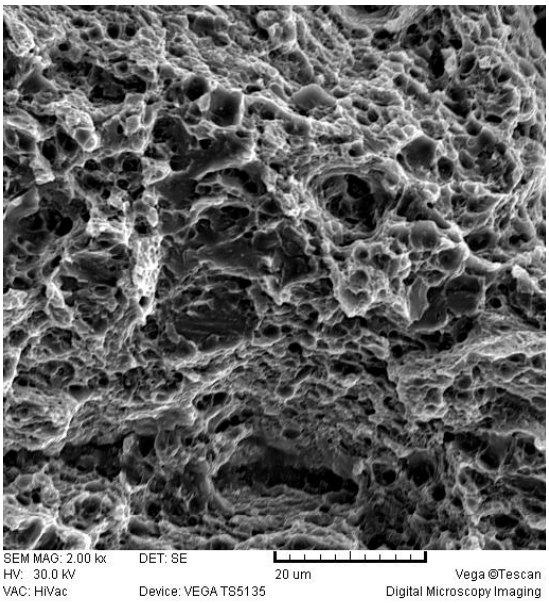


Fig. 11 Sample No. 2

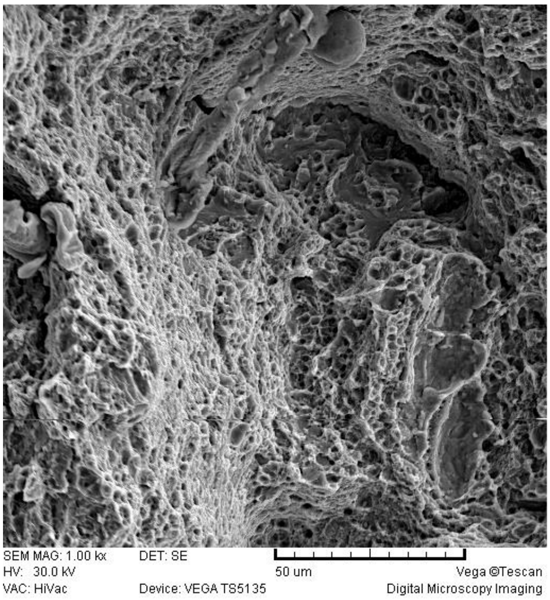


Fig. 12 Sample No. 3

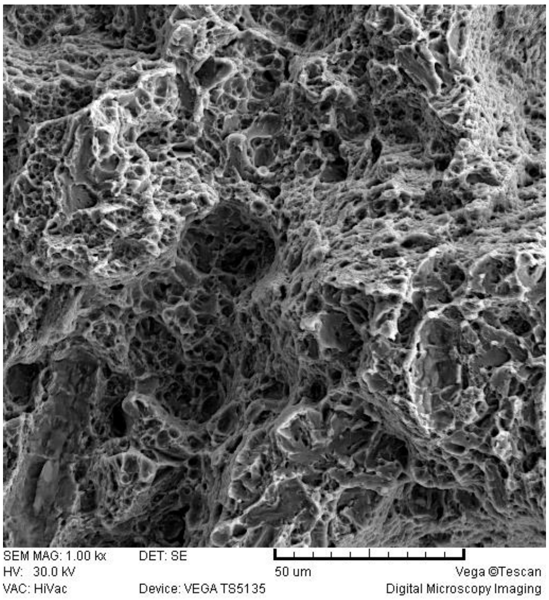


Fig. 13 Sample No. 4

4.3 Hardness test

The hardness testing was performed according to the Vickers method HV_{30}. Final metallographic analysis was complemented by hardness testing of the specimens used for the bending impact test. The surface hardnes was determined as a average value of three measurements on each of prepared samples and deremined as HV = 476 ± 12.

5 CONCLUSION

The chemical compositon evaluation confirmed that the analyzed main tank gun steel is close to the CSN 4216540 steel. The microstructure of analyzed steel was in general classified by high purity Level with small amount of inclusions of enormous size according to ISO 4967 standard. The microstructure was homogeneous, consisting of low-temeperature tempered martensite. The fractured surfaces of the available samples were heavily corroded and therefore unusable for fracture analysis.

The evaluated fracture surfaces of the samples after impact bending test showed that the breaking occurred as half developed cup-and-cone fracture, caused by thermal treatment process to achieve higher values of mechanical characteristics, which generally causes the toughness decreasing.

Fracturesurfaces were very inhomogeneous, which is associated to the line microstructure as a result of manifacturing and to the locally exclusion occurrance. Mechanical characteristics, contraction and hardness meet the artillery barrels requirements, but these characteristics were over the upper limit of the recommended range, which can cause toughness decreasing, but it is unlikely that this was the reason of the main tank gun destruction.

Acknowledgement

The paper was prepared with the support of the Project for the Development of the Organization of the Department of Mechanical Engineering, UoD "Promoting Education and Science in the Field of Engineering" and the specific research project of the Department of Mechanical Engineering FoMT 2012 "The Application of Modern Technologies for Components of Special Equipment".

References

[1] ISO 4967: 2003 (420471) *Ocel – Stanovení obsahu nekovových vměstků – Mikrografická metody využívající normovaná zobrazení (Steel – Determination of Content of Non-metallic Inclusions – Micrographic Method Using Standard Diagrams*). International Organization for Standardization, 2003.

[2] EN ISO 6507-1 (420374): 2006 *Kovové materiály – Zkouška tvrdosti podle Vickerse (Metallic Materials – Vickers Hardness Test).* International Organization for Standardization, 2006.

[3] KUSMIČ, D., HRUBÝ, V.: Corrosion resistence of plasma nitrided structural steels and modern methods of testing. In *Advances in Military Technology*. Volume 3, Issue 1. Brno : Univerzity of Defence in Brno, 2008. p. 65–77. ISSN 1802-2308.

[4] KUSMIČ, D., JULIŠ, M., ŠMÍD, M., PRŮŠA, S., POSPÍŠILOVÁ, S., OBRTLÍK, K., PODRÁBSKÝ, T.: Surface relief observation in fatigued cast superalloy inconel738lc using CSLM, SEM-FEG, and AFM. In *International Conference on Military Technology ICMT'11*. Brno : University of Defence Brno in collaboration with Oprox a.s., Brno, Czech Republic, 2011. p. 1493-1500. ISBN 978-80-7231-787-5.

[5] EN 10002-1 (420310): 2003 *Kovové materiály – Zkoušení tahem – Část 1: Zkušební metoda za okolní teploty (Metallic Materials – Tensile Testing - Part 1: Method of Test at Ambient Temperature)*. International Organization for Standardization, 2003.

[6] EN ISO 14556 (420380): Ocel – Zkouška rázem v ohybu na kyvadlovém kladivu tyčí Charpy s V-vrubem – Instrumentovaná zkušební metoda (Steel - Charpy V-notch Pendulum Impact Test – Instrumented Test Method). International Organization for Standardization, 2001.

[7] ČSN EN 10045-1 (420381): Kovové materiály - Zkouška rázem v ohybu podle Charpyho - Část 1: Zkušební metoda /V a U vruby/. Praha: Český normalizační institut, 1998. (Steel - Charpy V-notch and U-notch Pendulum Impact Test – Part 1: Test Method). Czech Institute for Standardization, 1998.

[8] HRUBÝ, V., KUSMIČ, D.: Analysis of pistol projectiles made by powder metalurgy technology. In *VTPS 2005*: *Zborník z 11. medzinárodnej konferencie konanej v dňoch 29. – 30. novembra 2005 v Liptovskom Mikuláši.* Liptovký Mikuláš : Akadémia ozbrojených síl, 2005. p. 30 – 38. ISBN: 80-8040-275-2.

Eng. David KUSMIČ, Ph.D.
Eng. Zbyněk STUDENÝ, Ph.D.
Prof. Eng. Vojtěch HRUBÝ, CSc.
Assoc. Prof. Eng. Emil SVOBODA, CSc.
University of Defence in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: david.kusmic@unob.cz
zbynek.studeny@unob.cz
vojtech.hruby@unob.cz
emil.svoboda@unob.cz

MODELLING OF TASK FORCE STRUCTURES

Vlastimil MALÝ, Petr HRŮZA

Abstract: This article describes a new approach to the planning process and new possible way of selection forces for international operations based on modular structures and units' capabilities required for particular operation. Modularity of military units' structure contributes to the thoughtful and purposeful utilization of operational capabilities, with regard to the nature of the environment where units are deployed. Interests and ambitions of the Czech Republic do not exclude participation of the Armed Forces across the full spectrum of military operations, yet their involvement in ensuring the joint commitments is expected especially in stabilization and peace support operations. The article describes the options of original software application developed during the "STRUCTURE" project solution aiming as a support for staff officers in the preparatory phase of operational planning.

Keywords: Module. Modularity. Modular Structures. Task Forces. Operational Planning Process. Decision-making Process. Software. Database. Access. Microsoft Visual Studio. C# language.

1 INTRODUCTION

The changing security environment with new emerging threats determines new requirements for the Armed Forces and their operational use. Modularity within NATO, EU or UN is not fully implemented. Application of modularity at the national level may be beneficial in the development of national contributions to the operations led by NATO, the EU or the UN.

The process of creating organizational structures of task forces to NATO-led operations (EU, UN) or ad hoc coalitions is affected by many factors having at national level a significant impact on the content and timing of the actual process of creating a multinational task force.

The primary step for the development and implementation of modular organizational structures is modules definition and description of the sort of modularity, methods and associated metrics as a basis for the introduction and use of a modular approach to developing organizational structures and the creation of task forces based on modularity.

The basic philosophy of the possible use of modularity within the Army of the Czech Republic in military operations is the ability to work in different types of operations and their scope, content and urgency are and will be very diverse.

The organizational structure of deployed Army units, number of people, weapon systems and other equipment or materials must be adapted to this wide range of applications.

The task forces composed of modules that will determine the capabilities and abilities will be created for tasks completion.

Modules and their capabilities are therefore essential for the creation of organizational structures of assigned task forces.

1.1 Initial documents for the creation of task forces

Organizational structure creating and capability assessment of task forces for the operation is an essential part of military planning process in the Czech Army during the preparation and deployment of forces and other army means into the operation.

The process of development and evaluation can be specified in different ways. Organizational structure creating and capability assessment are based on current requirements for assessment of key operational capabilities defined on the basis of the document "Declaration of Defense Capabilities - Towards NATO Forces in 2020".

As the baseline document that describes the desired operational capabilities of the typical units within NATO and the EU can be considered existing NATO Capability Codes/Statements, referred to as Annex 1 to document Defence Planning Capability Survey 2010, AC/281-N(2010)0014-FINAL (EWG(R)) issued on Feb 26, 2010. This document sets out the requirements for operational capabilities by the EU, as specified in Annex 2 of the EU Capability Codes.

An updated version of the capability requirements on units for multinational operations led by NATO are defined in the document Bi-SC Agreed Capability Codes and Capability Statements, SHAPE/CPPCAMFCR/JM/281143, issued on Oct 14, 2011. This document has been made in cooperation of specialized military authorities, both from NATO and the EU. Specified requirements on the ability of units are applicable for planning processes both in NATO, and the EU. These requirements express minimum set of capabilities, which must be included in a military component to fulfil the tasks assigned to the required extent, quality and highest efficiency.

1.2 Process of creating task forces within NATO

Creation of forces within NATO is initiated in Phase 4 of the Operational planning process – the concept of operations processing (Concept of Operations – CONOPS). It is processed at this stage so-called "Provisional Combined Joint Statement of Requirements" (P CJSOR) as a document that expresses the minimum requirements for military forces created to perform the operation with potential risks accepted. P CJSOR is processed by the planning team at the headquarters for operations (Allied Command for Operations - ACO) in coordination with the designated operational headquarters (JFC HQ). The created document is sent to the individual nations through national military representatives in SHAPE as information about the possibility to start of the planning process at the national level on the possible involvement of national military capacity in operations led by NATO (EU).

Particular selection and creation of forces for operations is the responsibility of the SACEUR in cooperation with the NATO Member States, or other non-member states, which may be also involved into the planning and execution of operations, including subordinate headquarters within NATO.

The aim of this selection process and creation of forces is to identify and confirm the national contributions to the operation with the requirements to create sufficient capacity in accordance with the requirements for the mission execution. Part of this process is the potential risks assessment on the basis of national restrictions defined by individual states.

The entire process is completed after the approval of the OPLAN and by release of order to perform the operation (NAC Executive Directive – NED), empowered by the Supreme Commander of Allied Forces in Europe (SACEUR) to perform the operation, forces activation and their acceptance into their subordination (Transfer of Authority - TOA).

2 SOFTWARE FOR TASK FORCE CREATION

The modular system is a system composed of individual modules. The system consists of the gradual integration of functional modules into the system according to specific operational requirements. The functionality of the system is based on variable number of modules. Term module and term modular system are very versatile and both are used almost in all disciplines and various branches, not only in military sphere.

The combination of modules (military units) at the national level and the creation of appropriate structures of the national task force for the operation must establish for operational commanders of multinational task groups sufficient basis for efficient use of task force manpower and other necessary resources.

Sophisticated interaction and combination of individual task force modules creates preconditions for efficient and effective response to various situations emerging within the operation goals performance process.

Task Force Commanders are able to flexibly change the battle group units' disposition to respond to the new challenges and requirements according to the current operations conditions and situation development, if necessary. The modular structure allows the task force commanders capability of extraordinary agility and ability to react to situations.

The aim of task forces creation is to create organizational structures of units, consisting of individual modules, capable to meet all operational requirements, which will be easy to combine.

The Czech Army provides units having the required capabilities, appropriate size, professional structure and personnel.

The created task forces should be able to conduct the required activities within the entire spectrum of tactical operations from crisis situation eliminating up to the combat operations performing.

2.1 Module definition

For the purpose of practical operational procedure we have defined the basic modules that are assembled into sets in order to create a modular system designed to meet the specific tasks of the operation.

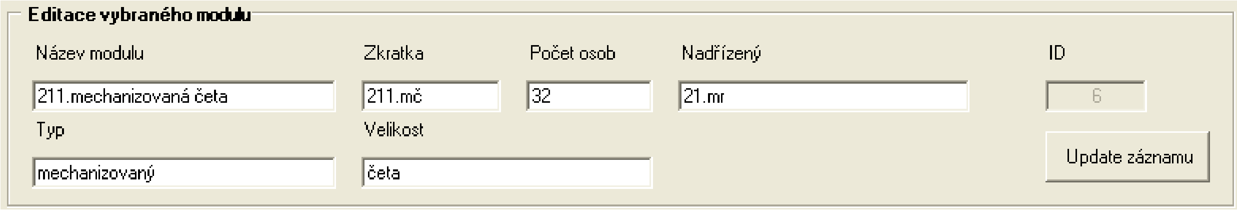
We have defined new definition of term "module" (one of the result of "Structure" project). The definition is as follows:

"*Module is the basic building element (entity, organizational structure), from which is formed the structure of the common national or multinational task force in terms and conditions of specific operation. The module is designed to meet the professional task (tasks) or to meet the required capabilities (skills) alone or in mutual interaction with other modules."* [1, page 9]

Modules are the basic building block of the new introduced software application. Every module is described by the module name, abbreviation (e.g. MPR.), the number of people, by choosing of superior module type (e.g. mechanized), and size (e.g. battalion). It is necessary for each module to set its availability (in defined time slots) and capabilities. The time availability is specified in our software for each month for each module, and we distinguish among 4 possible values:

- period of preparation to operation/mission,
- period of deployment in operation/mission,
- period of stabilization after returning from the last operation/mission,
- non-deployable module.

The user of the application (software) has to assign capabilities for each module from prearranged database containing all possible capabilities. The user can set percentage of level for each selected capability for each military unit (module).



Editace vybraného modulu

Název modulu: 211.mechanizovaná četa

Zkratka: 211.mč

Počet osob: 32

Nadřízený: 21.mr

ID: 6

Typ: mechanizovaný

Velikost: četa

Fig. 5 Part of application form enabling editing of selected module

2.2 Capabilities definition

Detailed identification of required operational capabilities for successful task completion is the primary basis for all process due to the complexity and expected changes during contemporary operations execution. It must be taken in the account in the formation phase of particular task force organizational structure at the national level for operation. Main goal is to meet the challenges in the entire spectrum of tactical operations during future operations (deployment, mission).

Then, assessment and detailed evaluation of (required) operational capabilities can be performed in the following areas:

- Doctrine, - Organisation;
- Training, - Materiel;
- Leadership, - Personnel;
- Facilities and - Interoperability;

well known as abbreviation: DOTMLPFI.

Particular capabilities requirements for a specific operation determine the size, structure and forces composition that will vary for each operation. Task force creation is very important and challenging process based on combination of modules depending on the required capabilities, operational goals, operational task, geographic space, time manner, etc.

Developed application described in this article provides users (operation planners) complete list of possible capabilities taken from the NATO document BI-SCD 80-90 NATO Tasks List.

2.3 Software for task force creation

Software application called "Creation of Modular Task Force Structure" is intended for creation of task force using modular approach for the whole spectrum of operations. The aim of task forces creation is to create organizational structure of units, consisting of individual modules capable to meet declared operational requirements.

The main software output (benefit) is easy task force creation for the selected (predefined) operation. Task forces are created for each individual unit rotation during all time of one operation.

Basic database used in this software application consists of the following data-tables:

- Scenarios;
- Operations;
- Capabilities and
- Modules.

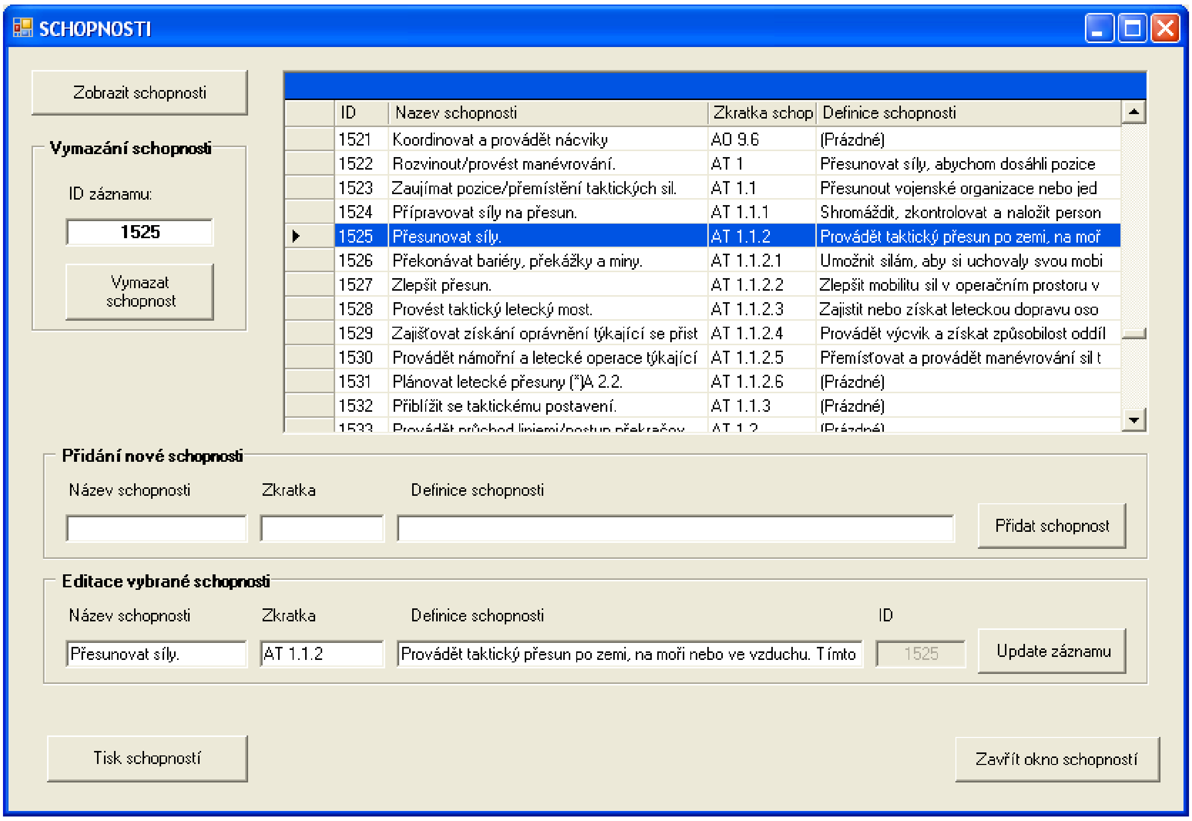
All database parts (data-tables) should be kept up to date to obtain objective and correct results.

The application is based on data stored in relational database. This database consists of individual database tables connected with relations within a particular relational data model. Database is stored in Microsoft Access database format and the application was written in Microsoft Visual Studio development environment using .Net Framework and C# language. Used data model and all the most important links between database tables used in our solution are shown in the Fig. 3.

Application user can perform all standard database operations as insert, edit and delete of all entries in each of used data tables in our data model. The basic input data for our application are scenarios, operations, capabilities and modules. We can see also several other tables making links between data-tables in the scheme (Fig. 3.) that are necessary for relational data model philosophy and operation.

The creation of a task force can be made after filling of at least one operation, filling a number of modules, assigning them a few capabilities and adding the availability of modules in the desired period of operation. These are the necessary presumptions before making a successful selection of modules for desired operation (and particular rotation).

Application allows us to print all partial results, list of modules for final selection for the task force, and all data from the database (data tables). User of application can print also lists of scenarios, operations, capabilities, modules and - as a main result - created task force. All prints are available also in Adobe Acrobat format (pdf file).



ID záznamu: 1525

	ID	Nazev schopnosti	Zkratka schop	Definice schopnosti
	1521	Koordinovat a provádět nácviky	AO 9.6	(Prázdné)
	1522	Rozvinout/provést manévrování.	AT 1	Přesunovat síly, abychom dosáhli pozice
	1523	Zaujímat pozice/přemístění taktických sil.	AT 1.1	Přesunout vojenské organizace nebo jed
	1524	Připravovat síly na přesun.	AT 1.1.1	Shromáždit, zkontrolovat a naložit person
▶	1525	Přesunovat síly.	AT 1.1.2	Provádět taktický přesun po zemi, na moř
	1526	Překonávat bariéry, překážky a miny.	AT 1.1.2.1	Umožnit silám, aby si uchovaly svou mobi
	1527	Zlepšit přesun.	AT 1.1.2.2	Zlepšit mobilitu sil v operačním prostoru v
	1528	Provést taktický letecký most.	AT 1.1.2.3	Zajistit nebo získat leteckou dopravu oso
	1529	Zajišťovat získání oprávnění týkající se přist	AT 1.1.2.4	Provádět výcvik a získat způsobilost oddíl
	1530	Provádět námořní a letecké operace týkající	AT 1.1.2.5	Přemísťovat a provádět manévrování sil t
	1531	Plánovat letecké přesuny (*)A 2.2.	AT 1.1.2.6	(Prázdné)
	1532	Přiblížit se taktickému postavení.	AT 1.1.3	(Prázdné)
	1533	Provádět průchod liniemi/postup překračov	AT 1.2	(Prázdné)

Editace vybrané schopnosti

Název schopnosti	Zkratka	Definice schopnosti	ID
Přesunovat síly.	AT 1.1.2	Provádět taktický přesun po zemi, na moři nebo ve vzduchu. Tímto	1525

Fig. 6 Basic application form for capabilities management

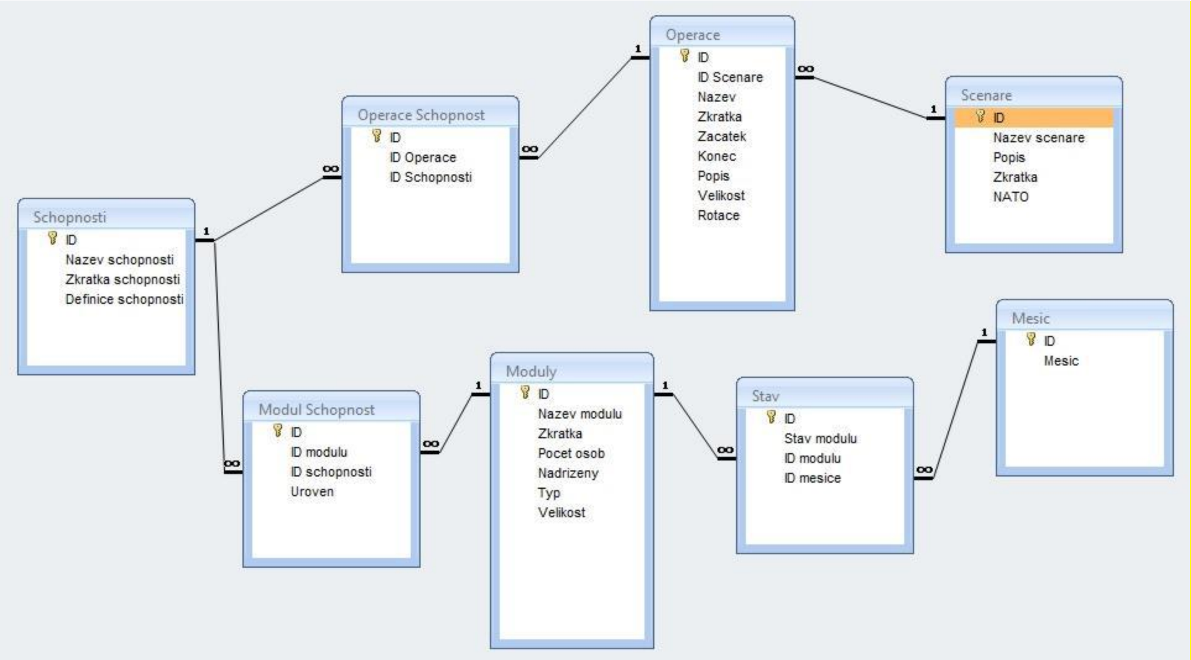


Fig. 7 Relational data model of used database (scheme taken from MS Access environment)

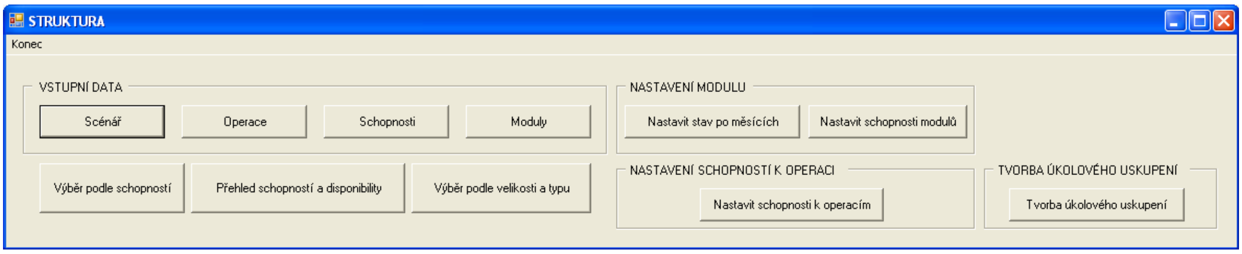

STRUKTURA
Konec
VSTUPNÍ DATA
Scénář
Operace
Schopnosti
Moduly
NASTAVENÍ MODULU
Nastavit stav po měsících
Nastavit schopnosti modulů
Výběr podle schopností
Přehled schopností a disponibility
Výběr podle velikosti a typu
NASTAVENÍ SCHOPNOSTÍ K OPERACI
Nastavit schopnosti k operacím
TVORBA ÚKOLOVÉHO USKUPENÍ
Tvorba úkolového uskupení

Fig. 8 Basic form (Main Screen) of the described software application

References

[1] DUBEC, R., HRŮZA, P., SPIŠÁK, J., ČERNÝ, J.: *Tvorba modulárních struktur úkolových uskupení.* Praha : Powerprint s. r. o., 2012. 82 s. ISBN 978-80-87415-54-2.

[2] “STRUCTURE”, Final Report of Defence Research Project. Brno : MoD CZE, 2009-2012.

[3] HRŮZA, P.: Generation of modular structures for operations. In *New Challenges in the Field of Military Scien 2010.* 7th International Scientific Conference. Budapest, Hungary : Bolyai Janos Military Foundation, 2010. ISBN 978-963-87706-6-0.

[4] HRŮZA, P., ČERNÝ, J.: Generation of the modular task forces structures. In *The 16th International Conference - The Knowledge-Based Organization - Management and Military Sciences*. Sibiu, Romania : Nicolae Bălcescu Land Forces Academy Publishing House, 2010. p. 44-47. ISSN 1843-6822.

[5] MALÝ, V., HRŮZA, P.: Modelling of Task Force Structures. In *Communication and Information Technologies.* 7th International Scientific Conference, Tatranské Zruby. Liptovský Mikuláš : AFCEA Slovak Chapter and Armed Forces Academy of general M. R. Štefánik, 2013. ISBN 978-80-8040-464-2.

Col. Assoc. Prof. Eng. Vlastimil MALÝ, CSc.
Lt. Col. Eng. Petr HRŮZA, Ph.D.
University of Defence
Kounicova str. 65
662 10 Brno
Czech Republic
E-mail: vlastimil.maly@unob.cz
petr.hruza@unob.cz

COMMON OPERATIONAL PICTURE AND A PROBABILISTIC MODEL FOR RECOGNITION IDENTIFICATION FRIENDLY OR FOE – IFF

Radoslav MASNICA, Jozef ŠTULRAJTER, Ivan PLICHTA

Abstract: When obtaining information from sensors and sources, a commander is seeking for information that is of value. Quality of information thus affects the decision of the commander. This article aims to describe a probabilistic model of knowledge on the battlefield and Identification Friendly or Foe – IFF and current overview of the situation for the commander and offers an introduction to the understanding of the relationship between information and their impact on the results of the fight. Such a model is used in other procedures to describe the relative information domination.

Keywords: Information domination. Identification Friendly or Foe – IFF. Common Operational Picture – COP. Command and Control System - C2. Sensors.

1 COMMON OPERATIONAL PICTURE - COP AND RECOGNITION ON THE BATTLEFIELD IDENTIFICATION FRIENDLY OR FOE – (IFF)

In the transformation of the army in the Information Age army needs to conduct combat operations in addition to weapons, information, and analytical tools to streamline the chain of command in combat operations. This concerns in particular the knowledge systems of combat situations and sensors and instruments to analyze the information.

This article aims to describe the probabilistic model of knowledge on the battlefield - recognition application Identification Friendly or Foe – IFF and the current review of the situation for the commander and offers an introduction to the understanding of the relationship between information and their influence on the outcome of the fight.

Such a model is used in other procedures to describe the relative information domination. There are two key features, value and quality. Information has value if it informs the commander and thus contributes to the knowledge of the combat situation. Quality of information depends on the accuracy, timeliness, and completeness. It is clearly true that valuable information or knowledge is of high quality. Conversely, the quality of information may have little or no value and thus may even detract from the knowledge of the real situation.

When obtaining information from sensors and sources, the commander requests and collects information to the maximum values for its decision. The problem is that it is rarely possible to accurately assess the quality of information received. Consequently, it must generally be assumed that a portion of what "he know" may be inaccurate. The quality and completeness of information thus affect the decision of the commander.

2 KNOWLEDGE OF THE BATTLEFIELD - COP

In the battlespace of operations, reconnaissance is at least as important as the maneuver and effective use of firepower. Units in the space of operations are ready for defensive or offensive operations. Of course, adversary actively seeks to achieve its objectives. Knowledge of the situation on the battlefield - Common Operational Picture (COP), recognizing units with application Identification Friendly or Foe – IFF is therefore an understanding of the intentions of the enemy. Understanding of the situation, of course, depends on the knowledge and experience of the commander.

The intention of the adversary can be learned directly from sources and sensors, or can be derived from knowledge of the opponent's forces, which the commander has.

3 PROBABILISTIC MODEL

Although knowledge is multidimensional, for the purpose of this model, to simplify the description, Assume that the only element of informations are data from its own sensors. Sensors gather information about the location of opponent's objectives and their recognizing with aplication and identification friendly or foe (IFF).

Example: Assume that COP is composed only of the location of the target (or critical subset of them, such as. location of the vehicle). Assume that the commander has intelligence information from sensors that indicate location of 5 targets (buildings, vehicles, etc.) in the area of operations. The commander wants to find out whether the objectives are own or foreign.

Let thus U be the number of targets located nearby of the sensors of the commander,

$$U \in \{0,1,2,\dots n\}.$$

We assume that U is a random variable and

$$P(U = u), \tag{1}$$

is the probability of detection of exactly u targets from n targets within its range.

The initial probability distribution of U depends on the information available to the commander from his sensors and sources. When first started, the information available from the reconnaissance is processed. In the worst case, the commander does not have any information regarding the location of the opponent's units available, and therefore we will refer to the situation that:

$$P(U = u) = \frac{1}{n+1}, \text{pre} \quad \mu \in \{0,1,\ldots n\}. \qquad (2)$$

This means that it is equally likely that any number of opponent's goals, up to n, is in its range.

After receiving the identification and reporting of the sensors, the probability distribution changes. Ideally, the final allocation of a probability

$$1, pre\ U = \mu\ a\ 0, pre\ U \neq \mu,$$

where μ is the number of units within the range of the sensor.

However, in reality, the location of some of the objectives will not be known with certainty at the time of the decision commander.

Probability distribution $P(U = u)$ can be influenced by several factors:

1. Number of confirmed reports from sensors: Distribution of probability $P(U = u)$ tends to concentrate all probability $P(U = u)$ for a fixed number of units within range u_f, it means:

   $$P(U = u_f) -> 1\ and\ P(U \neq u_f) -> 0.$$

2. Number of unconfirmed reports from sensors: Unconfirmed reports from sensors increase uncertainty.

   Impact on $P(U = u)$ is such that the probability distribution tends to "flatten", in the worst case to such that:

   $$P(U = u) = 1/(n + 1).$$

3. Reliability of sensors and sources: In some cases, the subjective assessment of the reliability, especially when assessing the results of visual observation. In the case of technical sensors their reliability varies with environmental conditions; unreliable messages are therefore ignored, resulting in the same effect on the value $P(U = u)$ as in the case of the second factor.

4. Terrain conditions: the outputs of sensors and sources that require direct line of sight could be heavily degraded by terrain conditions. The result is a reduction in the number of reports that is slowing down the convergence of probability $P(U = u)$.

5. Multiple confirmation: Confirmation of the aims from different types of sensors increases the reliability of the reported targets detection and therefore accelerates the convergence of the probability $P(U = u)$.

6. Time lag of information gathered: the lack of current reports decreases the probability $P(U = u)$ to maneuver the enemy.

4 EVALUATION REPORTS FROM SENSORS

The effect of factors suggest that we need to examine how to specify the probability distribution of U for sensors.

Therefore let $V \in \{0,1,2,\ldots n\}$, be another random variable which represents the number of detected targets within range of the sensor. Then:

$P(V = v)$ is the probability that the number of detected targets within range of the sensor is v. However, this number is subject to the number of goals μ within the range of the sensor. Therefore, we focus on $P(V = v | U = \mu)$ for $\mu \neq n$.

If we assume that the sensors are able to detect every target with probability q, then the conditional probability of the number of detected targets within the range of the sensor has a binomial distribution:

$$P(V = v|U = \mu) = b(v{:}\,\mu, q) = \\ = \binom{\mu}{v} q^{v}(1-q)^{\mu-v}, \text{for } v = 0,1,\ldots\ldots \mu. \qquad (3)$$

This view can be easily adapted to different levels of resolution.

At the lowest level, q is a composite probability representing the probability that all sensors can detect the target. At a higher level of resolution probability q_j determines the probability that the sensor **j** locates the target.

Furthermore, we assume that the commander must make a decision at a certain time and this limits the number of updates, reports from sensors, which can be used to refine the initial probability distribution. If we further assume that messages from the sensors are processed immediately, then the probability of finding targets within range

$$P(V = v\,|U = \mu), \text{for } v = \{0,1,\ldots n\} \qquad (4)$$

the i-th message from the sensor is then according to Bayes' formula [4]:

$$P_i = P(U = \mu|V = v) = \frac{P_{i-1}(U=\mu)b(v{:}\mu,q)}{\sum_{u=0}^{n} P_{i-1}(U=u)b(v{:}u,q)}, \qquad (5)$$

where the probability of messages from the i-th sensor is

$$P_{i-1}(U = \mu) = P_{i-1}\ (V = v|U = \mu).$$

In this formulation, the information from the sensor consists of a likelihood position of targets within range of sensors μ. This value therefore determines the value of the likelihood of detection targets (buildings, vehicles, tanks, etc.) in the application of identification IFF in the theater of operations.

4.1 Information - Entropy Model

After processing the information from each sensor varies the level of knowledge Commander such as a given in changes in the probability distribution.

$$P_i(U|V = v).$$

The actual amount of information can be measured using information entropy. Information entropy is a measure of the average amount of information in a probability distribution, and is defined as:

$$H[P_i(U|V = v)] = H_i(U|V = v) = -\sum_{u=0}^{n} P_i(U = u|V = v) \ln P[(U = u|V = v)] \tag{6}$$

The entropy function reaches its maximum, when the value of information in the probability distribution is the lowest (highest uncertainty). In practice, this occurs if the commander does not have any means to detect targets and has no prior information about the objectives in the area of the battlefield.

In this case, the finding of no objective applies:

$$P_0(U = u) = 1/(n + 1). \tag{7}$$

Then Entropy in this distribution is:

$$H_0(U) = \ln(n + 1). \tag{8}$$

Conversely, if the i-th sensor confirm with certainty the location μ units within range of the sensor, then the probability :

$$P_i(U = \mu|V = \mu) = 1 \quad and \quad P_i(U \neq \mu|V = \mu) = 0. \tag{9}$$

The processing of reports from n sensors is the entropy in the updated probability distribution given by:

$$H_0(U) = \ln(n + 1) - H_i(U|V = v) \tag{10}$$

The level of information can then be measured using standardized forms of entropy:

$$K_i(U|V = v) = \frac{\ln(n+1) - H_i(U|V=v)}{\ln(n+1)}. \tag{11}$$

5 USE IN COMBAT SYSTEMS

The procedure of determining the entropy and the probabilistic model, together with complexity theory are used to design a method to increase the level of information in COP and recognition targets on the battlefield with application identification (IFF) using new methods of network-oriented environment (Network Enabled Capability - NEC) [1].

For recognition of targets on the battlefield are used rangefinder (mLD) for determine distance to target and data transfer for identification (IFF) in communication channel in a network-oriented environment.

The described methodology is used in wiring complex personal combat system, which allows the evaluation of data from the exploratory system and laser rangefinder (mLD) with the methodology in the system of digital soldier systems (DSS) and its use in recognition targets in Command and Control (C2) systems and live simulation systems.

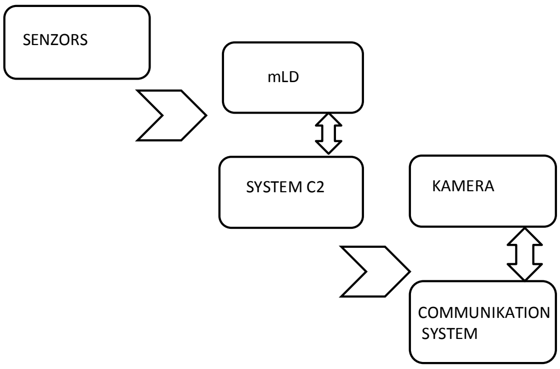


Fig. 1 Flow of information in wiring of complex personal combat system

In Figure 1 is shown the simplified block diagram as part of complex personnel combat system, which consists of (mLD) on the weapon, sensors and cameras connected with the C2 system with which information is transmitted in a communication system NEC [2].

On the basis of known data from the reconnaissance, target detection in the C2 system and firing elements, the involvement depicted in Fig. 1 allows better accuracy, elimination of striking own units and the use of a laser rangefinder (mLD) to ensure the transmission of information and training.

Involvement has application in the design of systems for digital soldier and small arms positioning systems and integration of combat systems for reconnaissance into digital soldier systems, equipped with sensors, radiation detectors and laser rangefinder, command and control C2, or controlled and uncontrolled missiles in conjunction with the system for digital soldier.

In a similar manner, it is solved the involvement of a complex vehicle combat system.

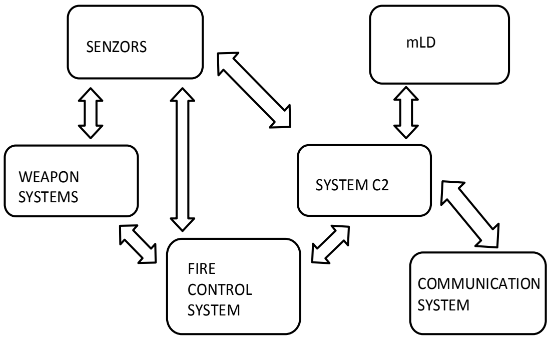


Fig. 2 Flow of information in wiring of complex vehicle combat system

Involvement in Fig 2 is formed from vehicle weapon systems, sensors, combat reconnaissance systems, command and control C2 systems, laser rangefinder (mLD) and communication system so that the system comprises a laser rangefinder to measure distance and data transmission laser interconnected system of C2 from laser data link receiver target, laser transmitter sector information and communication system to ensure acknowledgment objective data and links targeting system and fire control system for weapon platforms with C2 systems to ensure identification of goals and show identification friendly or foe – IFF. Involvement allows a parameter setting fire in fire control system, ensuring measuring coordinates focused on target focused objectives and identification friendly or foe – IFF. It also allows to ensure the transmission of identification and text data from the C2 system by laser, automated transfer of information to the goals of the radio network and also in a live simulation.

This technical solution allows increasing the level of value of information in COP and provides solutions for new recognition and identification friendly or foe – IFF in the network-oriented environment - NEC [3], which increases the accuracy, reliability information for further use and decision making.

Described technical solution proposals and involvement are part of patent applications PP-60-2013 and PA-61-2013 now pending at the ÚPV SR.

6 CONCLUSION

In the battle space of operations reconnaissance is as important as the maneuver and effective use of firepower. Quality of information depends on its accuracy, timeliness and completeness. Knowledge of the situation on the battlefield - Common Operational Picture (COP), recognizing of units with aplication and identification friendly or foe – IFF is therefore an understanding of the intentions of the enemy and adoption of effective measures and more decisions commander. When obtaining information from sensors and sources, commander requests and collects information that has value. Therefore, we focused on the description of knowledge of the situation on the battlefield using the traditional model of probability. Exploration and evaluation of information was then measured as a degree of uncertainty in probability distributions.

Probability distribution is adjusted by means of Bayesian method, which describes the processing of information from the sensors. This model may also be useful in quantifying information superiority and to build a model optimized to obtain information superiority, which will be a subject of further investigation and modeling.

References

[1] ALBERTS, D. S.: *Information Age Transformation: Getting to a 21st Century Military.* Washington, DC : CCRP , 2002.

[2] ALBERTS, D. S.: *Power to the Edge: Command and Control in the Information Age.* 2005. ISBN 1-893723-13-5.

[3] ALBERTS, D. S., GARSTKA, J. J., STEIN, F. P.: *Network centric warfare: developing and leveraging information superiority.* 2000. ISBN 1-57906-019-6.

[4] MOFFAT, J.: *Complexity Theory and Network Centric Warfare*. 2003. ISBN 1-893723-11-9.

[5] PERRY, W., MOFFAT, J.: *Measuring the Effects of Knowledge in Military Campaigns.* 1997. Jpl Res. Soc 48. pp. 965-972.

Eng. Radoslav MASNICA
Eng. Ivan PLICHTA, CSc.
CSBC Company Ltd.
Roľnícka 10
831 07 Bratislava
Slovak republic
E-mail: masnicar@csbc.sk
csbc@csbc.sk

Prof. Eng. Jozef ŠTULRAJTER, CSc.
Armed Forces Academy of general M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak republic
E-mail: jozef.stulrajter@aos.sk

THROUGH ECOLOGICAL RISK ASSESSMENT

Sergiy OREL, Oleksiy IVASCHENKO

Abstracts: The question of management by ecological safety of troops through assessment of ecological risk is considered in the article. As the model of risk assessment was used scheme, proposed by the United States Agency of Environmental Protection (USEPA). The main constituents of scheme are considered, applicable to ecological safety of troops. The example of ecological risk assessment for a military range is resulted.

Keywords: Ecological safety. Ecological risk. The Armed Forces. Risk assessment. Military activity. Human health. Biota.

1 INTRODUCTION

The aim of providing the environmental safety of the troops is to address two interrelated objectives: protection of personnel, equipment and weapons from hazards of the environment and protection of the environment from possible harmful effects of military activities [1]. Achieving goals requires appropriate management decisions. To take right decisions it is desirable to have criteria - some indicators of environmental conditions that characterize danger to people as well as to biota. A convenient criterion in this regard is an environmental risk - "the probability of damage to human life or health, the environment, life or health of animals and plants considering the severity of damage" [2]. The analysis of ecological risks is an effective tool that integrates environmental data with control solutions [3]. The risk analysis consists of three stages: assessment, management, and risk communication, herein the stage of the risk assessment is the most important.

2 REVIEW OF MODEL

There are various models of the environmental risk assessment [4], below we will use the scheme proposed by the United States Agency of Environmental Protection (USEPA) [5]. According to this scheme the ecological risk assessment is carried out in three stages:

1. *The formulation of the problem.* The main components of this stage are:

a) The determination of the objective of the risk assessment. The purpose of the assessment should fit the purpose of the risk management, so if the purpose of the management is to protect life and health of people and/or other valuable species, which are in the exercise of military activities, the assessment is to contain information about the risks that are specific to these species in this exact area in a manner acceptable to the people who make decisions: commanders in charge of decision-making to ensure the protection, representatives of superior headquarters, who are responsible for the military operations, members of the public and local authorities, if a military activity affects their interests, representatives of the environmental bodies, etc.;

b) The review of expected activities (took place or are taking place);

c) The description of the area. The territory of the expected or carried out military operations is described. Special attention is paid to sights of cultural and historical heritage, places of rare, endangered, and valuable species of flora and fauna;

d) The determination of the spatial and temporal zones. The latitude of assessment depends on what area and time period are the subjects of assessment. The time period determines possible harmful effects of environmental parameters (stressors) on people and biota (receptors). Short-term actions last for about 0.5 – 1.0 hour and cause a severe reaction. It is considered that a short-term action occurs either once or over time, so that a human body or biota have time to recover from the previous action. Long-term actions of stressors attend chronic diseases. Long-term actions are those which last for more than 12 % of lifetime of a living organism [6];

e) The selection of concerning objects. The choice is to identify the people and objects of the environment that are sufficiently sensitive to the military activities. The selection criteria for biota are the following [5,7]: 1) the importance of environmental protection in terms of public policy, 2) the importance in terms of maintaining the ecosystem of the region, in the area of a military activity action; 3) the sensitivity to military activities; 4) the importance in terms of preserving the environment for a future conduct of military activities, and 5) the importance to preserve the cultural and historical heritage;

f) The construction of a conceptual model. The model reflects the hypothesis that describes effects that may occur in the environment as a result of military activities, summarizes the results of the problem formulation phase and establishes cause and effect relationships. The strategy of the model structure consists of the following components [7]: 1) the determination of the influence mechanism of military activities on the environment, that presents it as a cascade process, the conditions of the environmental components caused by these processes and the processes which are a result of these conditions; 2) the determination of the environmental objects that are affected by military activities; 3) the relationship between a stressor exposure and an environmental object (receptor) response to it.

2. *The analysis of exposure and corresponding environmental effects*. An exposure (action) is a contact of an organism (receptor) with chemical, physical or biological agents (stressors). The characteristic (assessment) of the exposure is a risk assessment stage, during it the quantitative income of the stressor in a human body or biota in various ways (inhalation, oral, dermal) as a result of the contact with different objects of the environment (air, water, soil, food) is established. The exposure assessment implies measuring or determining the (qualitative and quantitative) frequency, the duration and ways of the stressor action in the environment on the receptor.

The most important steps in the exposure assessing are the following:

- determining the routes of the stressor action;
- identification of the environment of the distributed stressor;
- quantitative characteristic of the stressor (e.g., concentration);
- determining the time, frequency and the duration of the stressor;
- identification of the receptor that is exposed to the stressor.

Quantifying the magnitude of the exposure, which lasts for a period of time, the total exposure must be divided by the time interval interesting for a researcher. Thus, the obtained value is the average of the exposure per unit of time. Of course, the average exposure is also expressed as a function of the body weight and is determined using the equation

$$I = \frac{C \cdot CR \cdot EF \cdot ED}{BW \cdot AT} . \qquad (1)$$

For instance, if the stressor is a chemical, then:

I – the average exposure mg·kg^{-1} body weight per day;

C – the average concentration that affects a human or biota for a period of the exposure (e.g., mg ·liter^{-1} of water);

CR – the value of the contact, the amount of the polluted environment that is in contact with a body of a human or biota per unit time or per case action (e.g. liter·day^{-1});

EF – the action frequency, the number of days per year;

ED – the action duration, the number of years;

BW – the body weight, the average body weight for a period of the exposure, kg;

AT – the average time, the averaging period of the exposure, the number of days.

The action of the stressor on the receptor causes a reaction of its organism. The assessment of the dependence "dose - response " is a process of the quantitative characteristic of toxicological information and establishing a connection between the dose of the stressor that affects the body of the receptor, and cases of harmful effects in the exposed population. The analysis of the dependence "dose - response" implies the establishing of causal conditionality of the growth of harmful effects when exposed to this stressor, identifying a maximum dose that causes no reaction and a minimal dose that causes the development of an effect response, and also determining the intensity of the effect growth at increasing a dose. The value of the maximum dose, that causes no response, forms a very important concept of ***"reference dose (RfD)"***, i.e. the value that characterizes a daily stressor effect throughout the life of the receptor and is not likely to cause an unacceptable risk to the health of its sensitive groups.

In the assessment of the stressor action on a human body the international risk assessment methodology [2] suggests that:

- Carcinogenic effects, when exposed to carcinogens that have a genotoxic effect, may occur at any dose that causes damage initiation to the genetic material;
- The existence of threshold levels, below which harmful effects do not occur, is expected for non-carcinogenic substances and carcinogens with a non-genotoxic mechanism of an action.

In the assessing the effect of the stressor on biota organisms, especially in screening studies, only the existence of threshold levels is expected [3]. Herein, talking about the protection of the receptor implies the parameters of the environment, which ensure the survival, growth and reproduction of the population. In this case, the maximum value that causes no response is the value, called "***toxicity reference value* (*TRV)***". The value of *TRV* depends on the type of the stressor, a type of the receptor and, obviously, on a place of the interaction between the stressor and receptor, i.e. the physical and chemical properties of the environment. Depending on the calculation and use of *TRV*, they are divided into three types [8]:

- A reference dose (RfD) is usually determined in mg·[kg (body weight) per day]-1 and it is usually used to animals in determining oral income of the stressor through a food chain, including food, water and accidental consumption of soil;
- A reference concentration (RfC) is usually determined in mg·[kg or m3 (environment)]-1 and is used usually to the receptors located on the lower levels of a food chain and in direct contact with a contaminated environment (air, water or soil). However, *RfC* can be used to the receptors located on the upper levels of a food

chain by back conversion from *RfD* receptor through the stressor movement along the food chain to the *RfC* value of the environment that will not lead to an unacceptable level of an effect of the stressor on the receptor;

- A critical body residue (CBR) represents a concentration of the stressor in the body of the receptor, and is usually determined in mg·[kg (tissue)]-1 and applied to the stressors that are accumulated in the body of the receptor. This metric can be applied to any type of the receptor (plants, invertebrates, fish, animals) and is a limiting concentration, exceeding it leads to a toxicological response of the receptor.

3. The risk characteristic. This stage integrates the data on the dangers of the stressor, the exposure value, parameters of the dependence "dose - response" obtained at all previous stages of a research with the aim of a quantitative and qualitative risk assessment, the detection and the assessment of the relative importance of the existing problems for the well-being of people and biota.

The risk characteristic is performed according to the following steps:

- Summarizing the results of the exposure assessment and dependencies "dose (concentration) - response";
- Calculation of the risk for individual routes of the stressor income;
- Calculation of the risks subjected to aggregating (an income of one stressor in the body of the receptor by all possible routes from various objects of the environment) and cumulative (a simultaneous effect of multiple stressors) exposure;
- Detecting and analysis of the uncertainty of the risk assessment;
- Summarizing the results of the risk assessment and presentation of the obtained data to the persons involved in the risk management.

In the process of the risk characteristic the value of the acceptable risk is used, i.e. the probability of an event that has so small negative effects that for the received benefits from a risk factor, a person or a group of people or society in general are willing to take that risk.

For carcinogens the additional probability of the developing of cancer in a human body throughout a life (*CR*) is estimated based on the average daily dose over a lifetime (*LADD*). The *LADD* value is calculated from the equation (1) (*LADD* = *I*), herein the average time value *AT* is assumed to be 70 years (25550 days). The value of the carcinogenic risk is determined from the equation (2)

$$CR = LADD \cdot SF, \qquad (2)$$

where *LADD* is an average dose over a lifetime, mg·(kg·per day)$^{-1}$;

SF – a slope factor, [mg·(kg·per day)$^{-1}$]$^{-1}$, which represents the degree of the carcinogenic risk increase with increasing a dose per unit and is a value that describes the dangers of carcinogens.

The risk characteristic of the development of non-carcinogenic effects for humans and biota is based on the calculation of a hazard quotient by the equation (3)

$$HQ = AD/RfD, \qquad (3)$$

where *HQ* – a hazard quotient;

AD – an average dose, mg·kg^{-1} body weight per day, determined from the equation (1) (*AD*= *I*).

The hazard quotient is calculated separately for conditions of the short-term (acute) and long-term actions of the stressor. Herein, the average time *AT* of exposures and corresponding safe levels of the actions should be similar.

Tab. 1 Hazard Level Classification

Hazard		Hazard Level
Non-carcinogenic *HQ (HI)*	Carcinogenic *CR*	
<1.0	$< 10^{-6}$	Minimum - a desired (target) risk value in conducting health and environmental activities.
1.0–10.0	10^{-4} - 10^{-6}	Medium - valid for the conditions of military service. Under the impact on the civilian population, it requires a dynamic monitoring of the environment.
10.0–100.0	10^{-3} - 10^{-4}	Considerable - unacceptable to the civilian population, a dynamic control and an in-depth study of the sources and consequences of possible harmful effects are required for the conditions of military service to address the issue of risk management measures.
>100.0	$>10^{-3}$	High - not acceptable for the military service in a peacetime and for the population. It is necessary to take measures to eliminate or reduce the risk.

The risk characteristic of non-carcinogenic effects in an aggregate and cumulative effect of the stressors is based on calculating the hazard index (*HI*).

$$HI = \Sigma HQi, \qquad (4)$$

where *HQi* - hazard quotients for individual conditions of aggregate and cumulative effects of the stressors.

In assessing the risk to human health and well-being of biota caused by the influence of the stressors, it is advisable to focus on the criteria system of hazard acceptability [9] (Tab. 1).

3 CASE STUDY

The theoretical assumptions introduced above were used to assess the impact of the military range on human health and biota on the example of the International Peacekeeping and Security Center (IPSC) (a former military range in Yavoriv). IPSC is located in Lviv region. Its purpose is to train the Armed Forces of Ukraine. Tanks, armored personnel carriers, infantry fighting vehicles are used for the tactical training of troops in the military range, besides that educational fields for training communications, artillery, missile and artillery units, as well as a shooting range, are located at the military range area. A part of the military units are located at the territory of IPSC only for the time of exercises, and another part has a permanent location.

The territory of IPSC refers to the western ridge of Roztochia which is one of the most interesting physiographic regions of Western Ukraine, which is the boundary area of the East European platform and the edge of the Carpathian foothills. The variety of flora and fauna of IPSC is determined by the natural conditions of the region Roztochia, and especially its boundary location that facilitates the exchange of floral and faunal material between Polissia and the Carpathians. No wonder that the southeastern borders of the military range borders on the area of Yavoriv National Park, which, in turn, in its southern part borders on a nature reserve "Roztochia". The combination of mixed forests along with swamps and ponds led to the formation of a complex set of rich fauna species listed in the Red Book of Ukraine, including 1 species of reptiles, 18 species of birds and 7 species of mammals.

We will try to determine how safe the activity of the military range is for people, especially military men who stay permanently at this territory and its possible negative effects on the biota by the environmental risk assessment. A white-tailed eagle (Haliaeetus albicilla L.) is taken as an indicator type of biota. It is a valuable and rare bird that is not only included in the Red Book of Ukraine, but also in the European Red List.

It should be noted that a systematic monitoring of the environmental conditions in IPSC is not performed. The studies conducted in 1997 [10] found that there was some contamination of the soil with metals (Tab. 2) and slight air pollution at the time of exercises. The inspection of the military range conducted in 2009 [11] showed that the degree of contamination of the soil remained at about the same level, the contamination of the surface springs was within the national standards, there was no air pollution. Therefore, further the environmental risk was estimated concerning the influence on human beings and biota of contaminated soil.

Tab. 2 Concentrations and toxicological characteristics of soil pollutants of the military range

Characteristic	Pollutants			
	Lead	Nickel	Copper	Zinc
averaged concentration in the soil, mg·kg^{-1} soil	35	32	10	40
common sanitary standard of Ukraine (maximum permissible concentration), mg·kg^{-1} soil	3.0	6.0	4.0	23.0
SF, [mg·(kg body weight per day)$^{-1}$]$^{-1}$	0.042	0.84	---	---
RfD chronic income for a person, mg·(kg body weigh per day)$^{-1}$	0.019	0.0035	0.02	0.3
RfD chronic income for birds, mg·(kg body weight per day)$^{-1}$	1.6	6.71	4.0	2.66

Concerning the military the object of the study was chosen taking into account the most susceptible contingent. Thus, the object of the study was the officers’ personnel of the military compound which is always located at the territory of the military range. The calculation of the risk was carried out under conditions of the aggregate and cumulative exposure of a human body with soil pollutants according to the equations (1) - (4) with the standard values of exposure parameters recommended in [12]. The exposure averaging period made 70 years for carcinogens and 30 years for non-carcinogens.

The calculation of the risk to a biota representative – a white-tailed eagle – was carried by the equations (1) and (3), (4). The income of metals in a body of a bird, in principle, is possible only through a food chain.

The bird feeds mainly on fish, small mammals in the breeding season, and in winter - waterbirds and fish. The diet of an adult bird is 20-30 % - fish , 40-60 % - birds , 20-30 % - mammals, the weight of an adult bird is 3,0-4,5 kg, the life expectancy is 30 years. In the calculations, it was taken into account that the income of metals in the body of a bird was only possible through the meat of mammals (field mice) that feed on plants growing in the contaminated soils, as fish and waterbirds are hardly polluted due to the high quality of water reservoirs. Also the seasonal factor of consumption of contaminated food was taken into account (6 months per year). The exposure was calculated over a life period of the bird.

Comparing the results of the calculations (Tab. 3) with the acceptable risk values (Tab. 1) it can be noted that the risk of residence for servicemen in the military range is acceptable, and for biota it is very little, despite the fact that the soil contamination exceeds sanitary standards of Ukraine. So, there is no need for environmental measures, as there is no threat to life and well-being of any person or biota.

Tab. 3 Calculating the risk for people and biota at the territory of IPSC

Carcinogenic risk for people, *CR*	$5.62 \cdot 10^{-05}$
Non-carcinogenic risk for people, *HI*	0.433
Risk for biota (a white-tailed eagle), *HI*	$0.45 \cdot 10^{-04}$

4 CONCLUSION

The environmental risk assessment is a more accurate mechanism of assessment of the environment, in comparison with the established common sanitary standards and allows taking decisions in a more flexible way concerning the objects of the environment. So exceeding of concentration of metals in soil as compared to common sanitary standards must testify to the certain threat for people and biota and necessity of acceptance of nature protection measures. Assessment of risk testifies to absence of threat.

References

[1] Rule of the ecological providing in Military Forces of Ukraine (order of Minister of Defence №171)

[2] PAUSTENBACH, D. J.: *Human and Ecolo-gical Risk Assessment: Theory and Practice.* New York, NY : Wiley, 2002. 1586 p.

[3] SUTER, G. W.: *II. Ecological risk assessment.* Boca Raton, FL: Taylor & Francis Group, 2007. 654 pp. ISBN 1-56670-634-3.

[4] BRUCE K. H.: An examination of ecological risk assessment and management practices. In *Environment International*. 2006. Vol. 32. p. 983-995.

[5] EPA/630/R-95/002F. Guidelines for Ecological Risk Assessment. Washington, DC : 1998. Available at: http://www.epa.gov/superfund /programs/ nrd/era. htm.

[6] *The Air Toxics Hot Spots Program Guidance Manual for Preparation of Health Risk Assessments.* BLAISDELL, R. et al. Oakland, Cal.: OEHHA, 2003. 302 p.

[7] GLENN, W., SUTER, I., KETURAH, A. REINBOLD, WINIFRED, H., MANROOP, R., CHAWLA, K.: *Military ecological risk assessment framework (MERAF) for assessment of risks of military training and testing to natural resources.* Oak Ridge, TN : Oak Ridge National Laboratory, 2002. Available at: www.esd. ornl.gov/programs/ecorisk/documents/MERAF_final.pdf

[8] *FCSAP Supplemental Guidance for Ecological Risk Assessment. Technical Module B. Selection or Development of Site-specific Toxicity Reference Values.* Vancouver, BC : Azimuth Consulting Group, 2010. Available at: http://geoenvirologic.ca/Documents/20120631_TRV%20Module_EN.pdf.

[9] HAIYI, L., AXEA, L., TREVOR, A. TYSON: *Development and application of computer simulation tools for ecological risk assessment.* Environmental Modeling and Assessment,2003. V.8. p. 311–322.

[10] ПІДЛІСНА М.С. *Оцінка екологічного стану Яворівського полігону та вимоги з охорони довкілля при проведенні військових навчань* Львів: ВІНУ "ЛП", 1997. 31 с.

[11] МАНЕНКО А.К. *Екологічний та гігієнічний огляд зон об'єкту Яворівського загального військового полігону І категорії сухопутних військ збройних сил України.* Гігієна населених місць. 2009. № 54. С. 40 – 47.

[12] EPA/600/R-09/052F. Exposure factors hand-book. Washington, DC : 2011. Available at: http://www.epa.gov/ncea/efh.

Assoc. Prof. Sergiy OREL, PhD.
Lt. Col. Oleksiy IVASCHENKO
Hetman Peter Sagaydachniy Academy of the Ground Forces
Gvardiys'ka St., 32, Lviv
79012 Ukraine
E-mail: orelsm0@gmail.com
vania.ivanivan@yandex.ua

LESSONS LEARNED FROM MILITARY CYBER DEFENCE EXERCISES

Branislav KULICH

Abstract: Cyber attacks directed against the Armed Forces of NATO member states are on the rise. Range and sophistication of attacks are constantly evolving, moreover, we have to cope with increasing complexity and dependence on information technology. Cyber exercises in the military environment play an important role in the process of receiving human knowledge through experience. Furthermore, this experience is enhanced by synergic effect and competitiveness. This paper describes practical experience of such exercises in various stages and gives inspiration for future exercises.

Keywords: Cyber defence exercises. Incident handling. Red team. Talent management. Locked shields.

1 INTRODUCTION

Cyber defence exercises (CDX) focused on the area of information security have become widespread throughout the world over decades. Organizations that depend on examining the ability of individuals and teams in this field are professionally engaged in their preparation and organization. Exercises in cyberspace are organized according to different methodologies. In practice, their focus might be on defence, offense, or combination of both techniques.

Cyber exercises are intended to verify the ability of individuals and teams in an increasingly complex world of cyber crime. The appropriate form of the exercise is considered to be a competition among teams in cyber defence skills.

In developed countries, communities, and organizations, simple analytical exercises are being organized even at the level of primary education to underpin widespread talents in this field.

The essential component in the organization of cyber exercises is to find a way to deal with today's international situation in the cyberspace that can be characterized by rapid development of technology in the connected world.

The first section describes the Cyber Defence Exercise Locked Shields 2013 in brief. The second section presents lessons learned from the international exercise Locked Shields 2013 from the perspective of an active participant. The third part adds lessons learned in general. In the last part of this paper there are formulated challenges that should be applied in future military cyber defence exercises.

2 LOCKED SHIELDS 2013 IN BRIEF

The key characteristics of Locked Shields 2013 (LS13) were as follows:

- It was a live, technical, Blue/Red Team exercise: Blue Teams had to defend networks against real-time attacks.
- It was an international exercise: 18 organisations from 15 nations were engaged in preparing and executing LS13.
- The type of the exercise was a game: the teams did not represent the real organisations they worked for during their daily jobs, but they were placed in fictional roles. A lab environment was used instead of production networks.
- Over the course of two days the Blue Teams (BT) had to defend a pre-built network consisting of roughly 35 virtual machines against the Red Team's attacks. The infrastructure was initially insecure and full of vulnerabilities. To provide feedback to the teams and measure the success of different strategies and tactics, Blue Teams were assigned automatic and manual scores. Each Blue Team was accompanied by 1 or 2 legal advisors to encourage and facilitate cooperation, communication, and understanding among the technical and legal experts.
- Red Team (RT) members were not competing with each other. Their objective was to conduct equally balanced attacks on all the Blue Teams' networks.
- The White Team (WT) had the responsibility for preparing the exercise and controlling it during Execution. The Green Team (GT) was responsible for preparing the technical infrastructure. The Yellow Team's (YT) role was to provide situational awareness about the game, mainly to the White Team but also to all other participants.
- LS13 was organised by NATO Cooperative Cyber Defence Centre of Excellence in cooperation with Estonian Defence Forces, the Estonian Information Systems' Authority, the Estonian Cyber Defence League, Finnish Defence Forces, and many other partners.

Blue Teams from the following nations/organisations participated in LS13: DEU, ESP, EST, FIN, ITA, LTU, NATO NCIRC, NLD, POL, SVK.

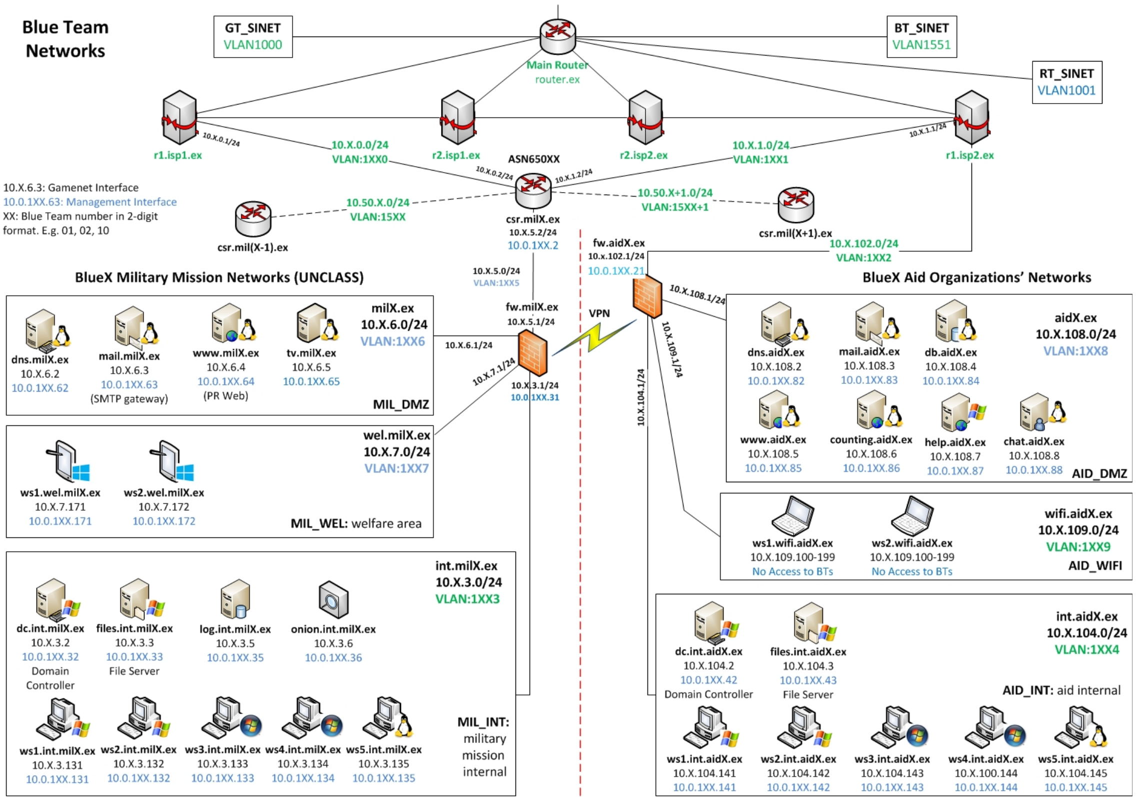


Fig. 1 CDX Locked Shields 2013 infrastructure scheme

3 SVK BLUE TEAM AND LOCKED SHIELDS 2013

The phases of Locked Shields exercise are described in the next context.

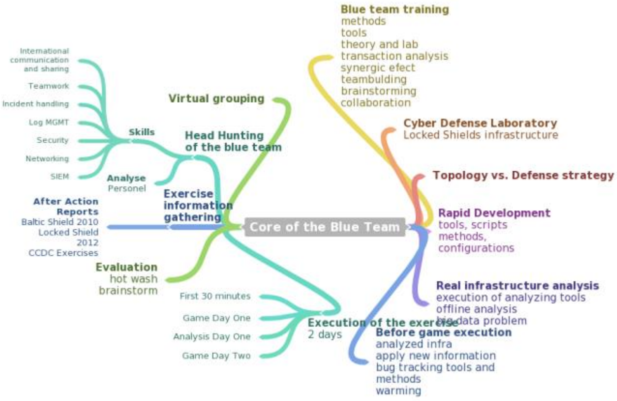


Fig. 2 Mind Map of the exercise phases

3.1 Information about the exercise

In the first step we were informed that we would participate in the exercise. We had an access to the basic information on the specialized website. All teams had registered and had filled up the names of individuals who would have the access to the specific information about the exercise.

From our perspective, we began the analysis. That was the starting point for personnel pick up and analysis methods. A lot of essential information was added during the exercise.

Lesson learned: It is crucial to inform every member of the team and to familiarize them with all the information. It is also important to add every new piece of information during the preparation phase of the exercise and to ensure that everybody understands it. The best tools for reaching this aim are lectures and creative discussions. Mental maps and brainstorming are another two possibilities how to manage the team.

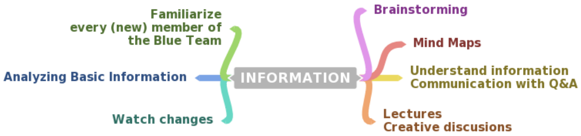


Fig. 3 Mind Map of the „information" phase

3.2 Personnel

Because of experience needs, we created a core team, which was responsible for analysis and preparation before the exercise started and in the latest stages we added another members to execute the exercise as one big team together.

Lesson learned: It is important to find and obtain people with these experience:

- "Learning the network" – understanding physical and logical topologies of network;
- System administration and prevention of attacks;
- Monitoring networks, detecting and responding to attacks;
- Handling cyber incidents;
- Teamwork: delegation, dividing and assigning roles, leadership;
- National and international cooperation, information sharing;
- Reporting;
- Ability to convey the big picture;
- Crisis communication;
- IT legal aspects.

It is beneficial to find some people with "hacker thinking". It means generally talented persons with specialized knowledge of technology . Character of the members is important as well. The ideal status is to have people with proven abilities and experience from other exercises or certificates.

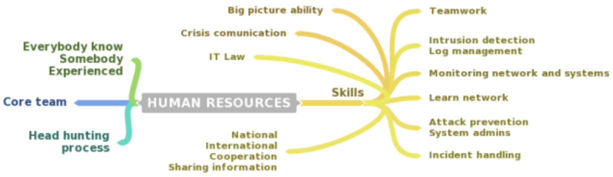


Fig. 4 Mind Map of the „human resources“ phase

3.3 V irtual groups

Individual players could be either a big contribution or danger for a team cohesion. Therefore if the group is bigger, it is important to appoint a team leader who will be responsible for fulfilling the goals of the group. Next important aspect is the plan and its compliance, since the matter of course is the collaboration of all the groups together. Another important part is to define the way how the members communicate, how they use collaboration tools, how they solve previous aims set, and how the experienced and well informed individuals give their knowledge to the younger members of the team.

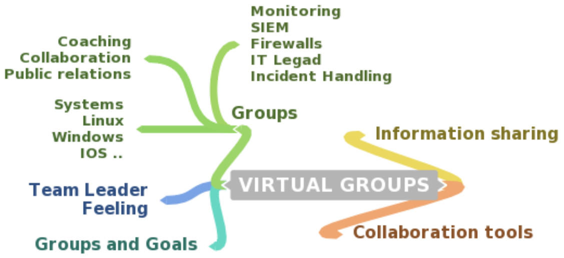


Fig. 5 Mind Map of the „virtual grouping“ phase

3.4 Seminars and exercises

Before the real game started it was necessary to define security risks, the participants' abilities, and the knowledge areas which were important to be learned or executed, following the topology of exercise.

Lesson learned: Licences for commercial software, educational courses on new technologies and procedures had to be prepared earlier. Occasionally individuals explore a new technology or procedure suitable for implementation, but it is essential to reconsider the risk of implementation of such a new procedure in a running exercise. It is important to find a balance between active and passive preparation. A valid attitude is to suppose and think about situations which are expected for the teams to go through during the game and to prepare individuals, technology, and information for all the backup scenarios. Last but not least, it is very important to have individuals fully focused on their roles in the teams and do not solve tasks which are not important for the exercise.

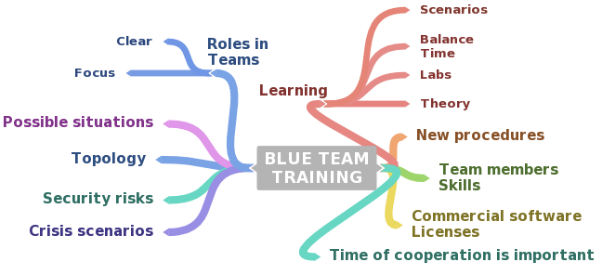


Fig. 6 Mind Map of the „blue team learning and training“ phase

3.5 Preparing the infrastructure

Before the exercise, it was necessary to check all technologies, to apply planned procedures and evaluate their effectiveness. To accomplish this, the most similar systems to the real exercise were used.

Virtual LAB

The ideal status while training for the game is to have identical infrastructure which will be used for the real exercise. The most timely-demanding part is to create the environment identical to the real one in all the layers. Vulnerabilities are not known during this part, they can be only supposed. The essential part is to foresee vulnerabilities of the technology and possible attacks based on known vulnerabilities. The virtual lab is an ideal place for testing, checking, and learning about new technologies. It is the best place to identify time requirements for separate processes used in forthcoming real situations.

Lesson learned: It is necessary to build a virtual lab in a very short time. It is also recommended to have a backup of the whole infrastructure and to consider final infrastructure capacity, and abilities of all team members.

Virtual servers

During the CDX it is possible to use two virtual servers. The type and connection depends on the strategy of the team.

Lesson learned: This is probably the most important decision of the exercise. Division of the systems into two groups: Linux and Windows could be a mistake, because overall functionality and ability to sustain the attacks is the key factor of success.

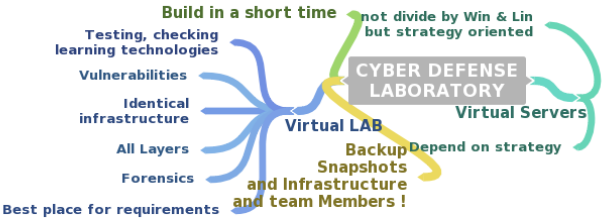


Fig. 7 Mind Map of the „cyber defence lab“ phase

3.6 Determination of topology and strategy of defence

Depending on the topology of the network, vulnerabilities of the system, aims of the exercise, rules, and experience, the technologies which would be put in the real action were chosen. The technologies and chosen tools usually have responsibility for analysis of systems, patch management, firewall operations, collecting and evaluating of logs, proxy systems and ips/ids functionality.

Lesson learned: Some of the technologies are compulsory and strictly given, so it is significant to find as much information as possible about them, train their basic and extended administration procedures. It is important to measure and see the dependencies of all Blue Team infrastructure and logical links to other Blue Teams systems.

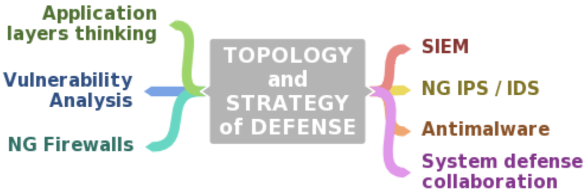


Fig. 8 Mind Map of the „topology and strategy of defence“ phase

3.7 Development of software, scripts and configurations

Detailed infrastructure research, analysis of the services, risks, development of counter-measures was crucial for the next advancement. If standard and accessible technologies are not sufficient, it is necessary to develop new ones. Most of the time this development is connected with automated software installing, automated collection of necessary information for analysis of the environment, patch management, replacement of services, and hardening of operating systems.

Lesson learned: The most significant added value of this step is automation of all the processes. The development should be in “Rapid development” style with consequent testing in the virtual lab. Managing of automation processes should take in account unpredictable mistakes, so it is important to maintain independence of individual processes. It could be sometimes useless to test technology many times, because the failure rate could paradoxically increase.

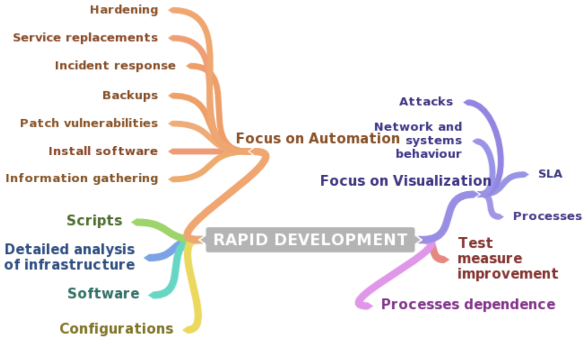


Fig. 9 Mind Map of the „rapid development “ phase

3.8 Analysis of infrastructure

At that moment, the Blue Team had a two-day access to the real infrastructure. Not all systems were active; sometimes a change of configurations or rules occurred at this stage. It was important to focus on analysis of services, vulnerabilities, and software installed in all systems. Identification of risks and making effective counter-measures was possible to perform offline, too, so it meant that it was not important to collect all information about the systems. The key aspect was to check functionality of the virtual servers and the technologies used for defence, monitoring, and installation.

Lesson learned: It is necessary to evaluate the information collected from the systems and services with all team members. As a result the team should be given a transparent map of the systems, services, vulnerabilities, counter-measures and responsible players. Also some vulnerability reports and estimation of attack areas should be prepared in advance. No analysis should be prepared by an individual member, but always by the whole team. This phase should be planned precisely and evaluated on time.

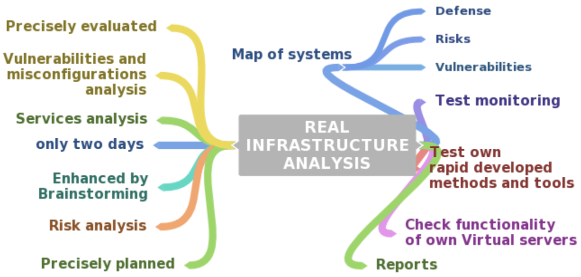

Precisely evaluated
Vulnerabilities and misconfigurations analysis
Services analysis
only two days
Enhanced by Brainstorming
Risk analysis
Precisely planned
REAL INFRASTRUCTURE ANALYSIS
Map of systems
Defense
Risks
Vulnerabilities
Test monitoring
Test own rapid developed methods and tools
Check functionality of own Virtual servers
Reports

Fig. 10 Mind Map of the „analysis real infrastructure" phase

3.9 Preparation of particular processes and advancements

Planned advancements depended on the analysis of environment and the abilities of the players. Technology, responsibility, time demands, and alternative procedures had to be clear. Cooperation, communication channels, and knowledge of all rules were also necessary.

Lesson learned: The leader should take into account occasional inevitable absence of key people. He should be also aware of unfinished processes and incomplete information and take care of the overload of the players. The amount of the tasks should be balanced. It is very time and energy-consuming so it is necessary to motivate the team, exclude the risks, and have alternative "backup" solutions at hand.

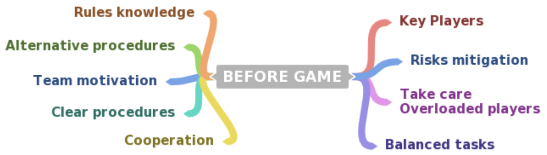


Fig. 11 Mind Map of the „before game" phase

3.10 Execution of the exercise

First phase – security implementation

The first phase of the exercise lasted 30 minutes. In that part, the Red Team was inactive and Blue Teams had to concentrate and follow the steps from the previous phase. Blue Team had to remove all the vulnerabilities which they found, implement security technologies, and connect them logically to the single net. The control and monitoring of overall functionality of the system was obvious. This phase was focused on implementation, patch management, monitoring of access, collecting and evaluating security logs, application of proxy servers and antivirus guards. All failures had to be resolved with high priority.

Lesson learned: After the real technologies are put into a scored game, it is essential to check the accessibility of all the services from an independent source. It occurs quite often that outwardly everything seems to be running, but scoring mechanisms are reporting failures. Discrepancies have to be resolved with the Green Team as soon as possible.

Second phase – game

After the introductory phase, the players were divided into virtual groups. Some individuals were often included into more groups simultaneously. Results from monitoring of services and security logs were basic indicators of incoming attacks on the infrastructure from the Red Team side. The Red Team made their attacks according to a precisely written scenario. Their campaigns were with different goals: Defacement of web sites, erasing important data, installation of malware, compromising operating systems, acquiring inappropriate access to services, denial of services and security technologies. In this phase the Blue Team sent information about detected vulnerabilities, current attacks from the Red Team side and denied services to the White Team. The Blue Team had to comply with requirements about making actual situation reports, summarization reports, and reports about the status of congestion of the Blue Team (stress reports). Media were also sending enquiries about situation and stating legal opinions. Legal questions were resolved by legal advisors of the Blue Team in cooperation with their IT specialists. The customers and employees of the simulated organization also sent their requirements.

Lesson learned: The summarization report is made after each day of the game, so it is good to write it on the fly. Sending reports and answers in the last minutes could cause congestion in the tasks. It is also necessary to monitor the infrastructure and share information about its current status and changes which are made continuously. If a problem occurs, the team leader has to take care of resolving it quickly. The task congestion in the team is not a rare situation, so the team leader must be prepared and make some minor or major team changes if it is necessary to do that. It is also important to watch all communication channels and reports about attacks generated by other teams. After the game day, evaluation and planning for the next day tactics should be done.

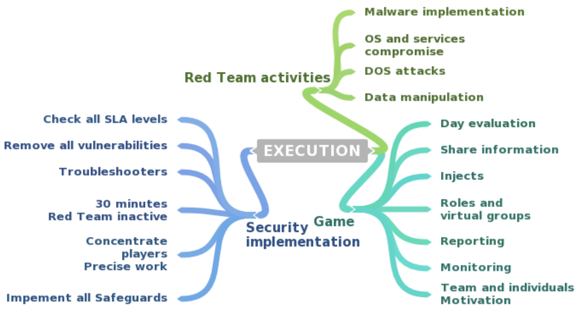


Fig. 12 Mind Map of the „execution" phase

3.11 Evaluation

The final evaluation began the last day and was realised through conference calls; however, the real evaluation began only after the questionnaires from all the teams and players had been sent.

Lesson learned: It is good to take advantage from the fact that the players bear the progress of the exercise in their minds and give them a task to write the feedback. It is also useful to have some questions prepared in connection with the aims of the exercise and to make evaluation of these questions individually and with the entire team as well. Every player expects a feedback. Therefore it is important to formulate and write down the lessons learned document reflecting evaluation of the exercise and suggestions for the next improvement as well as to prepare the final evaluation report together with the official after action report. As a result, the team gets a package of technologies, processes, activity reports of players, virtual teams, and the whole Blue Team activity record. Studying activity reports of other teams and technologies could be a contribution as well. It is inevitable to have full support from superiors, to attract their attention and to present final results with suggestions and improvements for the future.

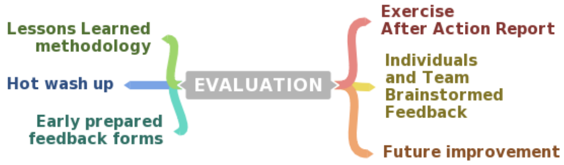

Lessons Learned methodology
Hot wash up
Early prepared feedback forms
EVALUATION
Exercise After Action Report
Individuals and Team Brainstormed Feedback
Future improvement

Fig. 13 Mind Map of the „evaluation“ phase

4 LESSONS LEARNED IN GENERAL

In the previous parts of the article there were described the lessons learned from individual phases of the exercise, but there is still a need to contribute other important facts.

4.1 Red Team

In practice it is known that creating information security requires education and experience. Every technology, whether simple or not, requires a lot of penetration tests. The ideal case would be to have a specialized red team, which could test the effectiveness of our defensive mechanisms. But this requires the highest level of security knowledge, which contains the area of vulnerabilities and exploits, programming one-purpose malwares, botnets management, campaigns, and social engineering. Every organization should have such a team available. The best security experts should be some previous members of the Red Team, because they can easily see the weakest parts of the organization or its infrastructure.

4.2 Exercises

Cybernetic exercises form the base for checking functionality of security teams, methods, and tools. Apart from defence exercises, there are also attack exercises organized worldwide, or exercises which combine both – attack and defence. Besides all the technical and practical exercises, the organizations can also join process exercises, which should check processes of collaboration and cooperation among organisational, national, and international units. Also interesting types of competitions are competitions organized with the aim to arrange security projects and solutions based on analytical tasks.

4.3 Social networks of military professionals

Cyber defence is a wide area. Development moves forward on the attacker’s side and also on the defence side. Every organization needs specialists for cyber defence, but there is a problem of how to obtain them, test them, and deploy them. Finding suitable candidates is possible through head-hunting methods, through public competitions in the IT area, through talent management or through connection of practice with educational institutions. The aim is to interconnect specialists and share experience, knowledge, opinions, and to collaborate on cyber defence projects.

4.4 The hackers

A hacker is a person who is not interested in attacking or harming the system. A hacker is a computer specialist, or a programmer with detailed knowledge, skills, and information about how the system works. He can cooperate with the system and can adjust it. If the team wants to win, it needs some hackers.

4.5 Next research is necessary

Automation and application of artificial intelligence in intrusion detection is essential. I see scope for research in new methods of intrusion detection on the base of artificial intelligence. Research and development of new methods help people respond more effectively to incidents in cyberspace.

5 CONCLUSION

Cyber defence exercises clearly show that the power of an individual may be multiplied with synergy effects during the exercises. Of course, it is necessary to configure the team properly and to use the qualities of individual players. We can create the right response to the current situation in cyber security by quality cyber security exercises and cooperation between individuals and teams. Spreading the "military hackers" community has great importance.

References

[1] Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report, Cyber Defence Centre of Excellence (CCDCOE) and Swedish National Defence College (SNDC), 2010.

[2] GEERS, K.: *Live-Fire Exercise: Baltic Cyber Shield 2010*. Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD COE).

[3] Cyber Defence Exercise Locked Shields 2012, After Action Report, Tallinn 2012, Swiss Armed Forces (SAF) Command Support Organisation, Finnish Defence Forces (FDF), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), and the Estonian Cyber Defence League (ECDL).

[4] HOFFMAN, L. J., RAGSDALE, D.: Exploring a National Cyber Security Exercise for Colleges and Universities, RN CSPRI-2004-08 The George Washington University, RN ITOC United States Military Academy, 2004.

[5] National Collegiate Cyber Defense Competition. Available at: http://www. nationalccdc.org/.

[6] CyberPatriot – the premier national high school cyber defense competition. Available at: http://www.uscyberpatriot.org/.

[7] CTF - Capture the Flag. Available at: http://en.wikipedia.org/wiki/DEF_CON, https://ctftime. org/.

[8] U.S. Cyber Challenge. Available at: http://www.uscyberchallenge.org/.

[9] Cyber Security Challenge UK. Available at: https://cybersecuritychallenge.org.uk/.

[10] NATO CCD COE - NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://www.ccdcoe.org/.

[10] ENISA - European Network and Information Security Agency. Available at: http://www. enisa.europa.eu/.

Eng. Branislav KULICH
Information Security Department
Stationery Base of CIS
Armed Forces of the Slovak Republic
Olbrachtova 5
911 01 Trenčín
Slovakia
E-mail: Branislav.Kulich@gmail.com

QUALITY VALUE ANALYSIS FROM CUSTOMERS' POINT OF VIEW

Iveta KMECOVÁ, Robert ZEMAN, Daniel KUČERKA, Monika KUČERKOVÁ

Abstract: In our contribution we highlight the importance of marketing and its great influence on running a business successfully. We present some results of the research focused on judging the process of providing quality value in business field.

Keywords: Marketing. (Quality) value. Customer. Business. Price of a product. Qquality of a service.

1 INTRODUCTION

In each economically developed country, the economy is based on a system of free enterprise and free competitiveness. These features are characteristic for a market economy. Enterprises should offer the value to the market with which the consumer is satisfied. And marketing is the way how to combat competitors successfully.

Marketing influences all areas of the company. Its main objective is [1] to meet the needs and wishes of people . The task of each enterprise is to find the target consumer, identify its needs, wishes, present a good product and promote it so that the customer would accept it at the demanding price.

All businesses should therefore be aware of this fact. In order to provide the quality they must employ the people who have high technical, professional profile and can adapt flexibly to the constantly changing market situations [2] .

The high quality is a crucial condition for the existence of some businesses. Therefore, the enterprises, if they want to survive in a competitive market and achieve the satisfaction of the customer, should use the tools of marketing mix in their policy [3].

It is therefore necessary to monitor, understand and analyze customer´s needs constantly. Only by knowing the customer's needs, we can offer the value to the market. This value is essential in order to maintain the success and achieve maximization of the profit.

2 MODERN MARKETING, MARKETING MIX

Modern marketing, as the Kotler [4] introduces, should be understood not only as the ability to sell, but in a new meaning as the meeting the needs of the customer. Marketing is defined as a social and managerial process by which individuals and groups satisfy their needs and desires in the process of production and change of products and values "[4].

Following this fact, we can say that the success of the company in the long term is determined by the company's marketing strategy which is set correctly. All marketing strategy is based on four basic tools of marketing mix.

Marketing mix in the form of “4P”, is based on the seller. Marketing staff, however, should take into account the form of a “4C” from the side of the target customer, making it much easier to determine the “ 4P “ [5]:

- value for a customer,
- customer costs,
- availability,
- communication.

Modern marketing [1], [4], requires from companies not only the creating of good products at attractive prices, as well as communication with customers and listening to them .

3 THE CONSUMER SURVEY AIMED AT ASSESSING THE PROCESS OF THE PROVIDING VALUE IN TRADE

From the reasons mentioned above, the research of customers was realized and it was focused on the evaluation process of the provided value in trade .

Based on the results obtained from the survey, we found out the reality and the respondents' views on the process of delivering value in the business. The results were obtained by questionnaires.

Objective of the survey

The aim of the survey was to assess the status of the value provided in the trade through the opinions and attitudes of respondents and also to predict the evolution of the relation the business - the customer.

Subject of the survey

- Rated attributes in the shop,
- Consumer´s satisfaction with the provided value in the shop,
- Opinions and consumer´s demands for the quality of products and services offered.

Survey sample

The survey was conducted in the months of February-March 2012. The survey sample consisted of 150 respondents in total.

It consisted of fourth grade students of study field, the first and second year of post-secondary study of Secondary vocational technical school in Hlohovec, teaching staff (teachers, masters, servants of economics department) of Secondary vocational technical school in Hlohovec, fourth grade pupils of

Secondary vocational technical school in Hlohovec and fifth grade students of University of Economics Bratislava (Faculty of Commerce, Department of Marketing) .

In the Tab. 1, we present the representation of respondents according to their education and age and the total number of respondents also expressed in percents.

Tab. 1 Structure of respondents according to the schools participating in the survey

School		1	2	3	4	5
18 - 29	Number	53	0	29	10	92
	[%]	57,6	0	31,5	10,9	100
30 - 39	Number	15	7	0	0	22
	[%]	68,2	31,8	0	0	100
40 - 49	Number	9	11	0	0	20
	[%]	45,0	55,0	0	0	100
50 - 59	Number	0	16	0	0	16
	[%]	0	100	0	0	100
M + F	Number	77	34	29	10	150
	[%]	51,3	22,7	19,3	6,7	100

1 - SVTS student, 2 - SVTS ped. Worker, 3 - SVS student, 4 - EUBA student, 5 - Total

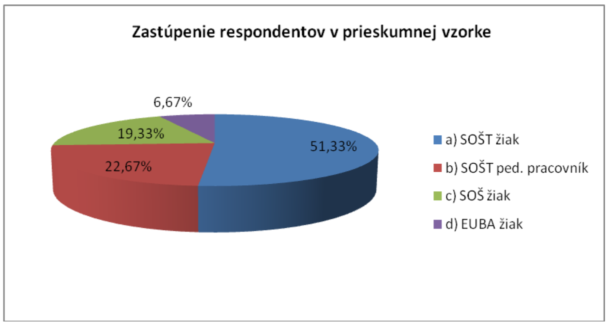


Fig. 1 Graphical representation of respondents (total M+F in %) according to the schools surveyed

Survey methodology

To implement the survey for finding out the opinions about the individual attributes constituting the value for the customer, we used the questionnaire method.

Hypotheses:

H1: The value for the customer is mostly the goods which company offers (quality / price).

H2: At least 50 % of respondents consider product quality as the most important factor when buying.

Organization of survey

Conducting the survey (in the case of Secondary vocational technical school in Hlohovec and Secondary technical school in Hlohovec), was agreed in advance with the school.

Respondents from Economy University in Bratislava, were randomly selected and contacted on a voluntary basis.

Partial results of the survey

We present the partial evaluation of the questionnaire for the assessment of the trade attributes that make up the value for the customer. The analysis was based on the percentage occurrence of respondents' answers to the items from the questionnaire.

For illustration with the approval of the survey contractor (Kmecová, 2012), we present the evaluation of several items of the questionnaire:

Item 1 *What do you think is the most valuable, according to which things you make your purchasing decisions and what attracts you most to a particular store?*

a) goods offered by a company (its quality, price, ..),
b) particular company / store / retail chain (you are happy with a particular brand of trade),
c) employees of the company (are nice, helpful advice, ...),
d) services (e.g. supply in houses , customer service , ...),
e) treatment of complaints.

In item 1, we wanted to learn from respondents, which they believe is the most valuable, according to what criteria they make their purchasing decisions. In the Tab. 2, we present the answers of respondents to the options listed above.

Tab. 2 Expressions of respondents by age group what they believe is the most valuable, how they decide when buying and what attracts them to particular trade

Answer		a)	b)	c)	d)	e)	f)
18 - 29	Number	77	10	1	2	2	92
	[%]	83,7	10,9	1,1	2,2	2,2	100
30 - 39	Number	15	5	1	0	1	22
	[%]	68,2	22,7	4,6	0	4,6	100
40 - 49	Number	18	2	0	0	0	20
	[%]	90,0	10,0	0	0	0	100
50 - 59	Number	10	2	4	0	0	16
	[%]	62,5	12,5	25,0	0	0	100
M + F	Number	120	19	6	2	3	150
	[%]	80,0	12,7	4,0	1,3	2,0	100

Item 2 How high the shop where you buy most often meets your expectations? Please evaluate the individual attributes. Please circle one of the options (1 - fully meets the expectations, 2 - meets, 3 - neither meets or not meets 4 - not meets, 5 - fully not meets).

a) price of products 1 2 3 4 5
b) quality of products 1 2 3 4 5
c) quality of services 1 2 3 4 5

d)	staff	1 2 3 4 5
e)	appearance of the shop	1 2 3 4 5
f)	overall atmosphere of the shop	1 2 3 4 5
g)	availability	1 2 3 4 5

In item 2, we wanted to learn from respondents how high the store meets their expectations. Respondents expressed their opinions to seven attributes of the shop.

In the Tab. 3, we present the answers of respondents (97 men and 53 women, total 150 respondents who formed an exploratory sample) to the mentioned attributes in the shop.

Tab. 3 Expressions of respondents (men + women of all ages) to the item 1, how high the shop where they do their shopping meets their expectations

Evaluation attribution				a)	b)	c)	d)	e)	f)	g)
Men + Women 150	I.	Range	1	11	19	15	19	22	12	40
			2	69	73	56	45	70	72	61
			3	58	45	57	46	45	54	36
			4	8	11	20	31	12	11	9
			5	4	2	2	9	1	1	4
	II.	Range	1	7	13	10	13	15	8	27
			2	46	49	37	30	47	48	41
			3	39	30	38	1	30	36	24
			4	5	7	13	21	8	7	6
			5	3	1	1	6	1	1	3

I. - Number of replies, II. - Expressed in %, (1 - fully meets the expectations, 2 - meets, 3 - neither meets or not meets, 4 - not meets, 5 - fully not meets the expectations); a) product price, b) product quality, c) quality of service, d) staff, e) store appearance, f) total atmosphere of store, g) availability of store

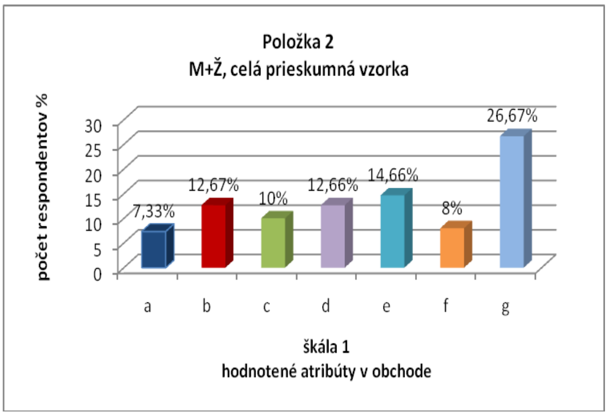


Fig. 2 Expressions of opinions of respondents (M+F together - whole survey sample, range 1) for item 2, how high the shop where they usually do their shopping meets their expectations

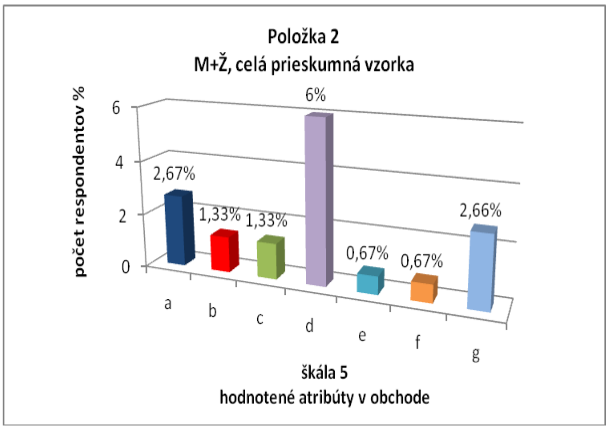


Fig. 3 Expressions of opinions of respondents (M+F together - whole survey sample, range 5) for item 2, how high the shop where they usually do their shopping meets their expectations

Item 3 When selecting a particular product I follow the following order of priority (please sort from 1 to 6, where 1 represents - most important, 6 - least important).

- price of product,
- brand of product,
- product quality,
- store / shop where to shop,
- impact of marketing communication,
- references from family, friends.

Tab. 4 Expressions of respondents (men + women of all ages)) on item 3 according to what I follow in selecting a particular product (1 is - most important, 6 - least important)

Evaluation attribution				a)	b)	c)	d)	e)	f)
Men + Women 150	I.	Scale	1	47	25	69	5	0	4
			2	55	32	48	5	2	8
			3	40	56	26	12	2	16
			4	4	22	6	61	14	40
			5	2	8	1	42	51	47
			6	2	7	0	25	81	35
	II.	Scale	1	31	17	46	3	0	3
			2	37	21	32	3	1	5
			3	27	37	17	8	1	11
			4	3	15	4	41	10	27
			5	1	5	1	28	34	31
			6	1	5	0	17	54	23

I. - Number of replies, II. - Expressed in %, (1 - fully meets the expectations, 2 - meets, 3 - neither meets or not meets, 4 - not meets, 5 - fully not meets the expectations); a) product price, b) product band, c) product quality, d) store where I buy, e) influence of marketing communication, f) family reference.

Tab. 4 shows the respondents' opinions of the entire survey sample of 150 respondents on the fact what they follow when buying a particular product for them.

From the Tab. 4 we can see that most respondents (46 %, 69 respondents), consider the quality as the most important attribute in choosing a particular product. Price is important (scale 2) for 55 respondents (36.67 %). Brand of product is the third in order of importance (scale 3) according to the replies of 56 respondents (37.33 %).

4 CONCLUSION

During the survey the data were obtained by the questionnaire method. In this article we presented the results obtained by evaluating the three items for illustration. The questionnaire included 17 items. The survey confirmed that the goods is the most valuable element that decides the purchase (see item 1, Table 2). The same opinion shared men and women in all age categories. The hypothesis H1 was confirmed. Based on the results obtained from the answers of respondents (men and women), we can conclude that the attributes - the price of products (a) option, quality of products (b) option, the appearance of shops (e) option, the overall atmosphere of shops (f) option and availability (g) option were on a 1-5 scale, evaluated by men and women, concerning the highest percentage range, with the same mark 2 - this means that the business meets the expectations. (Tab. 3, Graph 2, Graph 3)

The survey also confirmed that regarding the choice of a particular product and the importance of attributes (see Table 4) when making purchasing decisions , among men and women , the quality of the product plays the major role . If the product is not good , other attributes such as price , brand , etc. do not play such an important role in making decision. According to the opinions of the respondents, the impact of marketing communication (advertising on TV, ..) has the least influence on the purchase of respondents. H2 also confirmed this fact.

From the above findings of the survey and analysis we present the following recommendations for business enterprises:

- regularly seek the views of customers on the value provided in the store (it is necessary to ask for the products / services of the firm, it means which services are customers satisfied satisfied with, respectively dissatisfied and why),
- through questionnaires , for example 2 times a year to identify customers´ needs,
- publish references and recommendations of satisfied customers (on the company website, the company's promotional materials, etc.) - accept the requirements of customers (if it is possible) and put them into practice.

References

[1] BAJTOŠ, J.: *Psychomotorická zložka osobnosti žiaka – formovanie, rozvoj a hodnotenie v technicky orientovaných predmetoch.* Košice : Equilibria, 2007. ISBN 978-80-89284-07-8.

[2] CIBÁKOVÁ,V., BARTÁKOVÁ, G.: *Základy marketingu.* Bratislava : Iura Edition, 2007. 224 s. ISBN 978-80-8078-156-9.

[3] KMECOVÁ, S.: *Aplikácia nástrojov marketingového mixu v spoločnosti Zentiva, a. s. Hlohovec.* Bakalárska práca, 2010. Evid.č.: 16100/B/2010/2194151412.

[4] KMECOVÁ, S.: *Analýza procesu poskytovanej hodnoty v obchode*. Diplomová práca. Bratislava : Ekonomická univerzita, 2012. Evid.č.. 16100/I/2012/2194151412.

[5] KOTLER, P.: *Marketing od A do Z. Osmdesát pojmů, které by měl znát každý manažér.* Praha : Management Press, 2003. 203 s. ISBN 80-7261-082-1.

[6] KOTLER, P.: *Moderní marketing.* 4. vyd. Praha : GRADA Publishing, 2007. 1041 s. ISBN 978-80-247-1545-2.

Eng. Iveta KMECOVÁ, Ph.D.
Eng. Robert ZEMAN, Ph.D.
Eng. Daniel KUČERKA, Ph.D.
PhDr. Monika KUČERKOVÁ
VŠTE České Budějovice
Okružní 517/10
370 01 České Budějovice
Czech Republic
E-mail: kmecova@mail.vstecb.cz
zeman@mail.vstecb.cz
kucerka@mail.vstecb.cz
kucerkova@mail.vstecb.cz

HEALTH SECURITY IN THE EUROPEAN UNION

František GUBÁŠ

Abstract: Nowadays, at a time when the traditional view of security was challenged by the absence of military confrontation between states and nations, growing awareness is devoted to other sectors of security. The new phenomena that recently emerge are public health problems as a threat to security. The most serious problem is considered possible impact of the spread of communicable diseases and bio-terrorism upon security, particularly upon the stability of state and its armed forces. At a same time, the impact of health issues upon security of individuals and groups began to be recognized. Outbreak of pandemic influenza in 2009 spread all over the world proved that it is necessity to pay maximal possible attention to issues of health security.

Keywords: Security. Health security. Public health. Health threats.

1 INTRODUCTION

After the end of Cold War, with the vacuum created by the diminishing relevance of the confrontation between the two superpowers, the security literature began to address the phenomenon of the so-called "new threats". Among these new threats belong threats to public health and health security which has become an increasingly important international issue and has engaged the attention of national and international security community. Key issues to this increased prominence have been the emergence and spread of infectious diseases such as outbreak of pandemic influenza in 2009, but also other communicable diseases HIV, SARS or new drug-resistant strains of TB and the risk of usage of biological weapons, especially bio-terrorism.

There is of course nothing new about health as an international issue. Infectious diseases have never recognized state boundaries or system of international cooperation attempting to control their spread. What is different about recent attention to health issues is apparently successful attempt to move health beyond social policy and development of its agenda into realms of security policy. [9]

That's the reason why United States Department of Health and Human Services implemented definition of health security in the National Health Security Strategy and defines it as a state in which a nation and its people are prepared for, protected from, and resilient in the face of health threats. Health security is fundamentally composed of the people, programs, and institutions that keep us safe from outbreaks, terrorism, hurricanes, tsunamis, earthquakes, biological and chemical threats, and much more. [3]

Number and unpredictability of health security threats require devoting entire available sources and energy to be prepared to cope with public health concerns. What is more in the future we can expect initial threats from nontraditional sources, such as cyber attacks to infrastructure that could pose major risks to health security.

2 PLACE OF HEALTH SECURITY IN THE SYSTEM OF SECURITY SECTORS

Security as a concept is defined differently depending on approach to this concept by different authors. Security is in the Act No. 227/2002 Coll. [11] defined as state in which are maintained peace and state security, its democratic order and sovereignty, territorial integrity and inviolability of state borders, fundamental rights and freedoms and in which are protected lives, personal health, property and natural environment.

Similarly division of security into separate sectors is a subject of discussions. As basic division of security sectors can be assumed division made by represents of Kodan School Buzan, Weaver and de Wilde who divide them into military, environmental, economic, societal and political. [2] Since contemporary development tendencies indicate the need for increase in number of security sectors it is possible to add to already mentioned as well additional security sectors. Hofreiter in his monografy Securitológia [7] states division of security sectors into military, economic, political, societal, environmental and informational. The informational sector add based on development of global information and communication technologies and increase in dependence of state and other objects of political and economic life from information. Ivančík [8] went even further and add to already mentioned sectors also energy sector.

Based on contemporary tendencies we can add health sector as well, which aims of concern were until now included under societal sector. That can be done mainly based on multiplying problems threatening public health connected with health security of state, groups or individuals.

Problems of public health as security problem is as well mentioned in Security strategy of Slovak republic [1] article 58 where is stated that "SR will create environment and measures to be prepared to get know, verify and answer threats of epidemics and minimize consequences on the citizens and economy of SR and other states. SR will be also prepared for measures on protection against bio-terrorist attacks.“

Factors that are considered as threats for health security include:

- threat of global spread of communicable diseases (AIDS, SARS, H1N1),
- increase in concentration of chemical and radiological polluting substances in products and environment,
- worldwide increase threat in use of biological weapons (anthrax).

3 EUROPEAN UNION STRATEGIC FRAMEWORK ON HEALTH SECURITY

At EU level, the legal basis for addressing health threats is EC Treaty on functioning of the European Union Article 168, which states that Community actions shall complement national policies directed towards improving public health, preventing human illness and diseases, and obviating sources of danger to human health. Accordingly, EU action has focused on coordinating information and measures on communicable diseases and substances related to chemical, biological and radio-nuclear (CBRN) agents. The EU has established a system for epidemiological surveillance and reporting of communicable diseases and it is one of the key mechanisms for Europe-wide coordination on diseases between the Member States, the WHO and relevant public health agencies. This system includes an Early Warning and Response System (EWRS), which is formed by bringing into permanent communication with one another, through appropriate means, the Commission and the competent public health authorities in each Member State responsible for determining the measures which may be required to protect public health.

At international level, the Commission is also actively developing and strengthening existing relationships and collaborations on health security. The Global Health Security Initiative (GHSI) is an international partnership of like-minded countries to strengthen health preparedness and the global response to threats of CBRN substances and outbreaks of pandemic diseases. The initiative was launched by the G7 countries (Canada, France, Germany, Italy, Japan, the United Kingdom and the United States), Mexico and the European Commission in November 2001. [5]

Necessity for solving of health security problems is manifested by issuing numerous documents of the Commission. Mechanism of public health protection is described in commission staff working document „Health Security in the European Union and Internationally“.[5] „White book Together for health: A Strategic approach for EU 2008-2013“ [6] is strategic document which states that member states have the main responsibility for health policy and provision of healthcare to European citizens. However, there are areas where Member States cannot act alone effectively and where cooperative action at Community level is indispensable. These include major health threats and issues with a cross-border or international impact, such as pandemics and bio-terrorism, as well as those relating to free movement of goods, services and people. EU health strategy defines three strategic objectives fostering good health in an ageing Europe, protection of citizens from health threats and supporting dynamic health systems and new technologies.

The European Union health security framework addresses three main areas of work including:

- prevention of health security threats,
- preparedness for health security threats, and
- responses to health security threats.

3.1 Prevention of health security threats

In order to address precisely health security issues such as the prevention and management of pandemic diseases, the deliberate release of CBRN substances and other non-specific threats to health, the Council of Health Ministers set up an informal Health Security Committee (HSC) in 2001. The HSC, chaired by the Commission, is made up of officials from national governments and it has established a multi-annual work program. The 2007-2013 Health Program of the European Union has been the key financing mechanism for projects, setting up networks and initiatives to support the work of the HSC. [5]

EU is preparing plan for the next seven years term named Health Program 2014-2020 which should be approved in the beginning of 2014. One of the greatest challenges in this period is expected to be pandemics and emerging cross-border health threats. Positive influence on improvements in prevention of health security threats should have budget of 449.40 million EUR appointed for Health program in the period of years 2014-2020. It is 39 % more than in period of years 2008-2013.

3.2 Preparedness for health security threats

Preparedness is another area where coordination and cooperation between Member States and the Commission is crucial to ensure coherent responses focused on coordination for capacity building to health threats and cross-sector approaches.

3.2.1 Pandemics

Many European citizens are affected by influenza every winter. In normal seasonal influenza epidemic, between 5 and 10 % of the population becomes ill. Past influenza pandemics have affected the population with much severe magnitude than seasonal epidemics, with attack rates ranging from 10 to 50 %. There were three major pandemics in the twentieth century: the Spanish flu of 1918-1920 (the largest; it caused more than 20 million deaths, perhaps even 50 million deaths worldwide), the Asian flu of 1957-1958, and the Hong Kong flu of 1968-1969. The progression of a highly pathogenic avian influenza (HPAI) epidemic from China and Southeast Asia has given rise to concerns that an influenza virus might arise again, fully adapted to human-to-human transmission and capable of causing millions of deaths and huge economic damage.

Whilst it is impossible to predict next pandemic's onset, health, social and other essential services are likely to be under severe pressure from its outset. An influenza pandemic would result in a high level of public, political and media concern and will cause, throughout and beyond the pandemic period, widespread social and economic disruption. Anxiety, movement restrictions, constraints on public gatherings, distribution difficulties, great number of excess deaths are all likely to add to pressures and disruption to the society.

Effects of the pandemic on societies are inevitable, but careful preparedness and response planning can contribute to mitigating the extent impact. Planning for a pandemic is a complex matter as there is little knowledge of the likely impact: data are uncertain and there is a lack of common feature as well. Based on previous pandemics, expert advice and theoretical modeling, most national preparedness plans are based on planning assumptions which include attack rate, case fatality rate, clinical consultations, hospital admissions, rate of intensive care and work absenteeism.

Considerable progress has been made in recent years in terms of preparedness for influenza pandemics and all EU Member States have put in place national preparedness plans which were tested in practice during the influenza pandemic (H1N1) 2009. [5]

The 2009 flu pandemic or swine flu was influenza pandemic involving H1N1 influenza virus, which originated from previous combination of bird, swine and human flu viruses further combined with European pig flu virus. According to latest WHO statistics the virus has killed more then 18,000 people since it appeared in April 2009, however they estimate that the total mortality (including deaths unconfirmed and unreported) from H1N1 is approximately 284,500 people worldwide. Global infectious rate was 11-21 % and was lower than was previously expected.

It is primarily the responsibility of each Member State to take the measures best adapted to fight human influenza pandemics. However, no country can alone face the consequences of a pandemic. International cooperation is an absolute necessity if its impact is to be reduced. In the EU, where there are no internal borders, additional coordination measures are necessary. Hence the need for EU-level action.[4]

The most serious diseases with pandemic potential identified by WHO are avian influenza, Ebola, Marburg hemorrhagic fevers, Nipah virus, SARS and West Nile fever. Alarming come back in the last quarter of the 20th century was noted with cholera, epidemic meningococcal diseases and yellow fever.

3.2.2 Bio-terrorism

In the aftermath of 11 October 2001, much of attention to the links between health and security policy has been focused on perceived threats from biological weapons, most worryingly as wielded by terrorist organizations and rogue states what has been termed bio-terrorism. Renewed concerns over biological weapons, however, had begun to emerge in the early to mid 1990s. While selective attacks using biological weapons have been carried out in the past, increased potential for causing harm to mass populations and the relatively low cost of such weapons are believed to make the weapons especially attractive to such groups.

Chemical weapons were used in the past for example chemical agents were firstly used as weapons by Germany in WWI. Later was used mustard gas in several wars including British forces in Russian Civil War of 1919, Soviet forces in China in 1930s or Spanish and Italian troops in North Africa. Nerve agents such as sarin were used by Iraq against its Kurdish population in 1987-1988, Gulf War in 1991-1992, during attack on the Tokyo subways in Japan in 1995. [9] Last well known attack is dated on 21 August 2013 in the Ghouta area of Damascus in Syria, where chemical weapons were used against civilians and more than 1,300 people were killed in the attack.

EU security community after these events started discussions over the need to improve preparedness and response measures in the event of a major bio-terrorist attack. It was recognized that EU will not be able to prevent every bio-terrorism but have to improve our response to an incident. Much more effort have to be undertaken to anticipate strategic targets, improve surveillance, draft contingency plans, stockpile vaccines and treatments and train and inoculate health personnel. Once again it is not possible for any state of EU to solve this problem alone and therefore it's necessary to intensify cooperation between Member States.

3.3 Responses to health security threats

To support activities leading to higher level of coordination and cooperation was in 2005 established a general rapid alert system called ARGUS aimed at:

1. Providing an internal platform enabling the services of the Commission to exchange, in real time, relevant information on emerging multisectoral crises or foreseeable or imminent threat;
2. Making available an appropriate coordination process to be activated in the event of a major crisis;
3. Providing the context to communicate effectively with citizens and to offer a balanced, coherent and complete picture of the efforts deployed by the Commission.

ARGUS complements the other sectoral Rapid Alert Systems established by the Commission and operates in the event of multisectoral crises requiring action at Community level (such as the pandemic (H1N1) 2009).

The EU has also reinforced its capacity to ensure a coordinated approach for and support to Member States in disastrous situations. This cooperation takes place through the Community Mechanism for Civil Protection. It is aimed at cooperation and assistance in civil protection in case of major emergencies. It facilitates mutual assistance between Member States if national response capacities become overwhelmed, and it may include immediate civil protection and medical assistance.

The 2005 International Health Regulation (IHR), which applies to the 28 Member States, has created an international framework to prevent, detect, assess and provide a coordinated response to events that may constitute a public health emergency of international concern. It is important to note that the IHR calls for solidarity between countries in detecting and responding to health threats, and this should be the basis for greater equity in global health security. [5]

International public health security relies on the appropriate and timely management of public health risks, which depend on effective national capacities and international and intersectoral collaboration.

4 IMPLICATIONS FOR HEALTH SECURITY REALM

Public health problems are more and more often considered as threat to national but also international security. It is therefore task and responsibility of states as well as international health organizations and unions to take measures to prevent outbreaks of pandemics, spread of bio-terrorism or unintentional releases of chemical, biological or nuclear substances into environment and their negative influence on security of states, regions or even worldwide. It is equally or even more important to be prepared response to such health security threats once they occur. Improve preparedness for health security threats is possible through implementation of several measures.

One of the most important issues is improvement in international coordination, cooperation and collaboration. The knowledge gained by one state during solving of health security crisis can be useful for other states with high possibility of same negative phenomenon appearance. International cooperation can be organized as cooperation between two neighboring states, among member states of unions or organizations to prevent cross-boarder health threats. New and re-emerging health security threats are increasingly linked to sectors that are other than health alone and therefore it’s important to develop multisectoral cooperation as well.

The ability to take adequate response to health security threats is connected with detection of disease outbreak as early as possible. Strengthening early warning systems and surveillance is vital as well as mutual connection and cooperation of already existing systems of different organizations.

Strengthening of national health systems is feasible through smarter investments and preparedness of health services to provide health care in crisis situations. Capacity augmentation of medical treatment facilities in short period of time is decisive moment of successful treatment given to vast number of patient during major threats to public health. [10]

Implementation of new technologies into health security that are expected to develop profusely in the next years and decades will help fight health security threats more effectively.

In the area of health security research it would be useful to have closer collaboration both at European level among Member States’ research programs as well as worldwide. Attention in research should be particularly focused on new diseases emerging as a result of climate and demographic changes.

5 CONCLUSION

Many health security problems from the past, spread of communicable diseases, intentional or unintentional release of chemical, biological or radiological substances or even act of bio-terrorism reveal the fact that it’s to late to start preparing reactions for this negative phenomena occurrence once they happened.

Analyses and experiences proved highly likely possibility of such events occurrence in the future. It is therefore of immense importance for EU to take preventive measures ahead and be prepared for action once they became reality. This can be fulfilled through improvements in international and intrasectoral cooperation, coordination and collaboration and sharing of information and experiences on health security threats; strengthening and networking of existing surveillance and early warning systems; implementing new technologies into health security; closer collaboration in the area of health security research and strengthening of national health systems by ability increase capacities of medical treatment facilities during crisis situations in short period of time.

Taking of such measures will lead to improvement of health security of Member States, all EU but also strongly contribute to international health security in the world.

References

[1] *Security strategy of SR*. [online] Ministry of Defense SR, 2005. 15 pp. cit. [2014-01-27] Available at: http://www.mosr.sk.

[2] BUZAN, B., WAEVER, O., WILDE, J.: *Security: A New Framework for Analysis.* London : Lynne Rienner Publishers, 1998. 239 pp. ISBN 1-55587-784-2.

[3] CICERO, A., INGLESBY, T.: *Health Security Resolutions for 2014*. [online] cit. [2014-01-27] Available at: http://www.upmchealthsecurity.org/website/resources/publications/2014/2014-01-02- health_resolutions.html.

[4] European Commission 2005. Communication from the Commission to the Council, the European Parliament, the European economic and social committee and the Committee of the regions on Pandemic Influenza Preparedness and Response Planning in European Community. Brussels. 2005. 31 pp. [online] cit. [2014-01-24] Available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0607en01.pdf.

[5] European Commission 2009. Health Security in European Union and Internationally. Brussels. 2009. 17 pp. [online] cit. [2014-01-22] Available at: http://ec.europa.eu/health/preparedness_response/docs/commission_staff_healthsecurity_en.pdf.

[6] European Commission 2007. White Paper. Together for Health: A Strategic Approach for the EU 2008-2013. Brussels. 2007. 11 pp. [online] cit. [2014-01-22] Available at: http://ec.europa.eu/healtheu/doc/whitepaper_en.pdf.

[7] HOFREITER, L.: *Securitology*. Liptovský Mikuláš : Academy Forces Academy of General M. R. Štefánik, 2006. 138 pp. ISBN 978-80-8040-310-2.

[8] IVANČÍK, R.: Theoretical and methodological view of security. In *Crisis management 2012*. Roč. 10, č. 1. Žilina : Žilina university, 2012. p. 5-14. ISSN 1336-019.

[9] McINNES, C., LEE, K.: Health, Security and Foreign Policy. In *Review of International Studies 2006*. British International Studies Association, 2006. p. 5–23.

[10] TENCER, A., OZOROVSKÝ, V.: Crisis Preparedness Health of the Slovak Republic. In *Disaster medicine - experiences, preparation, praxis – collection of contributions.* Hradec Králové : Zdravotní a sociální akademie, 2011. p. 100–101. ISBN 978-80-905089-0-3.

[11] Zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu, núdzového stavu a o zmene a doplnení niektorých zákonov.

Cpt. Dipl. Eng. František GUBÁŠ
The General Surgeon Office
Gen. M. Vessela 21
Ružomberok
Slovak Republic
E-mail: frantisek.guas@mil.sk

MODELLING OF THE INVESTIGATION OF CYBERCRIME

Josef POŽÁR

Abstract: The continuing technological revolution in communications and information exchange has created an entirely new form of crime, cybercrime. Cybercrime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence. The article deals with selected aspects of computer crime with stress on some ways of forensic investigation of this phenomenon. Some typical ways of committing computer crime with regard to investigative situations are described here. The process of acquiring, examining, and applying digital evidence is crucial in the success of prosecuting a cybercriminal. In conclusion the author refers to possible education of the police officers about computer crime.

Keywords: Computer crime. Models of Digital Forensics Investigation. Event reconstruction. Crime Scene Investigation.

1 INTRODUCTION

Computer technology has advanced by leaps and bounds in recent years. The widespread growth of cybercrime has affected nations from all across the globe. Incidents of cybercrime have caused extensive loss to a nation’s economy. Loss of business profits and disruption of government and other services severely hampers the growth of any economy.

Attacks on information technology systems are increasing in number, and sophistication at an alarming rate. These systems now range from servers to mobile devices and the damage from such attacks is estimated in billions of dollars. However, due to the borderless nature of cyber attacks, many criminals/offenders have been able to evade responsibility due to the lack of supporting evidence to convict them. In this context, cyber forensics plays a major role by providing scientifically proven methods to gather, process, interpret and use digital evidence to bring a conclusive description of cybercrime activities. The development of forensics information technology solutions for law enforcement has been limited. Although outstanding results have been achieved for forensically sound evidence gathering, little has been done on the automatic analysis of the acquired evidence. Furthermore, limited efforts have been made into formalizing the digital forensic science. In many cases, the forensic procedures employed are constructed in an ad hoc manner that impedes the effectiveness or the integrity of the investigation. In this paper, we contribute with an automatic and formal approach to the problem of analyzing logs with the purpose of gathering forensic evidence.

One of the most common sources of evidence that an investigator should analyze is a logged event from the activities of the system that is related to the incident in question. Indeed, having the logs from all system events during the incident will reduce the process of forensics analysis to event reconstruction. However, log analysis depends largely on the analyst’s skills and experience to effectively decipher complex log patterns and determine what information is pertinent and useful to support the case at hand. Despite the paramount importance of this aspect, not much research effort has been dedicated to the automation of forensic log analysis.

2 COMPUTER CRIME DEFINITIONS

Computer crime, cybercrime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more category. Additionally, although the terms computer crime or cybercrime are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used to facilitate the illicit activity.[1]

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

3 DIGITAL INVESTIGATION DEFINITIONS

Before we describe the investigation process, we need to define the basic and fundamental concepts.[2] There are few agreed upon definitions in the area of digital forensic research, so we will clearly state the definitions we are using, even the most basic ones. Digital data are data represented in a numerical form. With modern computers, it is common for the data to be internally represented in a binary encoding, but this is not a requirement. A digital object is a discrete collection of digital data, such as a file, a hard disk sector, a network packet, a memory page, or a process.

In addition to its numerical representation, digital data has a physical representation. The bits in a hard disk are magnetic impulses on platters that can be read with analog sensors. Network wires contain electric signals that represent network packets and keyboard cables contain electric signals that represent which keys were pressed. A computer converts the electric signals to a digital representation. Digital data can be stored on many mediums and each has different properties that determine how long the data will reside.

Digital objects have characteristics, or unique features, based on their creator and function. We can use the characteristics to identify the data. The state of an object is the value of its characteristics. The state of a running computer process changes every time data is written to its memory.

A digital event is an occurrence that changes the state of one or more digital objects. If the state of an object changes as a result of an event, then it is an effect of the event. Some types of objects have the ability to cause events and they are called causes. Digital objects are stored in a physical form and their state can be changed by both physical and digital events. An object is evidence of an event if the event changed the object's state. This means that the object can be examined for information about the event that occurred. However, future events could cause an object to no longer have information about past events. Every object is evidence of at least one event, because there had to be an event that created the object.

An incident is an event or sequence of events that violate a policy and more specifically, a crime is an event or sequence of events that violate a law. In particular, a digital incident is one or more digital events that violate a policy. In response to an incident or crime, an investigation may begin. An investigation is a process that develops and tests hypotheses to answer questions about events that occurred. Example questions include "what caused the incident to occur", "when did the incident occur", and "where did the incident occur".

If the object whose state was changed by the event still exists, then we can examine it for information about the event and about other objects that were causes or effects of the event. Therefore, we can make our previous evidence definition more specific and state that an object is evidence of an incident if its state was used to cause an event related to the incident or if its state was changed by an event that was related to the incident. Rynearson observed, "Everything is evidence of some event. The key is to identify and then capture evidence relative to the incident in question."[3][i]

We will use the following definitions of evidence, which are a little more general and do not focus on the cause and effect relationship. Physical evidence of an incident is any physical object that contains reliable information that supports or refutes a hypothesis about the incident and digital evidence of an incident is any digital data that contain reliable information that supports or refutes a hypothesis about the incident. It is understood that an object has information about the incident because it was a cause or effect in an event related to the incident.

A digital data has a physical form and physical evidence can contain digital evidence. Using this definition, a hard disk is physical evidence and the sectors and files that contain information about the incident are digital evidence. The collection of the hard disk is the collection of physical evidence and the collection of a digital object from the hard disk is the collection of digital evidence. The difference between physical and digital evidence is in their format and has nothing to do with the type of incident. We can also have physical evidence for a digital crime.

With digital evidence, technology is always needed to process the digital data and therefore the only difference between a forensic and a non-forensic investigation of digital data is whether or not the evidence can be used in a court of law. A forensic investigation is a process that uses science and technology to develop and test theories, which can be entered into a court of law, to answer questions about events that occurred. In particular, a digital forensic investigation is a process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law.[4]

4 DIGITAL INVESTIGATION PROCESS MODELS

Each model of cybercrime investigation must perform those requirements and the following goals were used to define the model:

- The model must be based on the theoretical foundations of computing so that existing and future work in computer science can be used;
- The model must be general with respect to the technology being investigated so that the theory will apply to future as well as current technologies;
- The model must be capable of supporting events and storage locations at arbitrary levels of abstraction so that complex systems can be represented;

- The model must be capable of supporting systems with removable storage and event devices;
- The model must be capable of describing previous events and states so that all evidence can be represented.

To define the theory of an investigation, an investigation must be first defined. The definitions of a digital investigation, which is more commonly called computer or digital forensics, are considered first. This work uses the term digital investigation because the process being considered is related more to a crime scene investigation than the traditional forensic sciences.

A commonly referenced definition of computer forensics is that it „involves the preservation, identification, extraction, documentation, and interpretation of computer data."[5]

The Scientific Working Group on Digital Evidence (SWGDE), which is a group that was formed by the directors of federal labs, defines computer forensics as involving "the scientific examination, analysis, and/or evaluation of digital evidence in legal matters". [6]

The definition of digital evidence is considered next. Some examples include:

- "Information stored or transmitted in binary form that may be relied upon in court"; [7]
- "Information of probative value that is stored or transmitted in binary form"; [8]
- „Information and data of investigative value that is stored on or transmitted by a computer"; [9]
- "Any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi". [10]

Some of these definitions consider only data that can be entered into a legal system while others consider all data that may be useful during an investigation, even if they are not court admissible. In general, legal requirements, which are locale specific, limit the evidence that can be used and therefore the set of objects with legal value is a subset of the objects with investigative value. For this work, a general theory of evidence is used, which can be restricted to satisfy the rules of evidence in a specific legal system.

4.1 NIJ Electronic Crime Scene Model

The U.S. National Institute of Justice (NIJ) published a process model in the Electronic Crime Scene Investigation Guide. The guide is a first responder's reference to different types of electronic evidence and includes procedures to safely handle the evidence. The guide is oriented towards those who respond to the physical crime scene, so emphasis is placed on the collection process. The five phases are shown in Figure 1 and are listed here:

- Preparation: Prepare the equipment and tools to perform the tasks required during an investigation;
- Collection: Search for, document, and collect or make copies of the physical objects that contain electronic evidence;
- Examination: Make the electronic evidence „visible" and document contents of the system. Data reduction is performed to identify the evidence;
- Analysis: Analyze the evidence from the Examination phase to determine the "significance and probative value";
- Reporting: Create examination notes after each case.

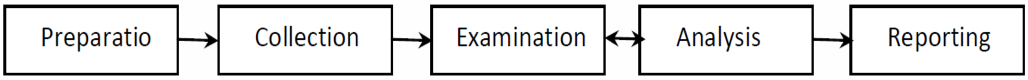


Fig. 1 The NIJ Electronic Crime Scene Guide has a process with five phases in it for a digital investigation

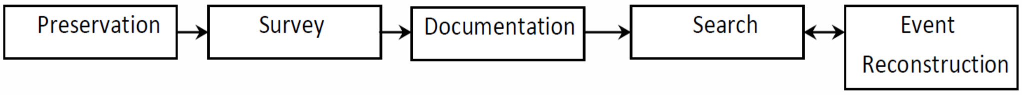


Fig. 2 The Integrated Digital Investigation Process Model has five phases, that are based on a physical crime scene process

The target of the paper was the Collection phase, so few details of the Examination and Analysis phases are given beyond lists of data types that may contain evidence for a certain type of crime. Without additional research, it was not clear if the requirements for the Examination and Analysis phases were different. It could be argued that the techniques used to reduce data in the Examination phase are simply a more general form of the techniques in the later Analysis phase, which performs data reduction by identifying the evidence that is significant. If this is the case, then the model has only a single phase that contains analysis techniques. There are several other models that have phases similar to this model, such as the framework from the Digital Forensic Research Workshop Research Roadmap [11] and the Abstract Process Model [12]. Because they are similar, they are not covered here.

This is because phases in a process model are created based on the experiences of one or more investigators and may not be complete for all types of investigations. An overview of some of the process models is given in the following four subsections.

4.2 Integrated Digital Investigation Process Model

A digital investigation process model based on the investigation process of a physical crime scene was also proposed. The model has high-level phases for the analysis of both the physical crime scene where the computer was located and the digital data. The *digital crime scene* was defined as ”the virtual environment created by software and hardware where digital evidence of a crime or incident exists."

The high-level Digital Crime Scene Investigation phase is organized into the same five phases that can be found in a physical crime scene investigation [13]. The phases can be seen in Figure 2 and are described here:

- Preservation: Preserve the state of the digital crime scene;
- Survey: Search for obvious evidence that is relevant to the investigation;
- Documentation: Document the digital crime scene;
- Search: Conduct a more thorough search for all evidence not found in the Survey phase;
- Event Reconstruction: Reconstruct the digital events that occurred at the crime scene.

5 AN EVENT RECONSTRUCTION SYSTÉM

Unlike the physical world, where an investigator can directly observe objects, the digital world involves many indirect observations. The investigator cannot directly observe the state of a hard disk sector or bytes in memory. He can only directly observe the state of output devices. Therefore, all statements about digital states and events are hypotheses that must be tested to some degree.

Digital investigations, or digital forensics, are conducted by law enforcement and corporate investigation teams on a regular basis. Yet, no formal theory exists for the process. A practitioner in the field can describe how he recognizes evidence for a specific type of incident, but the recognition process cannot typically be described in a general way.

5.1 An Event Definition

The phases and procedures for a physical crime scene reconstruction can be applied to digital crime scenes, but the results present some difficulties because there is evidence at a digital crime scene that is not typically used as evidence in a physical crime. With a digital environment though, the laws that are equivalent to gravity and forces are the instructions that make up the operating system and software. These instructions can be unique to every computer and may need to be used as evidence because an attacker may have modified them.

One of the goals of this work is to formally define the reconstruction process so that requirements and tools can be developed. Unlike physical evidence, all digital evidence requires tools to be used when examining it. This can make analysis more difficult, but it also has the advantage that some procedures can be more easily automated. With a formal model, we can develop requirements for the process. This section will describe our abstract model that can be applied to both physical and digital crimes.

We will now examine events in more detail and start with definitions. We define digital evidence of an incident as any digital data that contains reliable information that supports or refutes a hypothesis about the incident. Digital and physical objects have characteristics that help to identify them. The state of an object is the value of its characteristics, or the data it contains. An event is an occurrence that changes the state of one or more objects. A crime or incident is an event that violates a law or policy. From our previous definition of evidence, we can state that an object is evidence of an incident if its state was used to cause an event related to the incident or if its state was changed by an event that was related to the incident. Event reconstruction is the process of determining the events that occurred at a crime scene by using evidence characteristics.

In a continuous process, which occurs in the physical world, we cannot naturally discuss individual events. Instead, we must transform the continuous process into an approximate discrete process so that distinct events can be determined and examined. In a computer, events can occur only at each processor cycle and therefore the code that a computer executes is already a discrete process.

The roles of objects in events have been examined in many fields. In physics, objects can be cause and effects. Artificial intelligence uses the same concepts, but sometimes uses the term preconditions instead of cause. Regardless of terms, we, too, can classify objects with respect to their roles in events. At the highest level, we can use the following roles:

- Cause: An object plays the role of a cause if its characteristics were used in the event. A test for this role is to identify if the same effect would have occurred “if the object had not existed”. A cause object has an influence on the effect;
- Effect: An object plays the role of an effect if its state was changed by a cause object in the event.

Objects that are causes may be passive. That is, they are used in the event, but they are not changed by the event. If a cause object is changed by the event, then it is both a cause and an effect object. From this it follows that if an object is an effect but not a cause, then it must have been created as a result of the event. The changes to an effect object’s characteristics are related to the characteristics of one or more cause objects.

5.2 Event Reconstruction Process

With our definition of an event and its roles, we can examine the process that occurs in the event reconstruction phase. Recall that when the reconstruction phase begins, the evidence has already been recognized at the crime scene and collected. There are five phases in the reconstruction process:

1. Evidence Examination.
2. Role Classification.
3. Event Construction and Testing.
4. Event Sequencing.
5. Hypothesis Testing.

We will now discuss each of the phases in more detail. As one of our goals is to develop a model that can be used to build software tools, we also provide metrics for each phase. These can be used to compare different techniques and procedures that are implemented to perform event reconstruction.

Police agencies worldwide have struggled to define their role in policing cybercrime and to understand how to be effective in addressing the problem. This is partly because these types of crimes are extremely diverse. The Police of the Czech Republic consider cybercrime (e-crime) to cover:

All offences where information and communication technology is:

- Used as a tool in the commission of an offence;
- The target of an offence;
- A storage device in the commission of an offence.

Cybercrime includes traditional offending facilitated by technology such as telephony, the Internet and encryption. It also involves computer attacks. However, it is important to recognize that the bulk of e-crime we currently see is not attributed to hackers. In the Czech Republic, e-crime mostly involves traditional offending with components having electronic means. This includes trading in illegal drugs, fraud, harassment and many other types of criminal activity. Information technology has particularly influenced some traditional offending. Most notably, this includes: fraud, identity theft, organised crime.

However, cybercrime also includes new activity such as attacks on computers and new opportunities for crime enabled by electronic systems, such as services theft and software piracy. Worldwide these are significant and new problems.

5.3 Investigation of Cybernetic Crime [14]

In the digital forensics investigation practices, there are over hundreds of digital forensics investigation procedures developed all over the world. Each organization tends to develop its own procedures. Some focused on the technology aspects in data acquisition, some focused on data analysis part of the investigation [15].

As many of these procedures were developed for tackling different technology used in the inspected device, when underlying technology of the target device changes, new procedures need to be developed.

There is a range of methods and procedures published by investigators of cybernetic crime. [16] Each criminal act is specific, unique; it differs by its character, way of committing and concealing the cybernetic crime. Digital traces are voluminous, very dynamic, and the crime scene is unknown. That’s why a complete reconstruction of the crime is very difficult. We usually need a special software and hardware to analyze and decipher the digital traces. On the other hand, this method of investigating a digital act is influenced not only by nature and kind of committing, but also by the investigator as a person who decides to choose various methods and techniques of investigation. That is why the investigation of cybernetic crime is always team work performed by experts in different professional specializations. The actual investigation of the cybernetic crime concentrates itself as a rule on these basic aims:

1. To discover the way in which the intruder penetrated into the system. This step is usually divided in three parts:

a) Selection of possible ways of penetration, i.e. creation of a working hypothesis and delimitation of the sphere of the offender's activity;
b) Creating a hypothesis how the penetration happened;
c) Reconstruction of the penetration avoiding destruction of traces.

2. The investigator evaluates the data obtained and interrogates persons for the purpose of evidence.
3. To get useful information in order to retrace the way of the offender, how he penetrated into the system, etc. Here the investigator uses classical methods according to the so-called seven criminal investigation questions: who, where, when, what, how, why, with whom.
4. To find the motive of the offender and, consequently, to find out why he chose this very subject and what made him to attack the system.
5. To collect further data which enables to reduce the list of suspects and to take away the thing (computer and others) under article 79 of the Criminal Code of the Czech Republic.

From the investigative point of view the most important things are the cooperation between the investigator and experts, and the cooperation with the investigative, prosecuting and adjudicating bodies, especially with prosecuting attorney and judge.

6 EDUCATION OF POLICE OFFICERS

The changes in transport technology were as equally dramatic for Police as they have been and are with the changing information age. The officers of the bygone era were challenged; just as we are challenged today by the crime that is generated or accelerated through the use of cyberspace.

Continuous training ensures that personnel stay in touch with current developments of cybercrime. Such training programs also help the participants in keeping up to date with modern tools and techniques for investigating cybercrime.

It is essential that the Infrastructure and other systems used in the Cybercrime Investigation Cell also be checked and audited constantly and upgraded as and when required.

This category refers to investigators and police officers whose primary focus is not cybercrime but who are likely to encounter information technology as part of their work in other areas, e.g. fraud investigators, child protection officers and intelligence analysts. It also includes the important group referred to as “first responders", who must have enough knowledge and training to avoid inadvertently compromising important evidence.

In order to deal with these demands, the local police officer will require:

- Additional training in order to be able to negotiate through the applicable laws, policy and procedures relating to the cybercrime dimension to these reports;
- An understanding of the personal and organisational impacts of cybercrime in order to deal effectively with victims;
- A clear set of procedures for the recovery and handling of technology exhibits, particularly those requirements that differ from routine exhibit handling;
- A process of escalating a situation to operational support personnel where it is a matter beyond their capabilities. Support is necessary to assist an officer dealing with an incident with international connections (e.g., a person defrauded by an e-business being operated from another country). Increasingly, an officer will require basic knowledge to access international police networks immediately on taking up their appointment. Perhaps the most obvious example of this issue was the case of a South Auckland participant in a chat room who learned from a correspondent from the United States that they were planning to use firearms at a local school. The rapid involvement of the Police and FBI, together with very sensible communication from the New Zealander, operated to prevent a very serious crime. More of this can be expected;
- Materials to publicize the risks of cybercrime, and effective crime prevention techniques. Examples of these might be advice to retailers on credit card scams; advice on how to identify forged or misrepresented identity documentation (passports/drivers licenses from foreign nationals);
- Information systems that enable trend analysis for cybercrime matters. A weakness in current reporting of the Police of the Czech Republic is the inability to categorize offence and incidents as enabled by a specific technology (e.g. Internet) and thus crime mapping is constrained;
- Supervisors who are literate and comfortable with law, policy and practice related to cybercrime, and an ability to impart a confidence in their officers to perform in this area; and,
- Support and encouragement (incentives) to develop officers' skills and engage in the processing of cybercrime cases;.
- A highly specialized team of cyber experts based at the Office of the Commissioner to support districts and Interpol and Europol. Alternatively, one expert per district.

Local police officers have as much a need to develop and maintain cybercrime partnerships as do the policy and development specialists in a police headquarters.

This reflects the fact that specialist knowledge is in short supply, and subject to qualifications about security and probity, local police should seek out assistance from any reliable source in their local community. For example, working with partners in telecommunications, the computer industry, cybercafés, Internet Service Providers (ISPs), etc., can assist Police with their knowledge and skills.

7 CONCLUSION

As can be seen, cybercrime has a major impact on the economic growth of a nation. Valuable data is stolen by means of attackers. The various Internet attacks that have taken place have caused global losses amounting to billions of dollars. Cybercrime is a phenomenon whose effects are felt at a global level.

Certainly, cybercrime presents as one of the major challenges for the Police of the Czech Republic. As the information highway expands and the technology becomes more accessible, aspects of cybercrime and crime assisted by information and communication technology will feature in new crime and crime that might be regarded as traditional (burglary, theft, robbery, traffic violations, etc.). The development of technology appeals not only to law-abiding citizens but provides an unprecedented opportunity for criminal behaviour. Our officers will be trained in cybercrime to recognize that computers, cell phones, cameras, etc., will be featuring as 'crime scenes' in both traditional and new crimes. The Police of the Czech Republic, with its focus on community policing, is well placed to develop partnerships with other government and business agencies to work towards intervention and detection.

References

[1] Available at: <http://www.techterms.com/ definition/ cybercrime> [retrieved 22.02.2014].

[2] CARRIER, D. B., SPAFFORD, E. H.: An Event-Based Digital Forensic Investigation Framework. Available at: <http://dfrws.org/ 2004/day1/Carrier-event.pdf> [retrieved 22. 02.2014].

[3] RYNEARSON, J.: *Evidence and Crime Reconstruction. National Crime Investigation and Training.* 6 Edition Canada : Redding, 2002.

[4] HOUGHTON MIFFLIN COMPANY: *The American Heritage Dictonary.* 4 Edition, 2000.

[5] KRUSE, W., HEISER J.: *Computer Forensics: Incident Response Essentials. Addison Wesley*. 2001.

[6] Scientific Working Group on Digital Evidence. ASCLD Glossary Definitions : Version 1.0,2005. Available at: <http://swgde.org> [retrieved 12.01.2014].

[7] International Organisation on Computer Evidence. G8 Proposed Principles For The Procedures Relating To Digital Evidence, 2002. Available at: <http://ioce.org> [retrieved 3.01.2014].

[8] Scientific Working Group on Digital Evidence. ASCLD Glossary Definitions:Version 1.0,2005. Available at: <http://swgde.org> [retrieved 21.01.2008].

[9] ASR Data Acquisition and Analysis. SMART, 2005. Available at: <http://www.nhtcu.org> [retrieved 20.01.2014].

[10] CASEY, E.: *Digital Evidence and Computer Crime*. Academic Press, 2. Edition, 2004.

[11] PALMER, G. A.: *Road Map for Digital Forensic Research.* Technical Report, 2001.

[12] REIT, M., CARR, C., GUNSCH, G.: *An Examination of Digital Forensics Models.* International Journal of Digital Evidence. 1, (3), 2002.

[13] STUART, J., NORBY, J.: (editors). *Forensic Science: An Introduction to Scienti_c and Investigative Techniques.* CRC Press, 2003.

[14] POŽÁR, J.: Policejně bezpečnostní události a informace. In *Základy teorie policejně bezpečnostní činnosti*. Praha : Police History, 2006. s. 147 – 174. ISBN 80-86477-33-9.

[15] POLIT, M. M.: Six Blind Men from Indostan. Available at: <http://dfrws.org/2004/program. shtml> [retrieved 22.01.2008].

[16] POŽÁR, J.: *Základy teorie informační bezpečnosti*. Praha : Policejní akademie České republiky v Praze, 2007. s. 137–142. ISBN 978-80-7251-250-8.

Assoc. Prof. Eng. Josef POŽÁR, CSc.
Department of Management and Informatics
The Police Academy of the Czech Republic
Lhotecká 559/7
P. O. BOX 54
143 01 Prague
Czech Republic
E-mail: pozar@polac.cz