HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

IX. Évfolyam 1. szám 2014. március

NKE
BUDAPEST

A szerkesztőség elérhetősége:
Nemzeti Közszolgálati Egyetem,
1101. Budapest, Hungária krt. 9-11. A. épület 9. emelet, 901. iroda
Postacím: 1581. Budapest Pf.:15.
Telefon: +36-1-432-9000 /29-289/ *Fax:* +36-1-432-9025 *HM:* 29-289
e-mail: hadmernok@uni-nke.hu web: http://hadmernok.hu

Kiadó: Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Dr. Balajti István – NSPA
Bodoróczki János – Nemzeti Közszolgálati Egyetem, HHK HDI doktorandusz
Cser Orsolya – Nemzeti Közszolgálati Egyetem, HHK HDI doktorandusz
Derzsenyi Attila – Nemzeti Közszolgálati Egyetem, HHK tanársegéd
Dr. Földi László – Nemzeti Közszolgálati Egyetem, HHK egyetemi docens
Dr. Gáspár Szabolcs – Nemzeti Közszolgálati Egyetem, HHK KMDI doktorandusz
Gávay György Viktor – Nemzeti Közszolgálati Egyetem, HHK KMDI doktorandusz
Dr. Gyarmati József – Nemzeti Közszolgálati Egyetem, HHK egyetemi docens
Gyebrovszki Tamás – NBSZ Kormányzati Eseménykezelő Központ
Dr. Hornyacsek Júlia – Nemzeti Közszolgálati Egyetem, HHK egyetemi docens
Horváth József – Nemzeti Közszolgálati Egyetem, HHK KMDI doktorandusz
Hronyecz Erika – Nemzeti Közszolgálati Egyetem, HHK HDI doktorandusz
Dr. Kassai Károly – Honvédelmi Minisztérium, HIICSF, osztályvezető
Dr. Kátai-Urbán Lajos – Nemzeti Közszolgálati Egyetem, KI egyetemi docens
Kiss Béla – Nemzeti Közszolgálati Egyetem, HHK KMDI doktorandusz
Kis Enikő – Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala
Dr. Komjáthy László – Nemzeti Közszolgálati Egyetem, KI adjunktus
Kovács Zoltán – Nemzeti Közszolgálati Egyetem, HHK KMDI doktorandusz
Kurilla Boldizsár – Nemzeti Közszolgálati Egyetem, HHK KMDI doktorandusz
Dr. Kuti Rajmund – Audi Hungaria Motor Kft.
Morvai Cintia – OBKF
Nagy József –
Pataki János – Nemzeti Közszolgálati Egyetem, HHK HDI doktorandusz
Dr. Pátzay György – Nemzeti Közszolgálati Egyetem, KI egyetemi docens
Prisznyák Szabolcs – Nemzeti Közszolgálati Egyetem, HHK HDI doktorandusz
Schüller Attila – Klebelsberg Intézményfenntartó Központ
Dr. Sergyán Szabolcs – Óbudai Egyetem, NIK
Solymosi Máté – Somos Környezetvédelmi Kft.
Dr. Solymosi József – Nemzeti Közszolgálati Egyetem, HHK professzor emeritus
Dr. Sulányi Péter – Dr. Gór-Nagy Istvánné Ügyvédi Iroda
Szabó Sándor – Nemzeti Közszolgálati Egyetem, HHK HDI doktorandusz
Székely Zoltán – Pécsi Tudományegyetem, ÁJK DI doktorandusz
Szénási Sándor – Óbudai Egyetem, NIK tanársegéd
Tóth András – Nemzeti Közszolgálati Egyetem, HHK tanársegéd
Török Szilárd – Nemzeti Közszolgálati Egyetem, HHK KMDI doktorandusz
Vámossy Zoltán – Óbudai Egyetem, NIK egyetemi docens
Dr. Vass Gyula – BM Országos Katasztrófavédelmi Főigazgatóság

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Gávay György Viktor - Gyarmati József
gavay.gyorgy@uni-nke.hu - gyarmati.jozsef@uni-nke.hu

PRESENTATION OF OFF-ROAD VEHICLES, SELECTION AND ANALYSIS

Abstract

The process of purchase long and time consuming. The planned in-service time of the military devices is between 15-25 years and in this time their field of operation can also change. A capability analysis that measures the suitability for the widened scope of duties (for example disaster management tasks) is also possible with the usage of decision making support methods applicable in case of research and development. The MCDM processes provide opportunity for the comparison of existing devices with respect to task implementation.

A haditechnikai eszközök rendszeresítése hosszú, és időigényes feladat. Az eszközök tervezett üzemeltetési ideje 15-25 év között van és ez idő alatt az alkalmazási területük is megváltozhat. Döntéstámogató módszerek alkalmazásával lehetővé válik olyan vizsgálat, amely a változó feladatkörökre, például a katasztrófavédelmi feladatokra való alkalmasságot méri fel. Az MCDM[1] eljárásokkal lehetőség nyílhat a meglévő eszközök összehasonlítására a feladat végrehajtás szempontjából is.

Keywords: *military equipment, disaster, cross-country vehicles, applicability, SMART method ~ haditechnikai eszköz, katasztrófahelyzet, terepjáró gépkocsi, alkalmazhatóság, SMART eljárás*

[1] MCDM (Multi Criteria Decison Making) To solve the multi-criteria decision problems developed, the approach adopted by law [3].

FOREWORD

Disaster recovery is part of the tasks of the Hungarian Defence Forces. The available assets significantly affect the effectiveness of the organization. Selecting the vehicles for a task is an operative decision process and it has to be made on the basis of decision theory. A method that eases the selection process is needed. The MCDM methods are good for selecting cars [1] or the military devices [2]. The overall effectiveness of the devices correlated to each other can be seen with the correct usage of these methods.

This publication only deals with the comparison of the military off-road vehicles. The usage of off-road vehicles in the disaster recovery have been examined from different points of view. The analysis lacks the defensive criteria that are important for military usage, but instead it is based on criteria like ergonomics, number of transportable persons and mobility, which has been defined taking into consideration the VSE method.

THE METHOD OF THE ANALYSIS

The comparison is based on one of the simple processes of the MCDM the SMART (Simple Multi-Attribute Rating Technique) [4] method, which is introduced[2] according to the [5] item of the bibliography. The process has been modified by the authors several times, which made it interesting and usable also for the military-technical field and it has the following mathematical model: (1) [5]:

(1)

	A_1	A_2	$\cdots$	A_n	
C_1	$u(a_{11})$	$u(a_{12})$	$\cdots$	$u(a_{1n})$	w_1
C_2	$u(a_{21})$	$u(a_{22})$	$\cdots$	$u(a_{2n})$	w_2
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
C_m	$u(a_{m1})$	$u(a_{m2})$	$\cdots$	$u(a_{mn})$	w_m
	y_1	y_2	$\cdots$	y_n	

$$y_j = \sum_{i=1}^{n} w_i u_j(a_{ij})\ u_{(x)} \in [0;100]\ \ a \in R$$

where:

- C_i - the i^{th} criterion,
- A_j - the j^{th} alternative,
- a_{ij} - the value of j^{th} alternative according to i^{th} criterion,
- u_i - the i^{th} criterion utility function,
- w_i - the weight number indicating the importance of the i^{th} criterion.

According to the summary of the model the y_i value in the (1) model is the weighted average as per weight numbers of the alternatives' usefulness per criterion.

[2] VSE (Vehicle Slop Elavation) that describes the ability to conquer macro obstacles [9].

The amount of usefulness of the alternatives as per a criterion can be visually demonstrated by plotting the utility functions in a frame of reference indicating the minimum and maximum usefulness. The process consists of eight steps:

a) the identification of the decision maker,
b) the identification of the alternatives,
c) the definition of the criteria (criteria that can be numerically valued and that plays an effective role from the mission implementation point of view when using a device should be chosen),
d) definition of the criteria's utility functions (it is useful to define linear functions, which are good for illustrating the difference between the usefulness of the devices),
e) selection of the weight numbers (the priority of the criteria compared to each other can be defined experientially),
f) the calculation of the alternatives' values.

The devices and the criteria get listed in a decision matrix. The results define the overal effectiveness of the devices. The results can also be compared on the basis of economic criteria. Since no suitable data is available, no such analysis has been carried out.

The identification of the decision maker (a)

In this case the decision maker is the assigned commander. The best alternative is chosen by the decision maker.

Examined vehicle types as possible alternatives (b)

In this case the alternatives are made up of the off-road vehicle types accepted for use at the Hungarian Defence Forces:

- Uaz 469 B
- Opel Fontera
- Mercedes G270
- Mercedes G280

All four are off-road vehicles. All of them have approach angles, departure angles and ground clearance that have been configured according to the requirements of the off-road usage. The vehicles have either permanent or part-time 4WD. The technical data can be found in table

	Uaz 469 B	**Opel Frontera**	**Mercedes G 270**	**Mercedes G 280**
engine performance: P (kW)	53	85	115	135
engine torque: M (Nm)	170	260	400	410
weight: m (kg)	1600	1920	2540	2540
total weight (kg)	2300	2600	3500	3500
specific performance (kW/t)	22	32,8	32,8	38,7
number of passengers	7	5	5	5

1. table. Technical data [6] [7] [8]

Criteria and utility functions (c,d)

The introduction of the criteria should not always be separated from the definition of the utility functions belonging to them. In case of separation the logic of the criteria's selection would become harder to trace. The chosen criteria:

- ergonomics (it defines the pressure affecting the driver),
- passenger transport capacity (in case of disaster management tasks how many people can be transported with one vehicle),
- tactical mobility (capability to to move in difficult terrain),
- reliability (the result of task execution depends on the reliability of the vehicle).

Ergonomics: The extent of pressure affecting the driver is significantly important from his point of view. Working in a constantly disturbing, uncomfortable environment can lead to concentration problems. This can have a tragic outcome in case of emergency. In case of any unexpected situations or accidental driving mistakes the fast reaction of the driver can be the key to the successful task execution. It should also be taken into consideration that the tiring conditions also affect the performance of the executive force.

The usefulness of the vehicle can be defined with scoring. In this case "0" usefulness occurs when the instrument does not have any conditions belonging to the given criterion. The vehicle having the worst features, but possessing the condition can gain 1 point at the measurement, while the vehicle with the best features can gain 3 points.

When designing the Uaz 469 B, ergonomics was not considered important, so it clearly lags behind the level of modern vehicles. The Mercedes G 270 and 280 are on the same level, while the Opel Frontera is closest to a modern car in terms of comfort. In respect of ergonomics the amount of generated vibration affecting the driver is determinant. The amount of this can be defined with numbers by the "K" ride comfort indicator in the VDI 2057 standard. Since this data is not available, a definition that makes it possible to differentiate between given alternatives needs to be worked out. Our knowledge resulting from the usage of the types is not measurable data, it cannot be used. Such measurable or definable statements, features and data are needed which can be expressed with numbers and be used to determine the usefulness. The chosen sub-criteria:

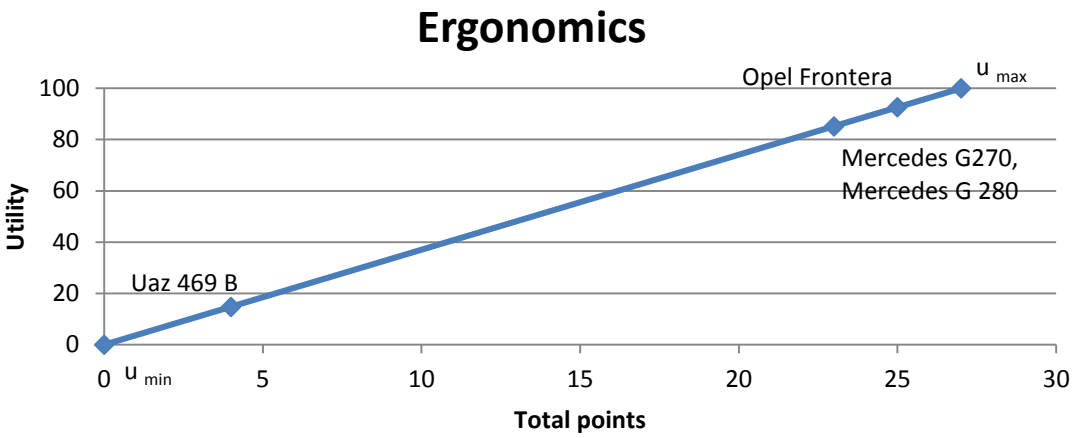
- driver's seat (adjustable height, adjustable back, arm-rest, headrest),
- the possibility to simply open the back door,
- the possibility to adjust the steering wheel,
- the existence of parking heater,
- the existence of air-conditioning[3]

The quality of the driver's seat consists of more criteria, on the basis of which the order can be set up with simple scoring (table 2).

	Uaz 469 B	**Opel Frontera**	**Mercedes G270**	**Mercedes G280**
adjustable seat	0	3	3	3
seat flexibility	1	3	3	3
adjustable back rest	1	3	3	3
headboard	0	3	3	3
seat side supports	1	3	2	2
adjustable steering	0	3	2	2
stationary heating	1	1	3	3
air conditioning	0	3	3	3
automatic turn signal	0	3	3	3
total points	4	25	23	23

2. table. Criteria of seat configuration

[3] Beside convenience criteria the air-conditioning system also has significance in terms of security. It can dehumidify the windshield in case of hazy, rainy weather conditions.

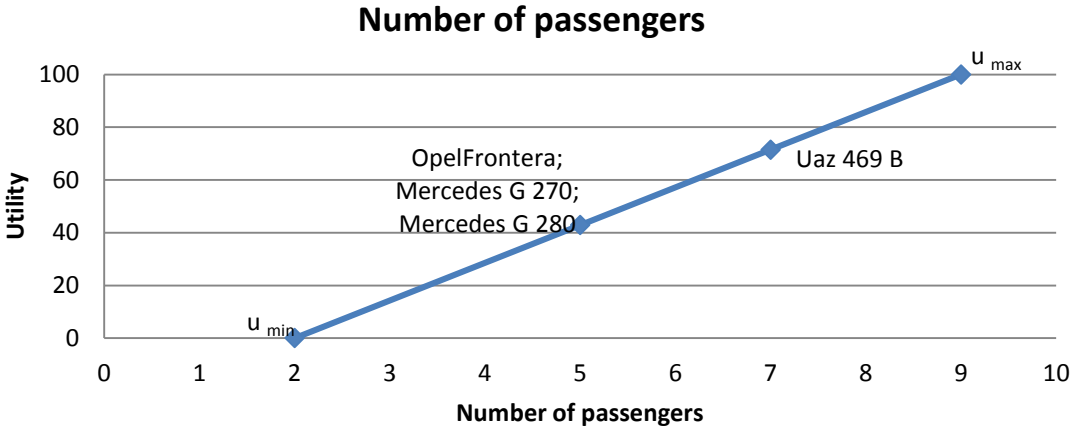


1. figure. Ergonomics

The utility function of the ergonomic criterion:

$$u(x) = \frac{100}{27}x$$

Passenger transport capacity: The seating capacity enabling passenger transportation essentially defines the degree of vehicle usability in case of task execution. When such vehicles are used in populated, disaster struck areas, the possibility of unforeseen disaster management tasks (such as people rescue) always needs to be taken into consideration. This question needs to be highlighted when determining the weight number and applying the comparison method. The least useful and the most useful parameters also need to be defined, which would be 2 and 9 in this case. 2 persons means of course 1 personnel and 1 transportable passenger, 9 is the number of maximum transportable people including the driver in case of vehicles that can be driven with category "B" driver's license. The usefulness of the alternatives with respect to the passenger transport capacity is displayed by figure 2.



2. figure. Number of passengers

The utility function of the passenger transport capacity criterion:

$$u(x) = \frac{100}{7}(x-2)$$

Tactical mobility: The vehicle mobility can be described with several well-definable parameters. The mobility can be measured with the help of speed, acceleration, ability to overcome obstacles, portability on the battlefield, manoeuvre capability and performance. The

disaster recovery activities clearly differ from the operational field activities in the fact that the defence capabilities of the vehicles play a less important role.

The required technical data is displayed in table 1. There are many factors that highly influence the mobility from the marching performance point of view and the most important is a specific performance (the amount of engine power per ton correlated to the weight of the vehicle) considering our examination.

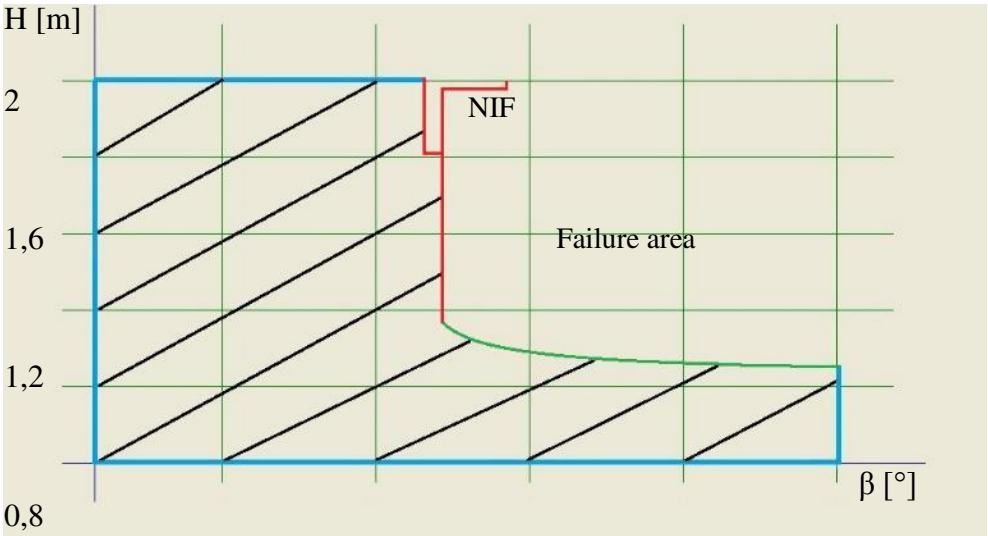
The most beneficial of these for us is the specific performance that reflects the ascending conquering capability.

The off-road capability of the vehicle is one of the most important requirements of military usage [9]. The VSE diagrams should be used for this purpose, for this process best illustrates the ability to overcome macro obstacles (graph 1). The obstacles that can be overcome by the vehicle are shown with the ruled field below the diagram. This means that neither the front nor the back console suffers any collision and the ground clearance is enough for the bottom of the vehicle to avoid the obstacles. The OMN (Obstacles Mobility Number) value can be determined by integral calculus on the basis of the given interval defined by the VSE chart [10]. The larger this value is, the better the ability is to overcome macro obstacles.

The diagram can be divided into two parts:

- NIF (Nose In Failure): the obctacle height that can be overcome with the front and back consoles is shown with the red lines,
- HUF (Hang Up Failure): the green coloured border-curve of the vehicle bottom collision.

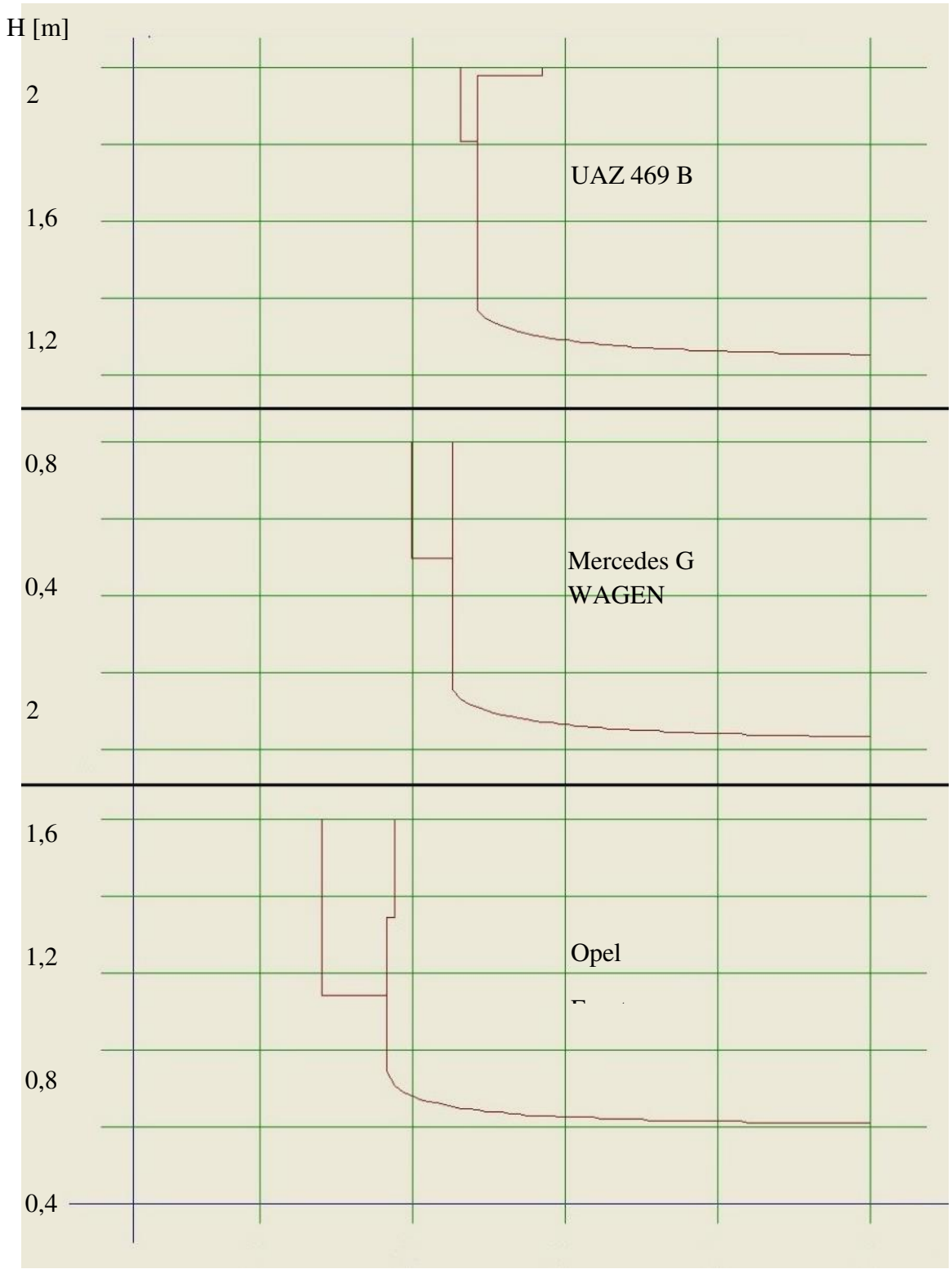
The H_{max} height is 2 metres, the angle of the obstacle's profile facing the vehicle's direction is 90° .



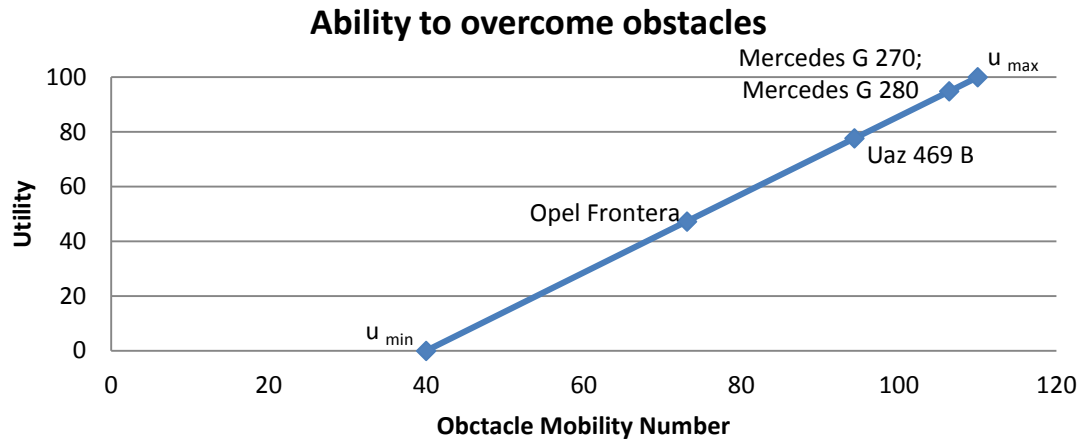
3. figure. Illustration the VSE curve

The VSE diagrams (figure 3) show the capability to overcome obstacles of the examined vehicle and also illustrate the difference between the compared vehicles.

The diagram of the Uaz 469 B and the Mercedes G 270 differ in the field of the NIF a little bit. The Opel Frontera's HUF curve that starts at a smaller angle value clearly indicates the possibility of getting stuck (graph 2). The program VSE for Windows 4.0 that edited the curves of the HUF and NIF functions was used to calculate the OMN numbers [11]. Defining the usefulness needs the minimum and maximum utility parameters. It is practical to set the OMN value of an average car as the minimum utility value, which is 40 in this case. The maximum value is that of the Unimog, which is 110 here.



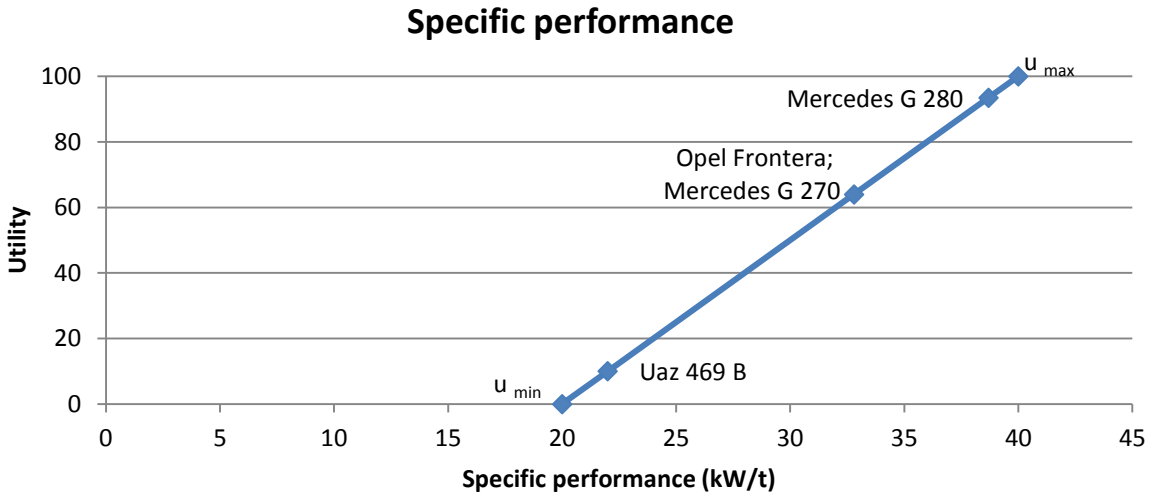
4. figure. Longitudinal VSE diagram of UAZ 469 B, Opel Frontera and of Mercedes G Wagen (short-wheelbase version)



5. figure. Ability to overcome obstacles

The utility function of the capability to overcome obstacles:

$$u(x) = \frac{10}{7}(x - 40)$$



6. figure. **Specific performance**

The utility function of the specific performance:

$$u(x) = \frac{10}{4}(x - 20)$$

The two main criteria of tactical mobility are marked as the two separate criteria of the SMART process. Determining a common score is possible but this is the simpler way.

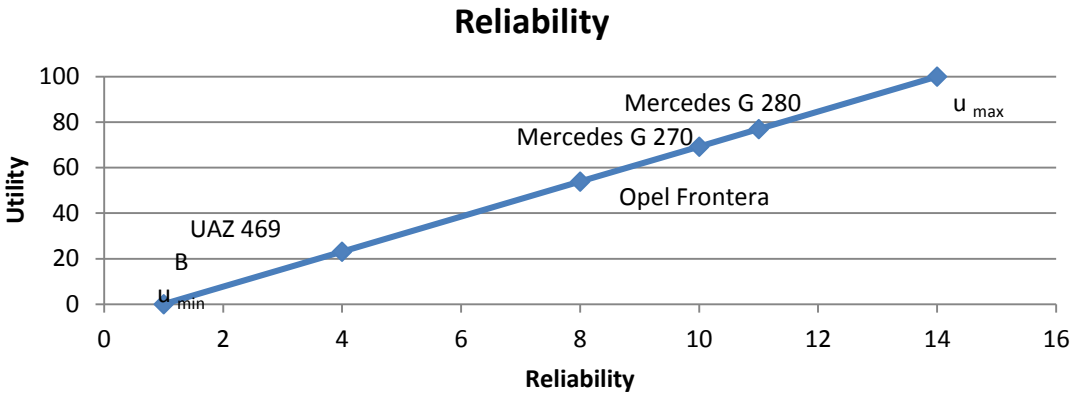
Reliability: When examining the usefulness, the question of reliability also needs to be taken into consideration. The age of the instruments affects the failure inclination. In this case the sensitivity of a modern diesel engine can bear a risk for the operational circumstances, just like an ignition problem in case of an older vehicle. In case of modern instruments such electronic or contact failures can occur that result in the engine commanding system restraining the engine's performance. If the endurance of the engine parts or the emission value of the exhaust fumes gets endangered, it is possible to go on with emergency operation even with limited engine performance.

In case of frequently and much used vehicles the preparedness of the operating personnel is the key that helps to restore the combat-readiness within a short time when making smaller reparations.

There is no precise data available for the measurement of reliability, so such features need to be defined that make it possible to compare the examined vehicles based on this criterion. Although no precise definition is possible regarding the field of reliability in this case, it would be a mistake to ignore this criterion. If the vehicle does not have the conditions required for the criterion it receives 0 points. The newest vehicle receives 10 points, the oldest gets 1 point.

	Uaz 469 B	Opel Frontera	Mercedes G 270	Mercedes G 280
engine oil pressure gauge	1	0	0	0
engine temperature gauge	1	1	1	1
engine oil temperature gauge	1	0	0	0
emergency mode	0	0	1	1
age	1	7	8	9
total points	4	8	10	11

3. table. Reliability affecting factors



7. figure. Reliability

The utility function of reliability criterion:

$$u(x) = \frac{100}{13}(x - 1)$$

Definition of the weight numbers (e)

Defining the weight number has a determinant significance regarding the result of the comparison. In case we would like to define the usefulness on the operational field it is practical to evaluate the experiences of the operating staff with the help of a survey. Although the questionnaires count as experimental results, they are still not of the same value as the exactly measurable reality. This data needs to be based on the original primary data collection.

The table 4 contains the chosen weight numbers which have been defined on the basis of estimation.

Definition of the values (f)

criteria	Uaz 469 B	Opel Fronrea	Mercedes G 270	Mercedes G 280	utility function	w. n.[4]
ergonomics	14,81	92,59	85,18	85,18	$u(x) = \frac{100}{27}x$	1
number of passengers	71,43	42,86	42,86	42,86	$u(x) = \frac{100}{7}(x-2)$	4
VSE	94,86	47,28	77,66	77,66	$f(x) = \frac{10}{7}(x-40)$	3
specific performance	10	64	64	93,5	$u(x) = 5(x-20)$	2
reliability	23,07	53,84	69,92	76,92	$u(x) = \frac{100}{13}(x-1)$	3
result	674,2	695,39	827,36	907,39		

4. table. Determining of the score

The weight numbers that are the result of the process can be found in the lower row of the table 4. The oldest vehicle has the least usefulness based on the chosen criteria and the evaluation method.

SUMMARY

The topic of the publication is the application of a decision theory. The presentation is possible through a theoretical example without the precise definition of the weight numbers. The alternatives' usefulness can be defined based on the listed criteria. This examination is an attempt to make a list of the usefulness of the off-road vehicles. The criteria were chosen entirely on the basis of real demands. Diagram illustrations clearly show the difference between the alternatives in case of all criteria. The question of the weight numbers is a critical point that can only be made entirely official with a much bigger research work. The last step of the SMART process would be the sensitivity test which has not been executed in this case. It is essential to create questionnaires that would make it possible to define precise weight numbers with the help of the information gained from the operating staff.

References:

[1] C. Burgha - Structuring and Weighting Criteria in Multi Criteria Decision Making (MCDM) http://www.researchgate.net/publication/251780347_Structuring_and_Weighting_Criteria_in_Multi_Criteria_Decision_Making_%28MCDM%29 (letöltve: 2014.01.21)

[2] Gyarmati József – Döntési modell kialakítása közbeszerzési eljárás során, Hadmérnök II. Évfolyam 3. szám - 2007. szeptember pp. 36-52

[3] Dr. Gyarmati József - Haditechnikai eszközök összehasonlítása közbeszerzési eljárás során Hadmérnök, I. évfolyam 2. szám 2006.

[4] Temesi József - A döntéselmélet alapjai Aula kiadó, Budapest 2002 ISBN 9639345644

[5] Dr. Gyarmati József – SMART, a többszempontú döntési probléma egy egyszerű megoldása, Hadmérnök III. Évfolyam 2. szám - 2008. június pp. 78-87

[6] Az UAZ 469B típusú terepjáró személygépkocsi anyagismereti és igénybevételi szakutasítása GJMŰ/126

[4] weight number

[7] Oktatási Segédlet a Magyar Honvédség gépjárművezetői állománya részére (MBG 270 CDI gépjármű típus ismeret szaktanfolyam)

[8] http://katalogus.hasznaltauto.hu/opel/frontera_2.2_dti_limited_aut.-2018770 (2103.04.24)

[9] Vartman György - Járművek akadályleküzdő képességének összehasonlítása a VSE módszer alkalmazásával, http://portal.zmne.hu/download/konyvtar/digitgy/nek/2003_2/14_vartman.pdf (2013.04.23)

[10] Dr. Laib Lajos - Terepen mozgó járművek Szaktudás Kiadó Ház 2002 Budapest ISBN 9639422010

[11] VSE for Windows 4.0 szoftver használati utasítás

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Bodoróczki János
bodoroczkijanos@gmail.com

U. S. ARMY SPECIAL OPERATIONS SUSTAINMENT

Abstract

First, the article presents an overview of Special Forces Sustainment. Such as: Army Sustainment Structure, Principle of Sustainment, and logistic imperatives. Next chapter gives some general ideas about army special operations forces logistics support framework: For example: structures, relationship, planning and preparation. Last but not least the author gives a summary about Sustainment Brigade, Special Forces groups, Health System Support, Contracting – and host nation support. This publication proposes an approach, and a concept for Sustainment of Special Forces and summarizes the ATP 3-05.40, former FM 3-05.140

Az első fejezetben a cikk áttekintést nyújt a különleges erők támogatásáról úgy, mint az Egyesült Államok szárazföldi haderőnem fenntartási struktúráról, a fenntartási alapelvekről, és a logisztikai alapelvekről. A következő fejezet rövid átfogó képet nyújt a szárazföldi haderőnem különleges erői támogatási kereteiről – struktúráról, kapcsolatokról, tervezésről, felkészítésről. Végül, de ne utolsó sorban a szerző összegzést nyújt a különlegese erőket közvetlenül támogató dandárról, a különleges erők néhány csoportjáról, az egészségügyi támogatásról, a befogadó nemzeti támogatásról. E publikáció egyfajta nézőpontot, illetve koncepciót ajánl a különleges erők támogatására, összegzi az ATP 3-05.40 (a korábbi FM 3-05.140) számú kiadványt.

Keywords: *Special Forces, Logistic, Support, Sustainment ~ különleges erők, logisztika, támogatás, fenntartás*

INTRODUCTION

The United States armed forces – especially Special Forces - are transitioning from more than a decade of war to a future that presents us with a range of challenges. There are major changes in security policy and war strategy over the past 18 months. Changes combined with fiscal uncertainty. It means that we must re-think how the Army sustains itself in the war today, or how the Army sustains itself in a next conflict. Nowadays every operation requires discreet, precise, operations. These are special operation forces core principles. Discreet, precise, operations provide the combatant commander a flexible military power in politically sensitive and culturally complex environments. These operations represent a combination of precise lethal and nonlethal options from direct action to civil affair operation. This kind of operations may enhance the legitimacy of partners because the capability is applied in a discreet manner. Special operation missions may require unorthodox approach, but this approach does not negate the principles of war: objective, offensive, mass, economy of force, maneuver, and unity of command, security, surprise, and simplicity. [1] Achievement of Special Forces depends on an effective Sustainment. The key document of the Special Operations Sustainment is the ATP 3-05.40, former FM 3-05.140. The ATP 3-05.40 proposes an approach and a concept for Sustainment of Special Forces. This Technique Publication provides the United States Army special operations forces commander and staff information on the structure and functions involved in Sustainment activities. [15]

OVERVIEW OF SUSTAINMENT

The type of operation, the deployment sequence, and the area of responsibility character the logistics environment of Army Special Operation Forces. The common line that runs throughout the environment is the problem of logistics integration and distribution to committed Army Special Operation Forces (ARSOF)[2]. [16] For the Army, Sustainment is the provision of logistics, personnel services, and health services support necessary to maintain operations. [3] [17]

Army Sustainment

Army Special Operation Forces Sustainment structures provide all functions to support missions. These kinds of structures are performing the following tasks:

- Expeditionary missions.
- Deploy early and rapidly.
- Collocate support unit.
- Fill logistical requirements.
- Provide effective operations logistics structures.
- Tie the Army Special Operation units to the operational theater of operations support structure.

Army common-user logistics is the responsibility of the theater of operations Army Service component commands. Army Special Operation rely upon Army Service component commands logistics structures to provide Service common user logistic to all Army forces in the area of operations. ARSOF units lack the robust logistics structure associated with Army. Operational logistics planning is critical to mission success and the ability of Special Operation

[1] JP 3-0, Joint Operations, Joint Chief of Staff, 2011, Chapter 1, Figure I-1: Principles of Joint Operations, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf, Download: (10. February 2014.)
[2] FM 3-05 (FM 100-25) Army Special Operations Forces, Headquarters, Department of the Army, 2006, Ch. 8
[3] ADP 4-0 (FM 4-0) Sustainment, Headquarters, Department of the Army, 2012, pp 1, https://armypubs.us.army.mil/doctrine/index.html, Download: (9. February 2014.)

sustainment requirements. ARSOF units operate under the c2 of theater special operations commands. Operational logistics planning begins with the theater special operations command's joint operations. Army special operations forces liaison elements develop the corresponding operational-level support and logistics requirements for SOF requirements. These liaison elements are in the 528th Sustainment Brigade (Special Operations) (Airborne). This deployable sustainment unit focuses on operational-level logistics planning and synchronization. The organization's mission is to provide operational-level sustainment for ARSOF missions. Every Special Forces group has a group support battalion, with a subordinate sustainment company, a maintenance company, a medical company, and three forward support companies. Each Special Forces battalion is supported by a forward support companies. These battalions are a multifunctional, direct-support logistical organization. This kind of subunit is a key of tactical ARSOF logistics. The responsibility of the Group Support Battalion is to plan, coordinate, and execute logistical sustainment operations. The 75th Ranger Regiment's mission is to plan and conduct Special Operations against strategic and operational targets. The regiment consists of a regimental headquarters, a Ranger Special Troops Battalion, and three Rangers. The Ranger Special Troops Battalion provides staff planning and supervision for all logistics in the regiment. The Army Special Operations Aviation Command mission is to equip, train, validate, conduct, and support special air operations. The Civil Affair mission is to appoint and influence the civil populace by planning, executing, and transitioning Civil Affairs operations, and multinational operations. The special operations acquisition and logistics center is a key staff element in support of ARSOF logistics. This staff section plans, coordinates, synchronizes, and integrates operational and strategic logistics and acquisition sustainment strategy in coordination with combatant commands, Services, components, and other agencies. 4 [1]

Principles of sustainment

The principles of sustainment are critical to guiding the success of generating combat power. These principles are the following: anticipation, responsiveness, simplicity, economy, survivability, continuity, improvisation, and integration. Sustaining of special operation missions is important to success.

- *Anticipation:* It means to foresee future operations and events identify the right support to sustain the force. Sustainment planners anticipate future events and requirements. Anticipation is enhances endurance.
- *Responsiveness* is the ability to meet changing requirements on short notice. It is providing the right support in the right place at the right time, and it includes the ability to see operational requirements. A responsive sustainment system is critical; it provides the ARSOF commander with flexibility and freedom of action.
- *Simplicity* is a minimum of complexity in logistics operations. It enables economy and efficiency of sustainment resources, ensuring effective sustainment operations. Simplicity is the most important key principles to sustainment mission success, because of size and nature of special operation missions.
- *Economy:* It means to provide effective sustainment using the fewest resources within acceptable levels of risk. Every resource is always limited. The commander achieves economy by prioritizing and allocating resources.
- *Survivability* is the ability to protect sustainment functions from destruction. Survivability is a function of protection. It consists of prevent or lessen hostile actions against personnel, resources, facilities, and critical information.

[4] ATP 3-05.40 (FM 3-05.140) - Special Operations Sustainment, Headquarters, Department of the Army, 2012, Chapter 1, pp 1-5, https://armypubs.us.army.mil/doctrine/index.html, (Download: 02. February 2014.)

- *Continuity:* It is the ability to maintain nonstop support during all phases of operations. Continuity is essential to strategic and operational reach.
- *Improvisation* is the ability to adapt sustainment to changing situations or missions. Every high-tech operational environment requires sustainment soldiers must quick use any means possible to maintain a continuous operation.[5]
- "*Integration* is the most critical principle. It is the deliberate coordination and synchronization of sustainment within any operation and at each level of war. ARSOF integrate their sustainment operations with other components of the joint force to benefit from each Service component's competencies and resources. Integration requires a thorough understanding of the commander's intent and synchronization of sustainment with the concept of operations. Integration of sustainment with joint forces (joint interdependence) allows efficiencies through economies of scale. It ensures the highest priorities of the joint force are met first and avoids redundancy. It also eliminates wasteful competition for scarce strategic-lift and theater of operations resources." [6]

Sustainment Warfighting function

Sustainment is the comprehensive term. It covers the functions of logistics, personnel services, and health service support. The sustainment Warfighting function is one of six Army Warfighting functions. The Warfighting functions of the Army are the following:

- movement and maneuver,
- fires,
- protection,
- sustainment,
- mission command,
- Intelligence.

These functions are producing combat power. Sustainment Warfighting function is a related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance [7] This chapter is about Warfighting functions.

Sustainment Warfighting functions are the following:

- Logistics - Planning and executing the movement and support of forces. It includes "military operations that deal with design and development, acquisition, storage, movement, distribution, maintenance, evacuation, and disposition of materiel; movement, evacuation, and hospitalization of personnel; acquisition or construction, maintenance, operation, and disposition of facilities; and acquisition or furnishing of services. " [8] [18]
- Supply – "Supply is the procurement, distribution, maintenance while in storage, and salvage of supplies, including the determination of kind and quantity of supplies." [9]
- Field services - Clothing repair and exchange, laundry, shower, mortuary affairs, aerial delivery, food services, etc.
- Maintenance – two level of maintenance: Field and Sustainment maintenance. It consists of inspection, testing, servicing, repair, rebuilding etc.

---

[5] ATP 3-05.40 Chapter 1, pp 5-6
[6] ATP 3-05.40 Chapter 1, pp 6
[7] ADP 3-0, Unified Land Operations, Headquarters, Department of the Army, 2012, Sustainment Warfighting Function, pp 44, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp3_0.pdf, (Download: 10. February 2014.)
[8] JP 4-0 Joint Logistic, Joint Chief of Staff, 2008, pp 120
[9] ATP 3-05.40, Chapter 1, pp 7

- Transportation – It includes motor, rail, air, and water modes. [10] [5]
- General engineering – General engineering support is other than combat engineering, it includes modify, maintain, or protect the physical environment. [11] [6]
- Operational contact support – Is a kind of planning for supplies from profitable sources in support of operations along with the contractors. [12] [7]
- Management functions.
- Personnel Services - human resources support, financial management, legal support, religious support.
- Human Resources Support - personnel readiness management, personnel accountability, personnel information, management, casualty operations, essential personnel services, band support, postal operations, reception, replacement, return-to-duty, etc. [13] [9]
- Financial management - finance operations, resource management. [14] [10]
- Legal Support - Legal support includes all legal services. It provides judge advocates and other legal personnel in support of units, commanders, and soldiers in an Area of Operation. [15] [11]
- Religious Support - Religious support facilitates the free exercise of religion, provides religious activities. [16] [12]
- Band Support - Army bands provide support to the force by tailoring music support throughout military operations. [17] [13]
- Health Services Support - Health service support is all services provided to promote, improve, conserve, or restore the mental or physical well-being of personnel. It also includes blood management; medical supply, equipment, operational stress control; and medical, dental, veterinary, laboratory, optometric, nutrition therapy, and medical intelligence services. [18] [14]

[10] FM 4-01.30 (FM 55-10) Movement Control, Headquarters, Department Of The Army, 2003, Chapter 1, http://cdm16635.contentdm.oclc.org/cdm/ref/collection/p16635coll8/id/55429, Download: 2014. February 10.
[11] FM 3-34.400 (FM 5-104) General Engineering, Headquarters, Department Of The Army, 2008, Chapter1 1 pp 1-12, http://www.globalsecurity.org/military/library/policy/army/fm/3-34-400/fm3-34-400.pdf (Download: 10. February 2014.)
[12] JP 4-10 Operational Contact Support, Joint Chief of Staff, 2008, pp 10: Operational Contact Support Principles http://www.dtic.mil/doctrine/new_pubs/jp4_10.pdf, (Download: 10. February 2014.)
[13] FM 1-0 Human Resources Support, Headquarters, Department of the Army, 2010, pp 15, Hr Core Competencies, http://www.ags.army.mil/Files/fm1_0.pdf (Download: 10. February 2014.)
[14] FM 1-06 Financial Management Operations, Headquarters, Department of the Army, 2011, Chapter 1, http://www.finance.army.mil/Publications/FM1_06.pdf, (Download: 10. February 2014.)
[15] FM 1-04 Legal Support to the Operational Army, Headquarters, Department of the Army, 2013, Chapter 1-2, http://www.globalsecurity.org/military/library/policy/army/fm/1-04/fm1-04_2013.pdf, (Download: 10. February 2014.)
[16] FM 1-05 Religious Support, Headquarters, Department of the Army, 2012, Chapter 1, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm1_05.pdf, (Download: 10. February 2014.)
[17] ATTP 1-19 U.S. Army Bands, Headquarters, Department of the Army, 2010, Preface, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/attp1_19.pdf, (Download: 10. February 2014.)
[18] JP 4-02 Health Service Support, Joint Chief of Staff, 2012, Executive Summary, pp 11, http://www.dtic.mil/doctrine/new_pubs/jp4_02.pdf, (Download: 10. February 2014.)

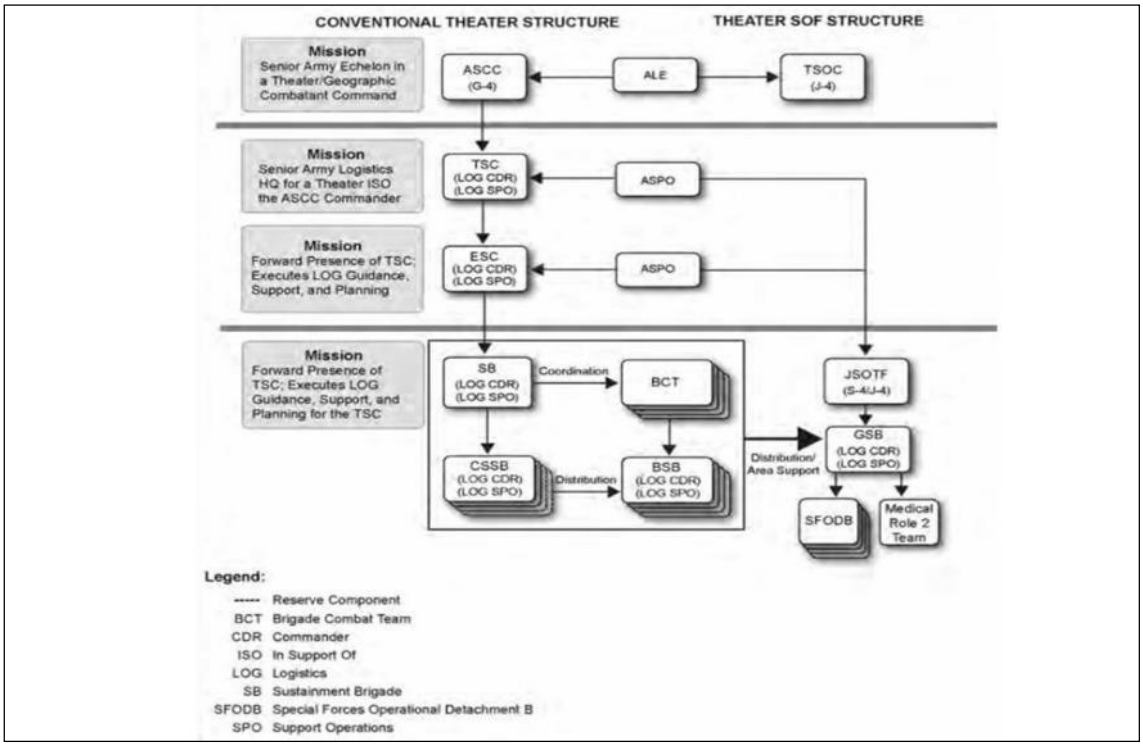
Expeditionary logistics imperatives

All of ARSOF commanders include the applicable imperatives in their mission planning and execution. The Theater Special Operations Command and Special Operation Task Forces expeditionary logistics imperatives are the following:

- Understanding the operational environment: ARSOF logistics systems are flexible, globally responsive, and rapidly deployable. That's why ARSOF must to understand theater of operations dynamics, theater of operations infrastructure, and sustainment capability.
- Unity of effort: Unity of effort means the coordination and application of all logistics capabilities. It focused on Theater Special Operations Command and Special Operation Task Forces commander's intent.
- Rapid and precise response: It consists of an ability of the supply chain to effectively meet the continuously changing needs of the task force.[19]
- Domain-wide visibility: Domain-wide visibility is the ability to see the requirements, resources, and capabilities across the logistics, both SOF and Army.

ARMY SUPPORT STRUCTURE, RELATIONSHIP

ARSOF operating and logistical structures differ greatly from Army conventional forces. The Special Forces Groups are the only units that have any type of organic direct support capability. Direct support capability is the group support battalion. There is a typical ARSOF sustainment structure on figure 1.



1. figure. Typical ARSOF sustainment structure[20]

[19] ATP 3-05.40 Chapter 1, pp 6-10
[20] Authority: FM 3-05.40, Chapter 2, pp 3, Figure 2-1

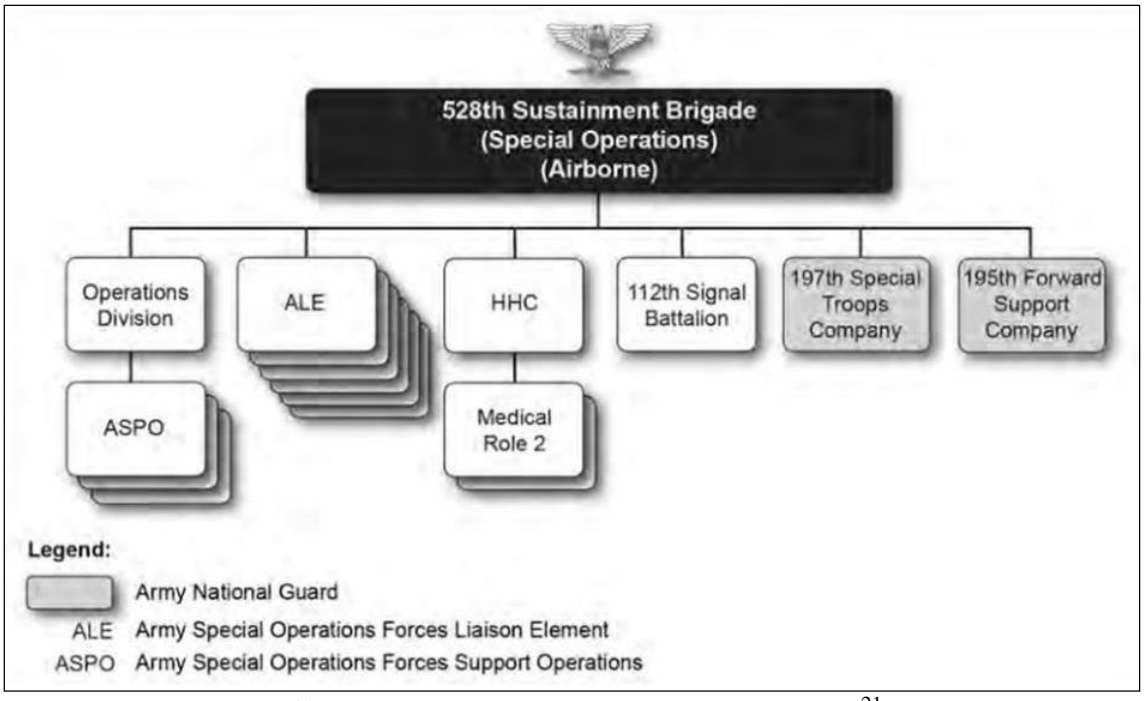
SUSTAINMENT BRIGADE

The 528th SB(SO)(A) is unique when compared to other Army sustainment brigades. It maintains global situational awareness of sustainment support structures. This sustainment brigade is formed to deploy small, modular teams. It also designed to provide senior logistics unit for an ARSOF-led Joint Special Operation Task Forces. The brigade staff is organized to plan support for deployed ARSOF teams. Brigade staff structure includes Army special operations forces liaison elements, beside the Army Service component command and the theater special operations command. This kind of liaison elements, are small teams of multifunctional logisticians. This element can offer direct support of theater special operations command planning efforts, exercises, and ARSOF operations. Alongside liaison elements, the brigade HQ includes an Operations Division. It comprised of a plans section and a support operations section. The mission of the 528th Sustainment Brigade is to originate the operational-level logistics conditions for ARSOF missions. The mission-essential tasks are the following:

Coordinate ARSOF logistics requirements:

- Deploy operational-level logistics,
- Deploy a tailored brigade HQ.

Figure no. 2 shows the organization of sustainment brigade.



2. figure. Organization of Sustainment brigade[21]

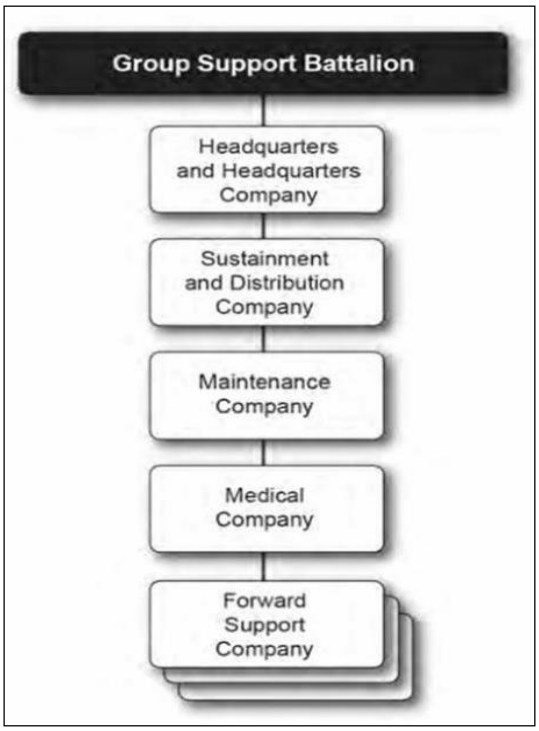
OVERVIEW OF SPECIAL FORCES SUSTAINMENT

SF detachments need to plan for a different of operations. It includes humanitarian, civil, and security assistance programs. Deployed Special Forces are usually isolated. Under their activity, the primary logistics provider is the Group Support Battalion.[22]

[21] Authority: FM 3-05.40, Chapter 3, pp 3, Figure 3-2
[22] ATP 3-05.40 Chapter 4, pp 1-4

Group Support Battalion

Group Support Battalion mission is to plan, coordinate, synchronize, and execute logistics operations for Special Forces Groups and Joint Special Operation Task Forces. If logistics support is not available in the Area of Operation, the Group Support Battalion is the primary support provider. Battalion provides rapidly deployable multifunctional logistics, health service support and force health protection. In area of operations, the battalion synchronizes its support with the conventional forces and coordinates with conventional force sustainment brigades. Forward support companies require Army logistics to provide logistics support during sustained operations. The battalion controls logistical facilities and sustainment operations. The headquarters and headquarters company of the GSB provides battalion-level administrative and supply support for all personnel. It also coordinates support for the SF battalions through the support operations section. Next picture shows the organization of Group Support Battalion.



3. figure. Organization of Group Support Battalion[23]

SUMMARY - CONCLUSION

United States Army Special Operation Forces has own support, and sustainment capability such as: Sustainment Brigade, Group Support Battalion, liaison element etc. This capacity provides rapidly deployable multifunctional logistic system. This kind of support system and capabilities are not available for every NATO member nation's SOF detachment.

References

[1] ATP 3-05.40 (FM 3-05.140) - Special Operations Sustainment, Headquarters, Department of the Army, 2012

[2] ADP 3-0, Unified Land Operations, Headquarters, Department of the Army, 2012

[3] JP 4-0 Joint Logistic, Joint Chief of Staff, 2008

[23] Authority: FM 3-05.40, Chapter 4, pp 3, Figure 4-1

[4] ADRP 4-0 Sustainment, Washington, DC, Headquarters, Department of the Army, 2012

[5] FM 4-01.30 (FM 55-10) Movement Control, Headquarters, Department Of The Army, 2003

[6] FM 3-34.400 (FM 5-104) General Engineering, Headquarters, Department Of The Army, 2008

[7] JP 4-10 Operational Contract Support, Joint Chief of Staff, 2008

[8] ATTP 4-10 (FM 3-100.21) Operational Contract Support Tactics, Techniques, And Procedures, Headquarters, Department of the Army, 2011

[9] FM 1-0 Human Resources Support, Headquarters, Department of the Army, 2010

[10] FM 1-06 Financial Management Operations, Headquarters, Department of the Army, 2011

[11] FM 1-04 Legal Support To The Operational Army, Headquarters, Department of the Army, 2013

[12] FM 1-05 Religious Support, Headquarters, Department of the Army, 2012

[13] ATTP 1-19 U.S. Army Bands, Headquarters, Department of the Army, 2010

[14] JP 4-02 Health Service Support, Joint Chief of Staff, 2012

[15] JP 3-0, Joint Operations, Joint Chief of Staff, 2011

[16] FM 3-05 (FM 100-25) Army Special Operations Forces, Headquarters, Department of the Army, 2006

[17] ADP 4-0 (FM 4-0) Sustainment, Headquarters, Department of the Army, 2012

[18] JP 4-0 Joint Logistic, Joint Chief of Staff, 2008

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Derzsényi Attila
attila.derzsenyi@hm.gov.hu

KATONAI BESZERZÉS I.
A KÖZBESZERZÉS, (KÖZ)BESZERZÉS, BESZERZÉS RENDSZERE

Absztrakt

A katonai beszerzésről sokaknak első hallásra a haditechnikai eszközök beszerzése jut eszébe, míg mások úgy vélik, hogy ez a közbeszerzés egy sajátos területe. Az idegen nyelvű fordításokban is előszeretettel használják a katonai beszerzés kifejezést a védelmi beszerzésekre1 vonatkozóan. A honvédség ellátásának biztosítása a beszerzéseken keresztül azonban ennél sokkal összetettebb, kiterjed a jogszabályi előírásokon kívül a speciális szabályozásokra, NATO, valamint Európai Uniós előírásokra is.

Many of the military procurement in the military assets may sound comes to mind, while others believe that it is a particular area of public procurement. Foreign-language translations are often used by the military procurement for the defense procurement contracts. The supply of the army through the acquisition, however, is much more complex, in addition to the regulatory requirements covers the special regulations in the European Union, NATO, as well as specifications.

Kulcsszavak: *katonai beszerzés, védelmi beszerzés, közbeszerzés ~ military procurement, defense procurement contracts, public procurement*

[1] defense procurement, defense acquisition

BEVEZETÉS

A beszerzés fogalomrendszere nem egységes sem a hazai, sem a nemzetközi szakirodalomban. Nagyon sok szinonim kifejezés terjedt el, mint például a vásárlás, az ellátás, az anyaggazdálkodás. A beszerzés általános definíciója szerint:

Beszerzés alatt értünk minden olyan tevékenységet, amelynek az a célja, hogy egy adott szervezetet mindazokkal a javakkal ellásson, amelyekre a szervezetnek szüksége van működése fenntartásához, és amelyeket nem saját maga állít elő."[2]

A beszerzés kifejezés a tudományos szakirodalmakban többnyire a civil logisztika, vállalati logisztika részeként kerül értelmezésre:

A beszerzés tehát jelenti egyrészt a felhasználandó (anyagok, félkész-, késztermékek, és ezekhez kapcsolódó információk) erőforrások megszerzésére irányuló tevékenységet, másrészt pedig azt a szervezetet, amely e feladat ellátásával foglalkozik.[3]

A hazai szakirodalmak nem foglalkoznak a katonai beszerzés definíciójával, valamint a honvédségi beszerzések értelmezése sem egységes. A beszerzéssel kapcsolatos oktatás a közbeszerzés joganyagára és az Európai Unió szabályozására korlátozódik. A katonai beszerzéssel összefüggő képzés kizárólag a honvédelmi tárca központi beszerző szervezeténél folyik, amely jelenleg inkább a gyakorlati tapasztalatok átadását jelenti. A beszerzés katonai vonatkozású további kutatása azonban nélkülözhetetlen az erre vonatkozó alapfogalmak, definíciók nélkül.

A cikkben kísérletet teszek a honvédségi (katonai) beszerzésre vonatkozó ismeretanyag rendszerezésére, valamint ismertetem, csoportosítom a honvédség által alkalmazott beszerzési típusokat. Mindezek eredményeként megalkotom a katonai beszerzés definícióját.

A definíció bizonyítása érdekében feldolgozom a jelenleg hatályos honvédségi beszerzésekkel foglalkozó jogszabályokat, utasítások, szakcikkeket kiegészítve a gyakorlati tapasztalataimmal. Az írás első része a katonai beszerzés hátterét valamint a jogszabályi rendelkezések feldolgozását tartalmazza. A második részben a honvédségi beszerzéssel foglalkozó utasítások, intézkedéseket mutatom be, melynek eredményeként a definíció javaslatot teszek.

KATONAI BESZERZÉS HÁTTERE

A rendszerváltást követően mind a katonai logisztika rendszere, mind a közigazgatás, ezen belül a haderő beszerzés szabályozási rendszere, szervezeti struktúrája nagymértékben átalakult. Tendenciaként megfigyelhető a jogszabályi előírások szigorodása, ezzel párhuzamosan pedig a beszerzés centralizációja.

Az Európai Unió felvételi követelményrendszerében meghatározottak szerint hazánk már 1995-ben megalkotta első közbeszerzési törvényét[4][5], amely a honvédségi beszerzésekre is kötelező érvényűvé vált. Azonban csak a közbeszerzésekről szóló 1995.évi XL. törvény 1999. évi módosítása tette lehetővé, hogy a Kormány rendeletben szabályozza a nemzetbiztonsági és

[2] Széchenyi István Egyetem- LOGISZTIKAI ÉS SZÁLLÍTMÁNYOZÁSI TANSZÉK :Beszerzési logisztika http://www.sze.hu/~hirko/web/Log1%20%28Egyetem%29/Beszerz%E9si%20logisztika.pdf

[3] Szegedi Zoltán, Prezenszki József : Logisztika-menedzsment, Budapest: Kossuth,

[4] A közbeszerzésekről szóló 1995 évi LXV törvény

[5] A törvény megalkotását az is indokolta, hogy az Európai Közösséggel és a tagállamai közötti társulás létesítéséről szóló, Brüsszelben 1991 december 16-án aláírt és az 1994. évi I. törvénnyel kihirdetett Európai Megállapodás alapján fennálló jogharmonizációs kötelezettségünk többek között kiterjedt a közbeszerzésre is, továbbá hazánk már régebben tervezte a GATT kormányzati beszerzésekről szóló kódexének aláírását

titokvédelmi körbe tartozó eszközök, valamint a haditechnikai eszközök beszerzésének rendjét.[6]

Az 1999-es NATO csatlakozásunkat követően a szövetségesi katonai műveletekben történő részvétel megkövetelte új típusú haditechnikai eszközök beszerzését, amelynek egy hányadát a NATO finanszírozta. Szintén szövetségesi előírás volt a NATO finanszírozású beszerzési szabályozás átvétele, amely rendszer nagymértékben eltért a hazai beszerzési előírásoktól.

2004-től már az Európai Unió tagállamaként a közbeszerzés közösségi előírásainak átvételére került sor, azonban a védelmi beszerzéseket közösségi szinten is speciálisan került szabályozásra. 2005-ben a közösségi szabályozással összhangban átalakításra került a közbeszerzési törvény, amely azóta számtalanszor módosításra került. 2011-ben megalkotott 2011. évi CVIII törvénnyel (a továbbiakban: Kbt.), a közbeszerzés átfogó reformja a védelmi beszerzéseket is mélyen érintette.

Beszerzés vonatkozásában nem kerülhetjük meg a költségvetés kérdését. A közbeszerzés épp a központi költségvetés ésszerű felhasználását hivatott szabályozni. Vannak olyan élethelyzetek, amelyek a közpénzek ésszerű felhasználását meghaladják, fontosabbak ennél (ilyen a védelmi, nemzetbiztonsági érdekek). Ilyen helyzetekben a közbeszerzési alapelvek (pl. nyilvánosság) nem érvényesülhetnek. A Magyar Honvédség azonban nem csak a központi költségvetésből gazdálkodik, hiszen a NATO által finanszírozott feladatokra kizárólag a NATO beszerzési előírások alkalmazhatók.

Az Európai Unió meghatározott esetekben a közösségi irányelvekkel összhangban szabad kezet adott a kormányok részére, hogy önállóan alkossanak meg bizonyos beszerzési szabályokat. Napjainkra kialakult a központosított közbeszerzés, hadfelszerelés (védelmi)-, nemzetbiztonsági célú-, büntetés végrehajtási-, műveleti-, tartós külszolgálatot teljesítők ellátását célzó-, NATO biztonsági beruházási beszerzések[7], amelyek szabályait törvények, kormányrendeletek és egyéb utasítások, intézkedések a közbeszerzés szabályaitól eltérően tartalmazzák.

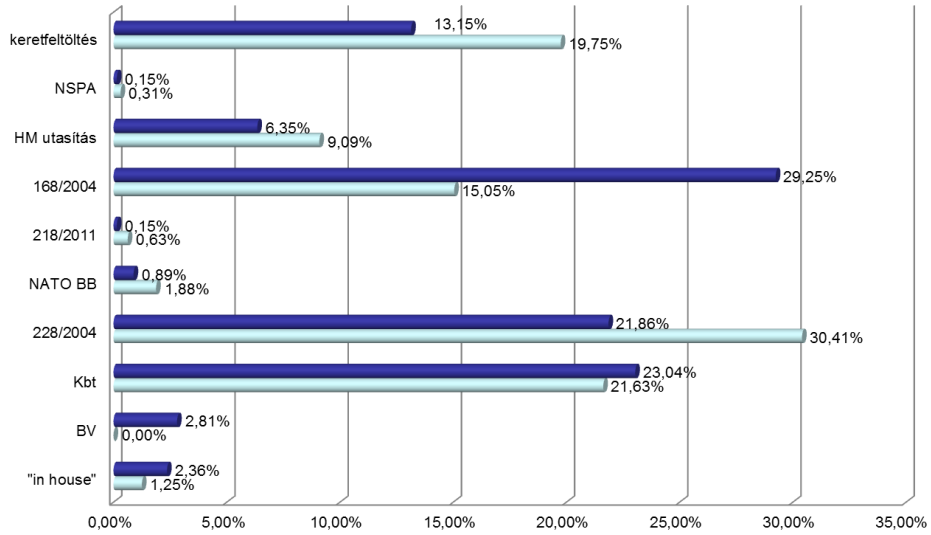
Sokakban joggal vetődhet fel a kérdés, hogy miért kell külön értelmezni, definiálni a katonai beszerzést. Amennyiben katonai beszerzésről beszélünk, akkor a katonai szervezetek beszerzését kellene vizsgálnunk. Azonban több mint 10-15 éve a katonai szervezetek csak korlátozottan rendelkeznek beszerzési jogkörrel. Helyettük a HM utasításban kijelölt központi beszerző szervezet jár el az alakulatok megbízásai alapján.

Hasonló a helyzet, amennyiben a katonai beszerzést leszűkítenénk a védelmi beszerzés fogalmára. Tény, hogy a védelmi beszerzés elsősorban a haderő sajátossága, azonban a közösségi irányelv és a hazai szabályozás is együtt kezeli a rendvédelmi, rendészeti beszerzésekkel. A védelmi irányelv katonai listája (ML) tartalmazza mindazon eszközöket és szolgáltatásokat, amit a védelmi beszerzés keretében beszerezhetőek. Annak ellenére, hogy hazai szabályozás kiegészítette a közösségi katonai listát (HUML később adod meg az értemezést.), továbbra sem tartalmaz minden katonai igényt.

A katonai beszerzés és a közbeszerzés között egyenlőséget nem vonhatunk, hiszen a közbeszerzési eljárás nyilvános lefolytatása a nemzeti minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit sértené. Ezt a közösségi irányelvek is kiemelten kezelik, ezért mind a védelmi, mind a minősített beszerzésekre eltérő szabályokat alkottak.

[6] Állami Számvevőszék 2004 novemberében készült 0451 sz jelentése „a Magyar Honvédség közbeszerzési rendszere működésének ellenőrzéséről”

[7] A felsorolás nem teljes, a cikk részletesen kitér az egyes beszerzési típusokra.



1. ábra. HM központi beszerző szervezete által lefolytatott beszerzési típusok aránya
Forrás: Katonai Beszerzési Információs Rendszer (KBIR)

A honvédelmi tárca beszerzési statisztikái[8] alapján megállapítható, hogy a közbeszerzési eljárások a katonai beszerzésnek csupán 20-25 %-át jelenti. Álláspontom szerint nem elegendő a katonai beszerzést folytató állomány részére a közbeszerzési referens képzés, mivel az kizárólag a közbeszerzési szabályokban való jártasságot segíti elő. A katonai beszerzésben annak eldöntése, hogy milyen jogszabály vagy utasítás alapján kell megindítani a beszerzést, nagyobb kihívást jelent, mint lefolytatni az eljárást.

A bevezetőben kifejtett háttér információkból kiindulva a számtalan szövetségi-, közösségi-, hazai beszerzés-közbeszerzés előírásokat célszerű megvizsgálni, rendszerezni.

KATONAI BESZERZÉS TÍPUSAI

Közbeszerzés:

A közbeszerzés egyszerű megfogalmazása szerint *a különféle szolgáltatások és fogyasztási cikkek költségvetési szervek által történő beszerzését jelenti*.[9] Ezen beszerzések közös jellemzője, hogy a finanszírozás közpénzekből történik és sokszor igen jelentős értékűek a megrendelések.

A közbeszerzés törvényi definíciója[10] szerint: *Közbeszerzési eljárást az ajánlatkérőként meghatározott szervezetek visszterhes szerződés megkötése céljából kötelesek lefolytatni megadott tárgyú és értékű beszerzések megvalósítása érdekében*.

A definícióból kiindulva kizárólag a törvényben meghatározott Ajánlatkérők folytathatnak le közbeszerzési eljárást. Annak ellenére, hogy jogszabályi előírás alapján minden honvédelmi szervezet jogosult lenne Ajánlatkérőként közbeszerzési eljárást lefolytatni, a tárca beszerzésére vonatkozó HM utasításban meghatározottak szerint ez a lehetőség igen korlátozott.

Fontos szempont a közbeszerzési értékhatár. Közbeszerzési értékhatár a közbeszerzésre kötelezett szerveknek megmutatja, hogy kell a közbeszerzési eljárást lefolytatni, és ha igen, milyen eljárásrendbe tartozik az adott beszerzés. Az értékhatár függ a közbeszerzés tárgyától is, azaz attól, hogy mit akarunk beszerezni. Ez lehet árubeszerzés, szolgáltatás megrendelés, építési beruházás, építési koncesszió, vagy szolgáltatási koncesszió.

---

[8] HM központi beszerző szervezete által 2004 óta alkalmazott Katonai Beszerzési Információs Rendszer adatai alapján.

[9] Az ügyvéd szerepe a közbeszerzési eljárásban http://www.bpugyvedikamara.hu/files/28/28147.doc.

[10] A közbeszerzésekről szóló 2011. évi CVIII. tv. 5 §

Az egyes beszerzési tárgyakra vonatkozó uniós és nemzeti értékhatárokat a Közbeszerzési Hatóság a Közbeszerzési Értesítőben és a Közbeszerzési Hatóság honlapján minden év elején elnöki tájékoztatóban teszi közzé. Az elnöki tájékoztató tartalmazza az uniós értékhatároknak a forintban kifejezett értékét is.

A közösségi szabályozás alapján meghatározott értékhatárt (közösségi) elérő beszerzés esetén a hirdetmények az EU hivatalos honlapján jelennek meg. A közösségi értékhatárt el nem érő, de a nemzeti értékhatárt meghaladó beszerzések szabályozása nemzeti feladatkör.

Nemzeti szabályozás alapján egyes termékek és szolgáltatások beszerzésére speciális eljárásrend, valamint az eljárásba épített előzetes és utólagos engedélyeztetés[11], ellenőrzés került kialakításra.

A közbeszerzés rendszerét a közpénzek felhasználásának szabályozására alakították ki alapvetően a közigazgatási szervek részére kötelező jelleggel. A közigazgatási szervek túlnyomó többsége alaprendeltetésű feladatait normál időszakban hajtja végre, belföldön.

A Magyar Honvédség vonatkozásában azonban számolni kell a külföldön (Európai Unión kívül) normál békeidőszaktól eltérő helyzetekben történő részvételre. Annak ellenére, hogy mind NATO, ENSZ, EU műveletekben jelentős a civil szolgáltatók bevonása, ezekben az esetekben nem a közbeszerzési rendszerben történik kiválasztásuk.

A közbeszerzési törvény számos olyan kivételt sorol fel, amelyre vonatkozóan nem kell a törvény szerinti közbeszerzési eljárást lefolytatni, ezekre felhatalmazta a kormányt, hogy külön rendeletet alkosson. A honvédelmi tárca vonatkozásában a cikk megírásakor hatályos HM Utasítás[12] főszabályként a központi beszerző szervezetet jogosítja fel közbeszerzési eljárás lefolytatására.[13]

Mivel a HM központi beszerző szervezet által lefolytatott eljárások negyedét teszi ki a közbeszerzés, a honvédségi szervezetek részéről pedig – az eddigi statisztikák alapján – közbeszerzésről nem beszélhetünk, kijelenthető, hogy a katonai beszerzés nem a közbeszerzés része, hanem éppen fordítva. A katonai beszerzés része a közbeszerzés.

Gyakorlati tapasztalataim alapján a közbeszerzés (általam megfogalmazottak szerint: közigazgatási beszerzés) a honvédségen belül olyan általános, időszakosan visszatérő szolgáltatások-, árubeszerzések esetén kerülnek alkalmazásra (élelmezés, személyszállítás, stb.), amelyekre nem vonatkoznak speciális előírások.

A (köz)beszerzés

A közbeszerzés és a kormányrendelet által alkotott beszerzési jogszabályok eltérő eljárásmódokat, sok esetben eltérő definíciókat is tartalmaznak. Vannak kormányrendeletek, amelyek háttérjogszabálya a Kbt., ezért visszahivatkozásokat találunk rá benne. Jellemzően azonban a kormányrendeletek a Kbt. kivételi köröket, azaz a közbeszerzés hatálya alá nem tartozó beszerzéseket szabályozza. Célszerűnek tartom a (köz)beszerzést megkülönböztetni a beszerzés általános definíciójától, tekintve, hogy itt jogszabály határozza meg az eljárásmódot. Amennyiben szabályozni szeretnénk egy adott szervezet beszerzési tevékenységét, mindenképpen különbséget kell tenni a két szabályzó között. A honvédség által alkalmazott definíciók alapján[14]:

közbeszerzés: a Kbt. hatálya alá tartozó beszerzés;

---

[11] A közbeszerzések központi ellenőrzéséről és engedélyezéséről szóló 46/2011. (III. 25.) Korm. rendelet

[12] A honvédelmi szervezetek beszerzéseinek eljárási rendjéről szóló 48/2012 (VII. 19.) HM Utasítás

[13] Kivételt képez a hazai nyelvképzés szolgáltatás, a nem haditechnikai besorolású gépjárműjavítás szolgáltatás és a kapcsolódó alkatrészek, valamint a honvéd tisztjelöltek "B" kategóriás, valamint a honvéd altiszt-jelöltek "B" és "C" kategóriás vezetői engedélyének megszerzését szolgáló tanfolyam tárgyú közbeszerzések közösségi közbeszerzési értékhatárig, valamint az MH BHD és MH EK közbeszerzési eljárásai.

[14] A honvédelmi szervezetek beszerzéseinek eljárási rendjéről szóló 48/2012 HM Utasítás

(köz)beszerzés: a Kbt. felhatalmazása alapján kiadott kormányrendeletekben meghatározott eltérő szabályok alapján végrehajtott beszerzés, valamint a közbeszerzés.

Összefoglaló néven a (köz)beszerzés: jogszabály[15] által szabályozott beszerzés, amelynek típusai:

a.) a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló *228/2004. (VII. 30.) Korm. rendelet*

A védelmi piacok a termékek és szolgáltatások széles skáláját ölelik fel, a nem hadi célokat szolgáló anyagoktól (irodacikkek, élelmezés) kezdve a fegyverrendszerekig és a különösen érzékeny természetű felszerelésekig (titkosító berendezések, illetve nukleáris, biológiai és vegyi felszerelések). A fegyverrendszerek gyakran olyan összetett rendszerek, melyek kifinomult technológiákat alkalmaznak, fejlesztésük többnyire hosszú időt vesznek igénybe, életciklusuk rendszerint igen hosszú, előállításuk pedig gyakran magas, vissza nem térülő költséggel jár.

A védelmi piacot alapvetően az különbözteti meg más piacoktól, hogy vevői oldalon szinte kivétel nélkül állami szervek állnak, a védelmi piacon kínált termékek és szolgáltatások pedig szigorú szabályozás alá esnek. Éppen ezért a piaci szereplők száma is korlátozott. Amikor 2004-ben Magyarország átültette a védelmi irányelvet[16] a hazai jogrendbe, a védelmi piacát is megnyitotta az Európai Unió többi tagállama előtt.

A védelmi beszerzések lefolytatásának alapját az Európai Unió direktívája (irányelve) határozza meg, amely a honvédelmi és biztonsági beszerzést együttesen szabályozza. A hazai jogalkotó az irányelv hatálya alá tartozó védelmi és nemzetbiztonsági célú beszerzéseket két különálló jogszabályban szabályozta, tekintettel arra, hogy a védelmi beszerzési kormányrendeletet a Honvédelmi Miniszter[17], a minősített beszerzési kormányrendeletet a Belügyminiszter[18] készítette elő.

A 228/2004. (VII. 30.) Korm. rendelet hatálya értékhatárra tekintet nélkül kiterjed valamennyi, a tárgyi hatálya alá tartozó védelmi beszerzésre. A védelmi beszerzések területén nincsen értékhatár alatti beszerzés, aminek egyik oka a védelmi piacon kínált termékekre és szolgáltatásokra vonatkozó szigorú szabályozás.

A védelmi beszerzés másik sajátossága, hogy nem szabályozza külön a nemzeti és külön az uniós eljárást. *Ezáltal a kis értékű katonai célú építési beruházás, vagy egy több milliárd forint értékű, összetett haditechnikai rendszer beszerzésére is ugyanolyan eljárás keretében kerül sor. Ez a megoldás a kisebb értékű beszerzések esetében felesleges – a beszerzés értékével arányban nem álló – adminisztrációs terheket ró az ajánlattevőkre*.[19]

---

[15] Alaptörvény T) cikk 2) bekezdése szerint: „Jogszabály a törvény, a kormányrendelet, a miniszterelnöki rendelet, a miniszteri rendelet, a Magyar Nemzeti Bank elnökének rendelete, az önálló szabályozó szerv vezetőjének rendelete és az önkormányzati rendelet. Jogszabály továbbá a Honvédelmi Tanács rendkívüli állapot idején és a köztársasági elnök szükségállapot idején kiadott rendelete."

[16] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2009/81/EK IRÁNYELVE: a honvédelem és biztonság területén egyes építési beruházásra, árubeszerzésre és szolgáltatásnyújtásra irányuló, ajánlatkérő szervek vagy ajánlatkérők által odaítélt szerződések odaítélési eljárásainak összehangolásáról

[17] A 228/2004. (VII. 30.) Korm. rendelet módosításáról szóló rendelettervezet http://www.kormany.hu/download/1/79/60000/Rendelettervezet.pdf

[18] a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló rendelettervezet http://www.kormany.hu/download/7/90/50000/TERVEZET.pdf

[19] Összefoglaló a „Hatásvizsgálatok és a kormányzati stratégiai irányítás rendszere egyes ágazati dokumentumainak elkészítése, valamint alkalmazási gyakorlatának támogatása a Honvédelmi Minisztériumban" című (ÁROP -1.1.19-2012-2012-0001 kódjelű) projekthez

A védelmi irányelv alkalmazása mindig is komoly nehézségekkel járt, mivel az alapvető biztonsági érdek fogalma meglehetősen homályos. Az irányelv alapján a Tanács 1958-ban elfogadott egy listát (ML- Military List), mely feltünteti azokat a fegyvereket, lőszereket és hadianyagokat, amelyekre a szabályozás kiterjed. Ugyanakkor azonban ez a lista meglehetősen általános jellegű, ezért nem mindig egyértelmű, hogy az egyes védelmi szerződésekre mely szabályok vonatkoznak.[20]

A tagállamok olyan felszereléseket is beszereznek, amelyek rendelkeznek ugyan a védelmi termékek sajátos jellemzőivel, mégsem nélkülözhetetlenek (feltétlenül) az adott ország biztonsági érdekei szempontjából. Magyarország is kiegészítette további termékekkel és szolgáltatásokkal (HUML- Hungarian Military List)[21]az irányelvben szereplő listát.

A haderő beszerzéseire vonatkozó HM Utasítás szerint a haditechnikai eszközök és szolgáltatások (beleértve az infrastrukturális beruházást) fegyverek, lőszerek és hadianyagok, valamint az alapvető biztonsági érdeket érintő beszerzések terén a honvédségnél kizárólag a központi beszerző szervezet járhat el, tekintettel arra, hogy ezekre közösségi, speciális szabályok vonatkoznak.

A védelmi beszerzésekre vonatkozóan - a Kbt. szabályaival összhangban - közösségi és nemzeti beszerzési eljárásrend folytatható. Az árubeszerzésre vagy szolgáltatásnyújtásra irányuló beszerzések esetén a 400.000 EUR értéket elérő, vagy azt meghaladó értékű beszerzések, építési beruházásra irányuló beszerzés esetén az 5.000.000 EUR értéket elérő, vagy azt meghaladó értékű beszerzések esetén a hirdetményeket (felhívást) az Európai Unió Kiadóhivatalának kell megküldeni megjelentetésre. Sajátossága a védelmi beszerzésnek, hogy nyílt eljárás kizárt, továbbá különleges eljárásmód lehetséges.

A védelmi beszerzés tehát a közbeszerzés egyik kivételi köre, melynek lefolytatásának rendjét és körét külön jogszabály határozza meg. A védelmi beszerzés azonban nem minden termékre és szolgáltatásra alkalmazható, amely a honvédség működése szempontjából releváns.

b.) A minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló *218/2011. (X. 19.) Korm. rendelet*

A biztonsági beszerzések lefolytatásának alapját (a korábban említett védelmi beszerzésekkel összhangban) az Európai Unió direktívája (irányelve) határozza meg, amely a honvédelmi és biztonsági beszerzést együttesen szabályozza.

A védelmi irányelv alapján „*A védelem és biztonság területén egyes szerződések olyannyira érzékenyek, hogy - speciális jellege ellenére-nem volna helyénvaló ezen irányelv alkalmazása. Ez vonatkozik a hírszerző szolgálatok beszerzéseire és a hírszerző tevékenység valamennyi típusával összefüggő beszerzésekre, ideértve a - tagállamok fogalom - meghatározásának megfelelően - a kémelhárítási tevékenységet is. Ez vonatkozik továbbá olyan különösen érzékeny beszerzésekre is, amelyek rendkívül magas minősítési szintet követelnek meg, mint például a határvédelemmel, a terrorizmus és a szervezett bűnözés elleni küzdelemmel összefüggő, a rejtjeltevékenységre vonatkozó, vagy a rendőrség vagy más biztonsági szervek által végrehajtott leplezett tevékenységekre vagy más hasonlóan érzékeny tevékenységekre vonatkozó beszerzések.*[22]

[20] Az Európai Közösségek Bizottságának közleménye: a Tanácsnak és az Európai Parlamentnek a honvédelem közbeszerzéséről szóló zöld könyv által elindított konzultáció eredményéről és a Bizottság jövőbeli kezdeményezéseiről (Brüsszel, 2005. december 6)

[21] a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló 228/2004. (VII. 30.) Korm. rendelet XXIII-XXV fejezet

[22] 2009/81/EK irányelv (27) bekezdés

Eljárás megindítása előtt legfontosabb kérdés, hogy az adott beszerzés a Kbt. vagy a minősített beszerzési rendelet hatálya alá tartozik, azaz hogy a beszerzés tárgya tartalmaz -e minősített adatot[23], vagy az ország alapvető biztonsági, nemzetbiztonsági érdekét érinti –e.

A Kbt. alapján[24] az ország alapvető biztonsági érdekével kapcsolatos beszerzés fogalma:

„olyan beszerzés, amelynek tárgya közvetlenül kapcsolódik az ország lakosságának fizikai, környezeti, egészségügyi, gazdasági, honvédelmi biztonságát befolyásolni képes építési beruházáshoz, árubeszerzéshez, valamint szolgáltatás megrendeléséhez, ideértve a védekezési készültség esetén a vízkár közvetlen elhárítása érdekében szükséges beszerzéseket is."

A minősített beszerzési rendelet az irányelvvel összhangban kétfajta eljárásrendet különböztet meg, a közösségi beszerzéseket és nemzeti beszerzéseket.

Közösségi beszerzést kell lefolytatni, ha:

- eléri az irányelv által meghatározott értékhatárt (árubeszerzés/szolgáltatás esetén: 387.000 €; építési beruházás esetén: 4.845.000 €) és
- beszerzés tárgya alapján érzékeny beszerzésnek minősül.
- Nemzeti beszerzést kell lefolytatni, ha
- minősített adatot, alapvető biztonsági érdeket vagy nemzetbiztonsági érdeket érint a beszerzés tárgya és a Kbt. szerinti nemzeti értékhatárt eléri,
- minden olyan esetben amikor nem az érzékeny közösségi beszerzési eljárásrendet kell alkalmazni.

A védelmi irányelv alapján nem tartozik a közösségi beszerzések hatálya alá a különösen érzékeny beszerzések, a hírszerző és elhárító tevékenységgel összefüggő beszerzések.

Kizárólag a nemzeti eljárásrendet kell alkalmazni a különösen érzékeny beszerzésekre[25]:

a határvédelemmel kapcsolatos, a terrorizmus és a szervezett bűnözés elleni küzdelemmel összefüggő, a rejtjeltevékenységre vonatkozó, valamint a Nemzeti Adó- és Vámhivatal vagy rendvédelmi szervek által végzett titkos információgyűjtő, illetve titkos adatszerző tevékenységgel közvetlenül összefüggő beszerzések.

A biztonsági beszerzési eljárások nem tartoznak a közbeszerzés és a Kbt. hatálya alá, annak kivételi körét képezik. Azonban a minősített beszerzési rendelet számos helyen hivatkozik a Kbt. szabályaira. Alapelvként a törvényben foglalt szabályokat rendeli alkalmazni, de ezen túlmenően megadja az eltérő szabályokat is.

Védelmi beszerzéssel ellentétben a biztonsági beszerzések vonatkozásában kötelező a közbeszerzések terén fennálló – Nemzeti Fejlesztési Miniszter - előzetes és utólagos engedélyeztetése.

d.) A központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről szóló *168/2004. (V. 25.) Korm.rendelet*

A közigazgatási szerveknek a saját közbeszerzéseit – meghatározott termékkörökre vonatkozóan (általános célú felhasználású termékek/szolgáltatások) - központosított közbeszerzési eljárás keretében kötelező lefolytatniuk annak érdekében, hogy az állami ráfordítások csökkenjenek, a költségvetési előirányzatok tervszerűen legyenek felhasználva, továbbá az eljárások lebonyolításához szükséges megfelelő szakértelem biztosítva legyen és végül az általánosan használt, azonos használati célú, jól tipizálható termékek koncentrált beszerzése megvalósuljon. Ezeknek a céloknak ismeretében és elérése érdekében a mindenkori Kormány kialakította az általa irányított szervezetek beszerzései között általánosan vagy időszakosan visszatérő módon szereplő azonos termékek és szolgáltatások előre meghatározott szabályok szerint történő beszerzéseinek rendszerét, a központi közbeszerzést.

[23] A minősített adat védelméről szóló 2009. évi CLV. törvény szerint

[24] Kbt. 4. § 3. pont

[25] A minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 218/2011. (X. 19.) Korm. rendelet 2. § 17. pont

Az állami normatíva alapján évente felülvizsgálva meghatározzák azoknak a termékköröket, illetve azok műszaki paramétereit, amelyek a központosított közbeszerzés hatálya alá tartoznak. Az úgynevezett központosított közbeszerzés lényege, hogy meghatározott ajánlatkérők[26] egy központi szervezeten keresztül, a központi szervezet (jelenleg Közbeszerzési és Ellátási Főigazgatóság) által lebonyolított közbeszerzési eljárásban központosítottan szereznek be bizonyos termékeket és szolgáltatásokat, pontosabban az eljárás eredményeként megkötendő keretszerződés vagy keretmegállapodás alapján valósítják meg egyedi beszerzéseiket. A lebonyolító szerv tehát gyakorlatilag több intézmény közbeszerzéseit fogja össze és bonyolítja le, mégpedig oly módon, hogy eközben bizonyos, külön jogszabályban meghatározott szolgáltatásokat nyújt az eljárásban részt vevők számára.

A központosított közbeszerzések vonatkozásában is kötelező a közbeszerzések terén fennálló – Nemzeti Fejlesztési Miniszter - előzetes és utólagos engedélyeztetése. A tárcaszintű beszerzések szabályozásáról szóló HM Utasítás[27] főszabályként a HM központi beszerző szervezetét jogosítja fel központosított közbeszerzési eljárás lefolytatására.

Kivételes esetben, amennyiben a KEF nem rendelkezik sem keretmegállapodással, sem keretszerződéssel, akkor az intézmény jogosult saját hatáskörben is eljárni a Kbt. szabályaival összhangban. Gyakorlatban ez sokszor okoz gondot, hiszen egy közbeszerzési eljárás lefolytatásának ideje több hónapot is igénybe vehet, ezalatt pedig a KEF szintén köthet keretszerződést, keretmegállapodást ugyanazon termékre (vagy szolgáltatásra). Ekkor az intézmény kénytelen visszavonni az eljárást.

Az engedélyezési folyamat időtartama alatt is előfordult, hogy KEF által kötött keretszerződés, vagy keretmegállapodás hatályát veszti (pl.költségkeret felső határát elérte). Ekkor az intézménynek – már így is jelentős határidő csúszással – közbeszerzési eljárást lefolytatni. HM tárca vonatkozásában a Kbt. részekre bontási tilalma miatt alapvetően közösségi eljárásrend kerül lefolytatásra

„Részekre bontás alatt azt kell érteni, amikor az ajánlatkérő egy közbeszerzést több szerződéssel valósít meg úgy, hogy azok értékét külön-külön veszi figyelembe a becsült érték megállapításakor és ezáltal nem alkalmazza a Kbt.-t, vagy nem a magasabb érték szerint alkalmazandó eljárási szabályok szerint folytatja le az egyes közbeszerzési eljárásokat.”[28]

c.) A fekvőbeteg szakellátást nyújtó intézmények részére történő gyógyszer-, orvostechnikai eszköz és fertőtlenítőszer beszerzések országos központosított rendszeréről szóló *46/2012. (III. 28.) Korm. rendelet*

2004 óta az egészségügyi termékek egy részére vonatkozóan kizárólag a központosított közbeszerzés keretében van lehetőség megrendelésre, szerződéskötésre. A Központi Szolgáltató Főigazgatóság[29] a Miniszterelnöki Hivatalt vezető miniszter irányítása alatt keretszerződéseket, később keretmegállapodásokat kötött. Ezáltal az egészségügyi intézmények részére a termékek típusa, ára, valamint a szerződő partnerek központilag meghatározásra kerültek. A beszerzéseket a 168/2004. (V. 25.) Korm.rendelet alapján kellett lefolytatni.

2005-ben kiadott HM utasítás[30] alapján az MH Egészségügyi Központ jogelőd intézményei (Honvédkórház – Állami Egészségügyi Központ (Honvéd, Rendészeti- és Vasútegészségügyi Központ); MH Dr. Radó György Honvéd Egészségügyi Központ) önállóan nem voltak

[26] Lsd: kormányrendelet személyi hatálya

[27] A honvédelmi szervezetek beszerzéseinek eljárási rendjéről szóló 48/2012 (VII. 19.) HM Utasítás

[28] A Közbeszerzési Hatóság útmutatója a részekre bontás tilalma alkalmazásához (KÉ 2013. évi 141. szám; 2013. november 29.)

[29] A Közbeszerzési és Ellátási Főigazgatóság jogelőd szervezete

[30] A Magyar Honvédség, valamint a honvédelmi miniszter közvetlen irányítása és felügyelete alá tartozó szervezetek beszerzéseinek eljárási rendjéről” szóló 102/2005. (HK 22.) HM utasítás;

jogosultak központosított közbeszerzés keretében egészségügyi termékeket beszerezni (megrendelni), kizárólag megbízás alapján a HM központi beszerző szervezet.

2011-ben a 168/2004 Korm. rendelet központosított közbeszerzési listájából (állami normatíva) kikerültek az egészségügyi termékek. Ezen egészségügyi termékek kiegészülve a gyógyszerekkel és egyéb gyógyszerészeti eszközökkel, egy másik kormányrendelet[31] hatálya alá kerültek. A korábbi gyakorlattal ellentétben 2011 májusától a magyar kórházak nem egyénileg, hanem egy kormányzati felügyelet álló (Nemzeti Erőforrás Minisztérium egészségügyi háttérintézménye) szervezeten, a Gyógyszerészeti és Egészségügyi Minőség- és Szervezetfejlesztési Intézeten (GYEMSZI)[32] keresztül szerezhetnek be gyógyszert és gyógyszerészeti eszközöket.

A Korm. rendelet értelmében a fekvőbeteg szakellátást nyújtó intézmények részére történő gyógyszer-, orvostechnikai eszköz és fertőtlenítőszer ellátása kizárólag az országos központosított rendszeren keresztül történik.

A gyógyszerek, orvostechnikai eszközök beszerzését - az OEP beszerzésein kívül - a GYEMSZI hajtja végre, amelyekre ezen szervezet keretmegállapodásokat, keretszerződéseket köt. A kórházak a GYEMSZI eljárásainak második részeként rendelhetik meg a termékeket.

Amennyiben a GYEMSZI keretmegállapodást köt, az intézmény az NFM előzetes és utólagos engedélyével rendelhet meg, indíthatja újra a versenyt.

A Kormányrendelet beszerzési szabályai vonatkoznak a Magyar Honvédség központi kórházára (MH Egészségügyi Központ) is, amelynek azonban alaprendeltetésű feladati közé tartozik a katona-egészségügyi képességek kialakítása és fenntartása; a Magyar Honvédség nemzetközi kötelezettségeiből adódó egészségügyi feladatok végzése; MH Közegészségügyi és Járványügyi Szolgálatának működtetése, a Magyar Honvédség egészségügyi tevékenységének felügyelete. Ez jelenti olyan egészségügyi anyagok és szolgáltatások beszerzését, amelyek a többi (civil) kórházaknál nem jelennek meg. Ilyen többek között a missziós egészségügyi felszerelések, oltó és ellenanyagok (pld: atropin tartalmú önampulla), amelyek a védelmi beszerzés hatálya alá tartoznak.

A beszerzések eljárási rendjéről szóló HM Utasítás 2012 decemberi módosítása már lehetőséget biztosított az MH Egészségügyi Központ részére, hogy feladatkörébe tartozó kötelezettségek teljesítése érdekében önállóan folytasson le központosított közbeszerzési eljárásokat (KEF-en és GYEMSZI-n keresztül), valamint közbeszerzési eljárást folytasson le.

Nincs lehetősége azonban védelmi célú beszerzéseket, nemzetbiztonsági célú beszerzéseket lefolytatni. A honvédelmi tárca éves beszerzési tervében már előre tervezni kell, hogy az adott (tárgyévi vagy azt követő) egészségügyi igény a közbeszerzés, központosított hatálya alá tartozik, így az MH Egészségügyi Központ jár el ajánlatkérőként; vagy speciális beszerzések hatálya alatt a központi beszerző szervezet megbízása szükséges. (a megbízás elkészítésének, jóváhagyatásának, ellenjegyzésének folyamata több hónapot is igénybe vehet)

Az MH Honvédkórház jogállása kettős:

- azon ellátások tekintetében, amelyek finanszírozása nem az Alapból (OEP) történik, hanem a HM tárca finanszírozza, nem köteles alkalmazni a rendszert;
- amelynek finanszírozása az Egészségügyi Alapból (OEP) történik, köteles a GYEMSZI-n keresztül a megrendelést végrehajtani.

e.) A NATO Biztonsági Beruházási Program keretében megvalósuló beszerzésekre vonatkozó részletes szabályokról szóló *109/2012. (VI. 1.) Korm. rendelet*

[31] A fekvőbeteg szakellátást nyújtó intézmények részére történő gyógyszer-, orvostechnikai eszköz és fertőtlenítőszer beszerzések országos központosított rendszeréről szóló 46/2012. (III. 28.) Korm. rendelet

[32] GYEMSZI-t a Semmelweis-terv hívta életre 2011. május 1-jével öt korábbi intézmény integrációjával (Egészségügyi Stratégiai Kutatóintézet (ESKI), az Országos Gyógyszerészeti Intézet (OGYI), az Egészségügyi Szakképző és Továbbképző Intézet (ETI) és az Országos Szakfelügyeleti Módszertani Központ (OSZMK), az Egészségügyi Minőségfejlesztési és Kórháztechnikai Intézet (EMKI)

A NATO, mint nemzetközi szervezet rendelkezik az általa finanszírozott beszerzésekre vonatkozó szabályokkal (AC-4/D/2261. számú dokumentum). A szabályok szerint, az abban foglalt beszerzési eljárástól csak kivételesen és a NATO hozzájárulásával lehet eltérni.

A NATO Biztonsági Beruházási Program (North Atlantic Treaty Organization Security Investment Program – a továbbiakban: NSIP) a NATO egyik kiemelt jelentőségű infrastrukturális beruházási programja, mely a NATO közös védelmi képesség biztosítása érdekében a szükséges beruházások megvalósítását a tagországok gazdálkodó szervezeteinek bevonásával teszi lehetővé. A beruházási feladatot kivitelező szállítót, nemzetközi pályázati eljárás során kiválasztják ki.

A NATO forrásokat biztosít és felügyeletet, ellenőrzést gyakorol a beszerzések felett, még akkor is, ha azok nemzeti eljárásban folynak. A felügyelet és ellenőrzés gyakorlása a közbeszerzési törvény szerint folyó közbeszerzési eljárásoknál nem biztosítható. Az EU közbeszerzési szabályok erre lehetőséget adnak. A közbeszerzési törvény és az EU közbeszerzési szabályai nem teszik lehetővé az ajánlattevői kör területi alapon történő megkülönböztetését, szemben a NATO beszerzési eljárásokra vonatkozó szabályaival, ahol csak a NATO tagországban bejegyzett gazdálkodó szervezetek vehetnek részt ajánlattevőként az eljárásban.

Hazánk NATO tagsága lehetőséget biztosít a magyar gazdálkodó szervezeteknek arra, hogy részt vegyenek az NSIP beruházásokban. A magyar gazdálkodó szervezetek szerződés teljesítési képességének megítélésére 2002-ben került létrehozásra a NATO Beszállítói rendszer. A rendszer egy állandó NATO beszállítói kör kialakítását és fenntartását tűzte célul, melyen belül a „NATO Beszállításra Alkalmas" címet nyert cégekre vonatkozóan Magyarország képes felelősen garanciát vállalni ezek szakmai, gazdasági, pénzügyi, és szükség esetén biztonsági megfelelőségéért.

A Kbt. kivételi körként határozza meg a nemzetközi szerződésekhez, megállapodásokhoz vagy szervezetekhez kapcsolódó beszerzési eljárásokat. E felhatalmazás alapján alkották meg a NATO Biztonsági Beruházási Program keretében megvalósuló beszerzésekre vonatkozó részletes Kormányrendeletet.

A korábban hatályos a NATO Biztonsági Beruházási Program keretében megvalósuló beszerzésekre vonatkozó részletes szabályokról szóló 40/2005. (III. 10.) Korm.rendelet a közbeszerzésekről szóló 2003. évi CXXIX. törvény felhatalmazásán alapult, ezért 2012-ben újra szabályozásra kerültek a NATO beszerzési szabályok, amelyek már figyelembe vették az új közbeszerzési törvény szabályait, szellemiségét.

Az NSIP esetében közbeszerzésről nem beszélhetünk, sőt még csak nem is az Európai Unió által szabályozott beszerzésről. Olyan esetekben, amikor az adott feladat költségvetésének egy részét a NATO, másik részét a hazai központi költségvetés finanszírozza, két külön beszerzési eljárást kell lefolytatni, eltérő jogszabályi alapon – eltérő eljárásrendben, eltérő időszükségletekkel.

f.) a büntetés-végrehajtási szervezet részéről a központi államigazgatási szervek és a rendvédelmi szervek irányában fennálló egyes ellátási kötelezettségekről, a termékek és szolgáltatások átadás-átvételének és azok ellentételezésének rendjéről szóló *44/2011 Korm. rendelet*

A büntetés-végrehajtási szervezetről szóló[33] törvényben foglaltak alapján a büntetés-végrehajtási szervezetet (BV) – a központi államigazgatási szervek, a rendvédelmi szervek, az egészségügy területén működő országos intézetek, szociális intézmények mellett - a Magyar Honvédség részére is ellátási kötelezettség terheli. Ez a kötelezettség a fogvatartottak kötelező foglalkoztatása keretében előállított termékek és szolgáltatások körére terjed ki[34], ami

[33] a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény 9/A. § (3) bekezdés

[34] A büntetés-végrehajtási szervezet részéről a büntetés-végrehajtásért felelős miniszter vezetése, irányítása vagy felügyelete alá tartozó szervek irányában fennálló ellátási kötelezettségről, a fogvatartottak kötelező

folyamatosan változik. (Munka, védőruha és egyenruházati termékek, egyenruházati lábbelik, egyenruházati kiegészítők, háztartási, egészségügyi papírtermékek, irodabútor, stb.)

A BV ellátás kizárólag a BV Központi Ellátó Szerve (a továbbiakban: BV KESZ) útján valósulhat meg, az igények bejelentésével. Az ellátási kötelezettség a nettó 100.000 forintot elérő vagy meghaladó igényekre terjed ki.

A honvédség speciális (NATO, ENSZ missziók) igényei azonban olyan minőségi követelményeket határoznak meg, amelyek szélsőséges időjárási körülmények között is képesek a személy védelmére. Ezzel összefüggésben a BV rendelet is kiemeli, hogy *az igényelt termékek és szolgáltatások kapcsán vizsgálni kell, hogy annak előállítása a fogvatartottak kötelező foglalkoztatása keretében történő előállítás keretei között biztosítható minőségi és mennyiségi korlátok mellett megvalósítható-e.*

További támpontot jelent, hogy a büntetés-végrehajtási szervezetről szóló törvény alapján *a BV-t nem terheli az ellátási kötelezettség a Magyar Honvédség tekintetében, ha a honvédelemért felelős miniszter rendelkezése alapján a Magyar Honvédség egyéb beszerzési eljárást folytat le.*

A jogszabályi előírás alapján a BV KESZ uniós értékhatárt elérő, vagy meghaladó ellátási igények esetén ajánlatot tesz az Igénybejelentő HM szerv részére. Amennyiben az Igénybejelentő elfogadja az ajánlatot, a Felek ellátási megállapodást kötnek.

Az ellátási megállapodás alapján a tárcák között a fedezet átcsoportosítása szükséges az államkincstáron keresztül, amely minimális időtartama 30 nap. Az átcsoportosítást követően a BV KESZ közbeszerzési eljárást folytat le az NFM engedélyeztetést követően (amely további minimum 85 napot jelent), amelyben a HM és MH tárca együttműködése elengedhetetlen (műszaki dokumentáció, szakértői bizottság, bíráló bizottság). Az eljárás eredményeként a KESZ köti meg a szerződést, az MH természetbeni ellátásként kapja meg a szolgáltatást.

Megállapítható, hogy a közösségi értékhatár felett az eljárási határidő hosszadalmasabb, a honvédségi beszerzés általi időszükséglet másfél-kétszerese, nem biztosított a BV KESZ által megkötött szerződés alapján a minőségi kifogás, szerződésmódosítás

A közösségi értékhatár alatt az Igénybejelentő részére a BV KESZ ajánlatot tesz, valamint kijelöli azt a szervezetet, amellyel szerződés köthető. Nem szükséges közbeszerzési eljárás lefolytatása és költségvetési fedezet átcsoportosítása.

Összességében tehát olyan termékekre, amelyek egyébként a közbeszerzés, vagy a védelmi beszerzés szabályai érvényesülnének, a honvédség köteles lenne a BV-től megrendelni, ha a honvédelmi miniszter másként nem rendelkezik. Közösségi értékhatár felett az eljárás hosszadalmas, közösségi értékhatár alatt pedig felelősen kell megállapítani, hogy az igényelt termék vagy szolgáltatás a közbeszerzés, a központosított közbeszerzés, vagy a védelmi beszerzés hatálya alá tartozik –e. A katonai szervezetek részére nagyobb körültekintést igényel a saját hatáskörű beszerzés, mivel a BV ellátás 100.000 Ft-tól került meghatározásra.

A tárca beszerzési eljárási rendjéről szóló HM utasítás (honvédelmi miniszter rendelkezése) feloldotta a problémát: a közösségi értékhatár felett a HM tárca központi beszerző szervezete folytat le Kbt. szerinti nyílt eljárást, amelyre a BV intézmények is jelentkezhetnek. Ezáltal biztosításra kerülne a HM tárca költségtakarékossági, gazdasági, célszerűségi elvárásai.

A közbeszerzési értékhatár feletti, de a közösségi értékhatár alatti esetekben a HM tárca központi beszerző szervezete végzi el a szükséges pontosításokat, egyeztetéseket, amely végén javaslatot tesz a BV szerződés megkötésére, vagy (köz)beszerzési eljárás lefolytatására.

Közbeszerzési értékhatár alatt, de 100.000 Ft felett az alakulat parancsnokának jogkörébe tartozik a döntés, hogy kíván –e BV szervezettel megállapodást kötni az ellátás biztosítása érdekében.

---

foglalkoztatása keretében előállított termékekről és szolgáltatásokról, azok átadás-átvételéről és az ellentételezés rendjéről szóló 41/2011. (XI. 25.) BM rendelet 1. sz. melléklet

g.) uniós támogatásból megvalósuló (köz)beszerzési eljárások

Az Európai Uniós források felhasználásra speciális közösségi és hazai szabályok vonatkoznak, amelyek többletkötelezettségeket rónak a kedvezményezettekre, ajánlatkérőkre, illetve többletjogokat adnak a forrásfelhasználást felügyelő szerveknek (irányító hatóság, közreműködő szervezetek).

Az uniós támogatásból történő beszerzési eljárás alapelvekben nem különbözik a korábban említett jogszabály által szabályozott beszerzésektől. Azaz a támogatást elnyert szervezet az adott jogszabályi rendelkezésnek megfelelően köteles közbeszerzési eljárást lefolytatni.

A speciális szabályokat külön rendelet, jelenleg a 2007-2013 programozási időszakban az Európai Regionális Fejlesztési Alapból, az Európai Szociális Alapból és a Kohéziós Alapból származó támogatások felhasználásának rendjéről szóló 4/2011. (I. 28.) Korm. rendelet tartalmazza.

A Korm. rendelet alapján a benyújtott uniós pályázatnak (támogatási kérelemnek) már tartalmaznia kell a költségvetésből nyújtott támogatásból megvalósítani tervezett tevékenységek, feladatok, beszerzések részletes ismertetését. *A közbeszerzési eljárások lefolytatásáért és Kbt. szerinti dokumentálásáért - a központosított közbeszerzés kivételével - a támogatást igénylő, illetve a kedvezményezett felelős. Ha a támogatást igénylő, illetve a kedvezményezett az ezen alcímben foglalt kötelezettségeit nem, vagy nem megfelelően teljesíti, és a felelőssége szabálytalansági eljárás keretében megállapításra kerül, a támogatási szerződés szerinti támogatás egy része vagy egésze visszavonható.*[35]

A honvédelmi szervezetek beszerzési eljárási rendjéről szóló HM Utasítás alapján azonban a HM központi beszerző szervezete jogosult közbeszerzési eljárás lefolytatására (így az uniós támogatásból megvalósuló eljárásokban is)

Uniós forrásból megvalósuló beszerzési eljárás előzetes és utólagos engedélyeztetése eltér a korábbi beszerzési típusoktól, azok többnyire a Közreműködő Szervezet[36] felé elektronikus formában történnek.

ÖSSZEGZÉS

A cikk első részében bizonyításra került, hogy a közbeszerzés a katonai beszerzés szűkebb része, továbbá az, hogy célszerű a (köz)beszerzés kifejezés alkalmazása a jogszabály által szabályozott beszerzésekre vonatkozóan. A katonai beszerzés olyan speciális terület, amely a beszerzési típusokat a legszélesebb körben alkalmazza, amely egy része a közigazgatásban is alkalmazott módszerek, másik része pedig a nemzetközi szabály, nemzetközi szerződés, nemzetközi megállapodás, kormányzati elgondolás alapján kimondottan a honvédség fenntartásával függ össze.

A cikk második részében már olyan különleges beszerzési előírások bemutatását végzem el, amelyek kimondottan honvédségi specialitások, mint a műveleti-, tartós külszolgálatot teljesítők ellátását célzó-, külföldi szervezetek által felajánlott haditechnikai eszközök-, NATO fenntartási Ügynökség bevonásával történő-, honvédségi közfoglalkoztatási programmal összefüggő-, „in house” beszerzések, valamint a honvédségnél meghatározott un. „kézi beszerzés”.

[35] A 2007-2013 programozási időszakban az Európai Regionális Fejlesztési Alapból, az Európai Szociális Alapból és a Kohéziós Alapból származó támogatások felhasználásának rendjéről 4/2011. (I. 28.) Korm. rendelet 37. §

[36] Az 1083/2006/EK tanácsi rendelet 2. cikk 6. pontja szerinti szervezet

Felhasznált irodalom

[1] Széchenyi István Egyetem- LOGISZTIKAI ÉS SZÁLLÍTMÁNYOZÁSI TANSZÉK :Beszerzési logisztika http://www.sze.hu/~hirko/web/Log1%20%28Egyetem%29/Beszerz%E9si%20logisztika.pdf (letöltés ideje: 2014. január 10.)

[2] Szegedi Zoltán - Prezenszki József: Logisztika-menedzsment Kossuth Kiadó, Budapest, 2008. ISBN: 9789630959124,

[3] Állami Számvevőszék 2004 novemberében készült 0451 sz jelentése „a Magyar Honvédség közbeszerzési rendszere működésének ellenőrzéséről Forrás: http://www.asz.hu/jelentes/0451/jelentes-a-magyar-honvedseg-kozbeszerzesi-rendszere-mukodesenek-ellenorzeserol/0451j000.pdf (letöltés ideje: 2014. január 10.)

[4] Az ügyvéd szerepe a közbeszerzési eljárásban http://www.bpugyvedikamara.hu/files/28/28147.doc (letöltés ideje: 2014. január 10.)

[5] A Közbeszerzési Hatóság útmutatója a részekre bontás tilalma alkalmazásához (Közbeszerzési Értesítő 2013. évi 141. szám; 2013. november 29.)

[6] Összefoglaló a „Hatásvizsgálatok és a kormányzati stratégiai irányítás rendszere egyes ágazati dokumentumainak elkészítése, valamint alkalmazási gyakorlatának támogatása a Honvédelmi Minisztériumban” című (ÁROP -1.1.19-2012-2012-0001 kódjelű) projekthez (2013) Forrás: http://magyaryprogram.kormany.hu/download/6/62/90000/AROP_osszefoglalo.pdf (letöltés ideje: 2014. január 10.)

[7] dr.Liszkai Rita: A minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól. JEGYZET (Belügyminisztérium) http://bmprojektek.kormany.hu/download/a/90/80000/Jegyzet%20Min%C5%91s%C3%ADtett%20beszerz%C3%A9st%20alkalmaz%C3%B3k%20r%C3%A9sz%C3%A9re.pdf (letöltés ideje: 2014. január 10.)

[8] Derzsényi Attila: Honvédelmi célú beszerzésről közérthetően (Katonai Logisztika Online 2011. év 1. szám) pp. 95-109. Forrás: https://www.parbeszed.hm.gov.hu/sites/kulso/Documents/katonaisajto/katonailogisztika/2011/1/Derzs%C3%A9nyi.pdf (letöltés ideje: 2012. 10. 31.)

[9] Derzsényi Attila: Honvédelmi tárca központosított közbeszerzése, Diplomamunka (Zrínyi Miklós Nemzetvédelmi Egyetem Budapest 2010) pp. 1-80

[10] Az Európai Közösségek Bizottságának közleménye: a Tanácsnak és az Európai Parlamentnek a honvédelem közbeszerzéséről szóló zöld könyv által elindított konzultáció eredményéről és a Bizottság jövőbeli kezdeményezéseiről (Brüsszel, 2005. december 6) Forrás: http://www.kozbeszerzes.hu/static/uploaded/document/Kozlemeny_Vedelmi_HU.pdf (letöltés ideje: 2014. január 10.)

Hivatkozott jogszabályok jegyzéke:

[1] Alaptörvény

[2] A honvédelem és biztonság területén egyes építési beruházásra, árubeszerzésre és szolgáltatásnyújtásra irányuló, ajánlatkérő szervek vagy ajánlatkérők által odaítélt szerződések odaítélési eljárásainak összehangolásáról, valamint a 2004/17/EK és 2004/18/EK irányelv módosításáról szóló az Európai Tanács és Parlament 2009/81/EK irányelve (eur-lex.europa)

[3] Az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alapra és a Kohéziós Alapra vonatkozó általános rendelkezések megállapításáról és az 1260/1999/EK rendelet hatályon kívül helyezéséről szóló 1083/2006/EK tanácsi rendelet (eur-lex.europa)

[4] A közbeszerzésekről szóló 1995 évi LXV törvény (Complex jogtár)

[5] A közbeszerzésekről szóló 2011. évi CVIII. tv. (Complex jogtár)

[6] A minősített adat védelméről szóló 2009. évi CLV. törvény (Complex jogtár)

[7] a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény (Complex jogtár)

[8] A 2007-2013 programozási időszakban az Európai Regionális Fejlesztési Alapból, az Európai Szociális Alapból és a Kohéziós Alapból származó támogatások felhasználásának rendjéről 4/2011. (I. 28.) Korm. rendelet (Complex jogtár)

[9] A közbeszerzések központi ellenőrzéséről és engedélyezéséről szóló 46/2011. (III. 25.) Korm. rendelet (Complex jogtár)

[10] A védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló 228/2004. (VII. 30.) Korm. rendelet (Complex jogtár)

[11] A minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 218/2011. (X. 19.) Korm. rendelet (Complex jogtár)

[12] A központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről szóló 168/2004. (V. 25.) Korm.rendelet (Complex jogtár)

[13] A NATO Biztonsági Beruházási Program keretében megvalósuló beszerzésekre vonatkozó részletes szabályokról szóló 109/2012. (VI. 1.) Korm. rendelet (Complex jogtár)

[14] A fekvőbeteg szakellátást nyújtó intézmények részére történő gyógyszer-, orvostechnikai eszköz és fertőtlenítőszer beszerzések országos központosított rendszeréről szóló 46/2012. (III. 28.) Korm. rendelet (Complex jogtár)

[15] A büntetés-végrehajtási szervezet részéről a büntetés-végrehajtásért felelős miniszter vezetése, irányítása vagy felügyelete alá tartozó szervek irányában fennálló ellátási kötelezettségről, a fogvatartottak kötelező foglalkoztatása keretében előállított termékekről és szolgáltatásokról, azok átadás-átvételéről és az ellentételezés rendjéről szóló 41/2011. (XI. 25.) BM rendelet (Complex jogtár)

[16] A Magyar Honvédség, valamint a honvédelmi miniszter közvetlen irányítása és felügyelete alá tartozó szervezetek beszerzéseinek eljárási rendjéről" szóló 102/2005. (HK 22.) HM utasítás; (Complex jogtár)

[17] A honvédelmi szervezetek beszerzéseinek eljárási rendjéről szóló 48/2012 (VII. 19.) HM Utasítás (Complex jogtár)

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Derzsényi Attila
attila.derzsenyi@hm.gov.hu

KATONAI LÉGISZÁLLÍTÁSI KÉPESSÉG (LOGISZTIKA ELŐTT ÁLLÓ FELADATOK ÉS AZOK LEHETSÉGES MEGOLDÁSAI)

Absztrakt

A katonai légiszállítás a rendszerváltást követően saját kapacitással, majd szállítmányozó cégek kiválasztásával valósult meg. Gazdaságossági szempontok figyelembe vételével célszerű a szállítmányozói feladatok civil szolgáltatótól történő átadása a katonai szervezeteknek. Ennek feltételeit a közbeszerzési jogi környezet is biztosítja.

In the wake of the change of regime military air transportation was accomplished through the military's own capacity and later on by selecting haulage contractor companies. Taking the economic aspects into account shipping tasks should be taken over by military organizations. Terms and conditions of this process are ensured by the public procurement legal environment also.

Kulcsszavak: *légiszállítás, közbeszerzés, szállítmányozó, dinamikus beszerzési rendszer ~ air transportation, public procurement, shipping agent, dynamic purchasing system*

BEVEZETÉS

A cikk megírásának ötletét az adta, hogy a HM Védelemgazdasági Hivatal jogelőd szervezete, a HM Fegyverzeti és Hadbiztosi Hivatal 2013. júniusában részvételi felhívást jelentetett meg *„Állami Légiszállító Flotta –szállítógép beszerzése és hozzá tartozó kiképzéssel és induló alkatrész készlettel”* tárgyban.[1] A HM tárca által kiadott közlemény szerint: *„A Malév megszűnésével olyan, az ország szempontjából stratégiai fontosságú képesség tűnt el, melyet szükséges pótolni. A HM által javasolt Állami Légiszállító Flotta létrehozása nem a Malév szerepét kívánja betölteni, hanem egy a katonai, állami és civil igényeknek megfelelő, a nemzetbiztonsági szempontokat is figyelembe vevő légiszállítási megoldási javaslat állami légi járművel, katonai üzemeltetésben.”*[2]

A közbeszerzési eljárás ugyan eredménytelenül zárult, ezért érdemes továbbra is elemezni a Magyar Honvédség jelenlegi légiszállítási képességét, illetve más NATO és EU tagállamokban már sikeresen alkalmazott olyan beszerzési lehetőségeket, amelyek hatékonyabb ellátási képességet biztosíthatnak.

A katonai többnemzeti feladatokban történő részvétel katonai (két-és többoldalú együttműködési megállapodások útján) és polgári (közbeszerzés útján) szállító kapacitás igénybevételével, komplex szállítmányozói szolgáltatás és a nemzeti légihidak formájában valósult meg, melyet a témában megjelent korábbi szakirodalmak részletesen kifejtettek. Szászi Gábor a *„MALÉV felszámolásának várható hatásai a katonai légiszállítási feladatok végrehajtására”*[3] című cikkében a saját eszközparkkal biztosított légiszállítási képesség szükségességére hívja fel a figyelmet a védelmi képesség folyamatos biztosítása érdekében.

Álláspontom szerint a légiszállítási képesség fenntartása nem kizárólagosan a hazai védelmi feladatok ellátását érinti. Kiemelendő hazánk NATO és EU tagságból fakadó kötelezettsége is, amelyek a kollektív védelmi műveletekben történő hozzájáruláson túl, a szövetséges műveletekben történő részvételt is jelenti. Szarvas László *„A Magyar Honvédség nagytávolságú szállítási lehetőségei”*[4] című cikkében kifejti, hogy a hazánkhoz hasonló nagyságú vagy hozzánk hasonló helyzetben lévő NATO/EU tagországok is törekednek stratégiai légi szállítóképességeik megteremtésén vagy növelésén. Ennek egyik első lépése volt 2002 novemberében a NATO Prágai Csúcsértekezleten elfogadott többnemzeti alapon létrehozandó garantált rendelkezésre állási szerződések megkötése, a polgári fuvarpiacon meglévő viszonylag szűkös kapacitások katonai célokra történő lekötése.

Az eddigi tanulmányok alapvetően közlekedési szakmai oldalról közelítették meg a téma vizsgálatát. A jelenlegi jogszabályi környezetben a polgári kapacitás igénybevételének nélkülözhetetlen feltétele a beszerzési eljárás lefolytatása. A több mint 10 éves katonai beszerzési tapasztalatom alapján (munkám során több alkalommal részt vettem a légiszállítási képesség beszerzésében), a légiszállítás beszerzésközpontú megközelítésével új ellátási módszerek, elvek vezethetők be, amelyek kialakításával gyorsabb, hatékonyabb ellátási forma valósulhat meg.

Az általam javasolandó beszerzési módszer részletes feltárása előtt célszerűnek tartom megvizsgálni, mely katonai légiszállítási területen szükséges polgári kapacitás gyakoribb igénybevétele, ezzel együtt beszerzési eljárás lefolytatása.

---

[1] Ajánlati felhívás:TED- HL/S 182829-2013-HU S107 05/06/2013 (http://ted.europa.eu)

[2] MTI hírek: Állami légi szállító flottát tervez a kormány http://www.honvedelem.hu/cikk/38640

[3]Szászi Gábor: A Malév felszámolásának várható hatásai a katonai légiszállítási feladatok végrehajtására; Repüléstudományi Közlemények 2012. évi 2. szám pp.1036-1045 http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/86_Szaszi_Gabor.pdf

[4] Szarvas László: Stratégiai Légiszállítási Képesség – egy új többnemzeti megoldás 2008/7 Nemzet és Biztonság pp.60-76 http://www.honvedelem.hu/files/9/8723/a_mh_nagytavolsagu_szallitasi_lehetosegei-szarvas_l.pdf

SZÁLLÍTÁSI KÉPESSÉG

A rendszerváltást követően a Magyar Honvédség katonai szerepvállalása nagymértékben megváltozott. Az EU és NATO tagságból adódóan a közös védelmi képesség kialakítása került előtérbe, amely a szövetség tagállamain kívüli területek békeműveletire összpontosított. Ezek a többnemzeti műveletek hatékonyabb és egyben olcsóbb logisztikai megoldásokat igényeltek. A képesség fokozása érdekében mind a NATO[5], mind az EU[6] tagállamai közös légiszállítási képesség kialakítását határozták el. Az Európa Tanács Főtitkársága által kiadott „Európai Biztonsági Stratégia" című kiadványában[7] is külön hangsúlyt kap az EU tagállamok stratégiai légiszállítási képességének megerősítése.

A sokrétű katonai feladatra igénybe vett szállító képesség álláspontom szerint – a teljeség igénye nélkül – többféleképpen csoportosíthatóak:

- Jellege szerint: személy, teher, vegyes, (ill. veszélyes-különleges áru, védett személy);
- Távolság szerint: nagy, közepes, kis;
- Funkciója szerint: polgári, katonai, vegyes;
- Leszállási szükséglet szerint: közbenső leszállással, leszállás nélkül;
- Célállomás: válságkörzet, műveleti terület, béketerület;
- Közreműködő felek: hazai, NATO, többnemzeti.
- Stratégiai/taktikai: A stratégiai légiszállítás személyek, anyagok és technikai eszközök gyorsan és nagy (akár kontinenseken átívelő) távolságra, hadszíntérre történő ki- és visszatelepítését foglalja magában, míg a taktikai légiszállítás a személyi állomány és egyéb rakomány hadszíntéren belüli, megbízható és gyors szállítását biztosítja

A releváns, hazánkat érintő stratégiai katonai légiszállítási képességek az alábbiakból tevődnek össze:

Stratégiai Légiszállítási Képesség (SAC):

Tíz NATO-nemzet (Amerikai Egyesült Államok, Bulgária, Észtország, Hollandia, Lengyelország, Litvánia, Magyarország, Norvégia, Románia és Szlovénia) és két Békepartnerségi (PfP) nemzet (Finnország és Svédország) írták alá a Stratégiai Légiszállítási Képességről (Strategic Airlift Capability – a továbbiakban: SAC) szóló, 2008. szeptember 23-án hatályba lépett Egyetértési Szándéknyilatkozatot (Memorandum of Understanding - MOU).[8] A SAC program keretében három Boeing C-17 típusú amerikai stratégiai szállító repülőgép került megvételre, amelyek működtetése NATO-konzorcium keretében történik A gépeket a részt vevő nemzetek előre megállapított óraszámokra vehetik igénybe.

A SAC program elindítását 2007 nyarán jelentették be a NATO tagállamok védelmi minisztereinek brüsszeli találkozóján. Ezután a C-17-es szállítógépek beszerzésére és működtetésük támogatására megalakult a NATO Légiszállítást Kezelő Szervezet (NATO Airlift Management Organisation, NAMO), és annak végrehajtó ügynöksége a NAMA (NATO Airlift Management Agency).[9]

---

[5] Védelmi Képesség Kezdeményezés- Telepíthetőségi és Mozgathatósági Követelmény (DCI DM)
[6] Fő célkitűzés 2010 (Headline Goal 2010)
[7] Európai Biztonsági Stratégia
http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568HUC.pdf
[8] Honvédelmi Minisztérium: Stratégiai Légiszállítási Program http://www.kormany.hu/hu/honvedelmi-miniszterium/hirek/nato-strategiai-legiszallitasi-program-sac
[9] 2012. július 1-től a NATO ügynökségek reform határozatokkal összhangban a NAMO és NAMA része lett az új NATO-támogatási Ügynökségnek az NSPA-nek.

Megítélésem szerint a Magyarországot érintő katonai feladatok légiszállítási igényének nagysága jóval meghaladja a SAC programban lekötött repülési órákat, ezért ezen képesség mellett továbbra is szükséges más kapacitások igénybevétele.

Stratégiai Légiszállítási Átmeneti Megoldás (SALIS)

A 17 tagállam által létrehozott Stratégiai Légiszállítási Átmeneti Megoldás (Strategic Airlift Interim Solution - SALIS) által korlátozott mértékben, de előre rögzített áron, többek között hazánk részére is 2006 eleje óta elérhetővé vált elsősorban a túlméretes technikai eszközök szállítására egy garantáltan rendelkezésre álló polgári légi szállítókapacitás. A lipcsei bázisrepülőtéren 72 órás készenlétben áll 2 db, valamint további 4 db (6, illetve 9 napos készenlétű) AN-124-es típusú óriás szállító-repülőgép, NATO, EU, vagy nemzeti célokra. [10]

Tekintettel arra, hogy ez a program – a nevében jelzettekkel megegyezően – átmeneti megoldás, hosszabb távú alternatív lehetőség kialakítása szükséges.

Nemzeti légihidak (német, cseh, svéd, norvég, dán)

Az ún. „légihidakat"egyrészt maga a NATO, másrészt pedig a missziókban részt vevő tagországok hadseregei működtetnek. A repülőgépek kapacitásainak függvényében, a központ légihidak segítségével juttatja el a kisebb utánpótlási szállítmányokat anyaországból a célállomásra. Emellett pedig a váltások és a pihentetések között felmerülő rendkívüli személyszállítások is ezeknek a légihidak segítségével történnek. [11]

A légihidak gépei külföldi katonai bázisokról, illetve polgári repülőterekről indulnak, emiatt a felszerelések és személyi állomány eljuttatása a légi berakó állomásokra jelentős idő és költségtöbblettel jár.

Komplex szállítmányozási keretszerződés

Korábbi hazai gyakorlat alapján a repülőgépes személy-, és anyagszállításokra egy, a civil szférában működő, nemzetközi szállítmányozási cég magyar képviseletével kötöttek komplex keretszerződést. A meghatározott feladatokra e cég gyűjtötte be a piaci szereplők árajánlatait, amelyek közül a Katonai Közlekedési Központ vezetése döntött arról, hogy melyik jelentkezőt bízzák meg a szállítással. Sajnálatos tény, hogy a nyugati országok légitársaságainak gyakran problémát okozott az egykori szovjet utódállamokban a berepülési és a diplomáciai engedélyek beszerzése. Márpedig egy Magyarországról induló repülőgépnek át kellett repülnie Románián, Bulgárián, Törökországon, Azerbajdzsánon, Grúzián, Örményországon és Türkmenisztánon is, hogy afgán légtérbe érjenek. Mindez azt is jelentette, hogy egy-egy repülésre legalább tucatnyi, különféle engedélyt kellett beszerezni.[12]

A szállítmányozó igénybevételének előnye, hogy az adott katonai feladathoz legjobban alkalmazható szállítási kapacitás biztosítása gyorsan megoldható. A szállítmányozó által végzett piackutatás, előre megkötött megállapodások alapján azonnal – váratlan helyzeteket is biztosító – alternatív lehetőségek közül választhatunk.

A szállítmányozó alapvetően profitorientált, így érdeke a nagyobb haszonkulcs elérése a katonai költségvetés rovására. Ebből adódik hátránya, hogy a közbeszerzési eljárás keretében egy szállítmányozóval, több évre kötött vállalkozási szerződés plusz költséggel – a szállítmányozó profitjával - jár, továbbá a konkrét szállító kiválasztása csak a szállítmányozó által megadott piaci szereplői listából lehetséges.

---

[10] Vigh Attila A Honvédelmi Minisztérium Fejlesztési és Logisztikai Ügynökség Anyagi-Technikai és Közlekedési Igazgatóság Közlekedési Osztály helye, szerepe a missziós logisztikai támogatás rendszerében (Hadmérnök, III. Évfolyam 3. szám) http://hadmernok.hu/archivum/2008/3/2008_3_vigh.pdf

[11] Szűcs László: Akik a szállítást tervezik http://www.honvedelem.hu/cikk/19206

LÉGISZÁLLÍTÁSI KÉPESSÉG BESZERZÉSÉNEK LEHETŐSÉGE

A korábban kifejtésre került jelenlegi, hazai stratégiai légiszállítási képességet célszerű beszerzési oldalról is megvizsgálni. A hazai képesség megteremtésének lehetséges beszerzési formái:

Saját légi szállítógép beszerzés (eszközvásárlás): Egy önálló nemzeti stratégiai légi szállító flotta létrehozása a legtöbb azonnali erőforrást igénylő beszerzési forma, mivel – a nemzetgazdaság teherbíró képességének ismeretében - nem csak a repülőeszköz beszerzési és fenntartási költségigényeit kell figyelembe venni, hanem azt a különleges infrastrukturális igényt is, amely egy bázisrepülőtér kialakításához kötődik. Jelentős költségtényezőt jelent a személyi állomány kiképzéséhez kapcsolódó költséghányad is. Előnye viszont a szuverén rendelkezés az egész kapacitás fölött.

Többnemzeti beszerzés (eszközvásárlás): Szövetségi szinten is előnybe részesített ellátás előnye a költségek megoszlása a résztvevő felek között. Hátránya, hogy arányaiban ez a beszerzési forma is számottevő költségvetési erőforrás meglétét igényli.

Többnemzeti bérlés: A szolgáltatás igénybevételére irányuló beszerzési forma lényege magának a gépnek a bérlése. Előnye, hogy a teljes beszerzési költséghez képest nem jár azonnali jelentős erőforrás igénnyel. Hátránya, hogy az eszköz életciklusára vetítve költségigényesebb.

Szállítási kapacitás vétele piaci feltételek közt: Szintén szolgáltatás beszerzése, azonban nem a teljes gép repülési óráinak bérlésére, kizárólag annak egy meghatározott részére irányul. Előnye, hogy mindig van szabad piaci kapacitás és csak a konkrét szolgáltatásért kell fizetni. Az eddigi tapasztalatok alapján azonban a hátránya, hogy – főleg tömeges igény, például egy humanitárius válság kialakulásakor indított segítségnyújtási művelet esetén – a piaci árak minden esetben megemelkednek. Kiemelt költség tételt jelent a polgári felhasználástól eltérő alkalmazás biztosítási díja. A szállító továbbá előírhatja, hogy milyen körülmények fennállása esetén vállalja a feladat teljesítését.

SZÁLLÍTMÁNYOZÓI TEVÉKENYSÉG

2004-2005-től a szükséges légiszállítási kapacitás biztosítása érdekében közbeszerzési eljárás keretében olyan nemzetközi szállítmányozó cég kiválasztása történt, aki képes volt a stratégiai szállítási igényeket a szerződésben meghatározott feltételekkel kielégíteni.[12] Több szállítmányozó céggel is történt keretszerződés megkötése, többek között a Dán DFDS szállítmányozó vállalattal, a JAS Cargoways Kft-vel. A cikk alaptémájához kapcsolódóan szükségesnek tartom bemutatni a szállítmányozás folyamatát, valamint a szállítmányozó tevékenységét is.

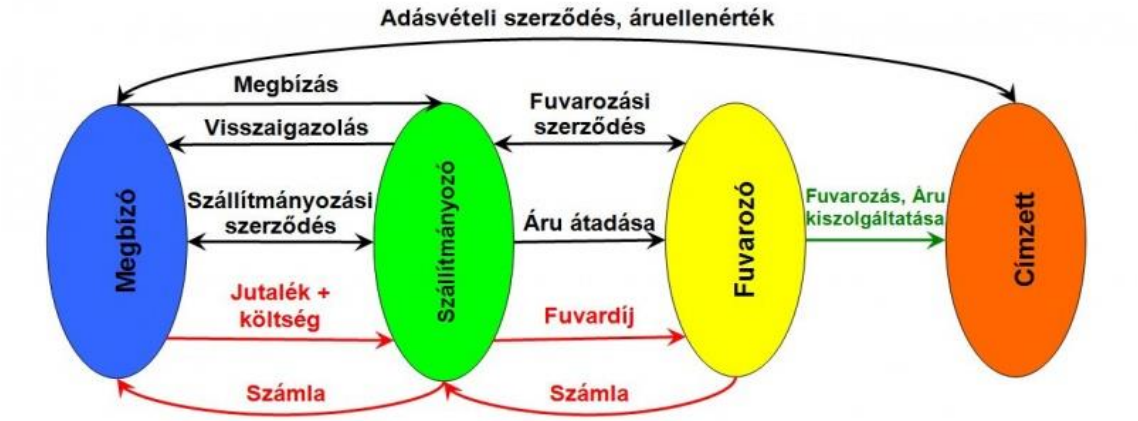
A szállítmányozás jogszabályi fogalma: ”*Szállítmányozási szerződés alapján a szállítmányozó köteles valamely küldemény továbbításához szükséges fuvarozási és egyéb szerződéseket a saját nevében és megbízója számlájára megkötni, valamint a küldemény továbbításával kapcsolatos egyéb teendőket elvégezni, a megbízó pedig köteles az ezért járó díjat megfizetni.”*[13] A szállítmányozó a fuvaroztató és fuvarozó közötti viszonyba bekapcsolódó szolgáltató. Helyét az eladó (fuvaroztató) és fogyasztó (címzett) közötti árutovábbítási folyamatban az alábbi ábra mutatja. [14]

---

[12]Szászi Gábor: A Malév felszámolásának várható hatásai a katonai légiszállítási feladatok végrehajtására; Repüléstudományi Közlemények 2012. évi 2. szám pp.1036-1045
http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/86_Szaszi_Gabor.pdf

[13] Polgári törvénykönyvről szóló 1959. évi IV. törvény (Ptk) 514 § (1) bekezdés

[14] A szállítmányozás és a fuvarozás jellemzői (http://hu.wiki.weblogtrade.eu/:)



1. ábra. A szállítmányozás folyamata
(Forrás:WebLogTrade)

A szállítmányozás alapvető gazdasági funkciója az árutovábbítás. A szállítmányozó ugyanakkor összehangolja az összetett fuvarozási tevékenységet és ellátja a szállítás során felmerülő raktározási, kezelési feladatokat is.

A szállítmányozó (speditőr) a saját nevében a megbízója számlájára vásárolja meg a fuvarozási és az áru továbbításához szükséges egyéb szolgáltatásokat. Arra vállalkozik, hogy az árutovábbítást a mindenkori piaci helyzetnek megfelelően a megbízója szempontjából a lehető leghatékonyabban megszervezze.[15]

A szállítmányozó bekapcsolásának általános indokai:

- Kedvezőbb fuvardíjak és fizetési feltételek elérése;
- Az áru - és fuvareszköz alakulás szempontjából legkedvezőbb elrendezésről a fuvareszközben. Ezzel csökkenthető az áru egységére jutó fuvardíja, a rakodási költség, valamint elkerülhetővé válik a nem megfelelő csomagolásból adódó átcsomagolási költség.
- Földrajzi és tarifaismerete, fuvarpiaci információi, szállítmányozói kapcsolatai, árinformációi az adott fuvarfeladat megvalósításához a lehető leggazdaságosabb és legbiztonságosabb útvonal kiválasztását eredményezhetik.
- A fuvarozási feladat sürgősségéhez mért legkedvezőbb megoldás megszervezését csak jó kapcsolatokkal és tapasztalatokkal rendelkező szállítmányozó képes biztosítani.

A szállítmányozó tevékenységének alapja a széleskörű fuvarozói kör ismerete, a fuvarozókkal kötött együttműködési megállapodások, a fuvarozók által biztosítandó erők és eszközök naprakész ismerete. Ennek nélkülözhetetlen eleme az arra speciálisan kiépített informatikai rendszeren alapuló - a gyakori beszerzések lebonyolítására szolgáló - teljes mértékben elektronikus program.

A katonai kiadások csökkentése érdekében indokolttá vált a szállítmányozó profitjának minimalizálása. Ennek egyik lehetséges formája az, ha a haderő saját maga veszi át a szállítmányozó szerepét. Tekintettel arra, hogy míg a szállítmányozó korlátlanul köthet szerződést, megállapodást polgári fuvarozóval, addig a központi költségvetésből gazdálkodó honvédelmi szervezetre szigorú közbeszerzési szabályok vonatkoznak.

Mindenképpen olyan rugalmas ellátási-beszerzési rendszer kialakítása válik szükségessé, amely képes a szállítmányozó szerepkörét átvenni: így különösen a potenciális fuvarozókkal kötendő olyan megállapodásokat, amely nem járnak előzetes kötelezettségvállalással. Ennek

[15] Magyar Logisztikai Egyesület: A közlekedés lokális fejlesztése a globalizáció tükrében (Tanulmány, 2007. szeptember) http://www.tranzitonline.eu/cikkek/a-kozlekedes-lokalis-fejlesztese-a-globalizacio-tukreben

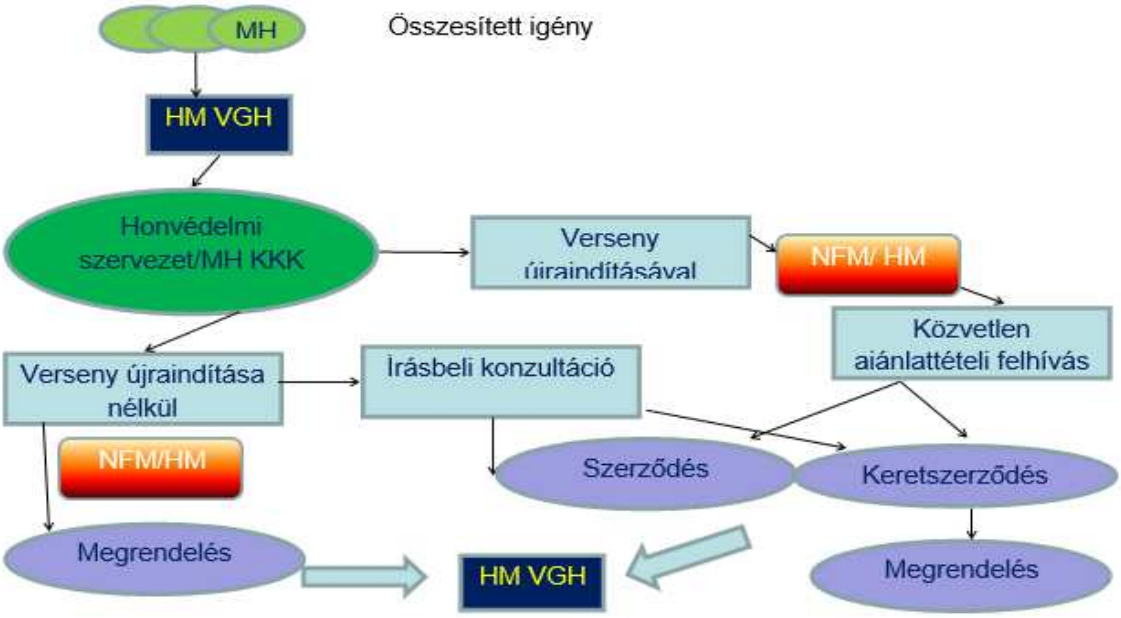
egyik megoldási módozata – amelyre vonatkozó előkészületek már megtörténtek – a keretmegállapodásos eljárás.

HADERŐ, MINT SZÁLLÍTMÁNYOZÓ

A honvédségi beszerzések korszerűsítésének első lépcsőjeként bevezetésre került a keretmegállapodásos eljárás alkalmazása. 2012-ben megjelent cikkemben[16] a honvédelmi szervezetek ellátása érdekében - folyamatosan jól működő – új típusú beszerzési- logisztikai rendszer működtetésére tettem javaslatot. A javasolt keretmegállapodásos eljárás alapján a honvédelmi szervezetek kisebb időigénnyel, hatékonyabban képesek lehetnek az ellátást biztosítani. Ezzel összefüggésben a „*honvédelmi szervezetek beszerzési eljárásának rendjéről"* szóló HM utasítás[17] módosításra került, lehetővé téve a korábban még nem alkalmazott keretmegállapodásos beszerzési eljárás alkalmazását.

A honvédelmi tárca által bevezetendő új – keretmegállapodásos - eljárásforma hosszabb távon kiszámíthatóbb ellátást biztosít az alakulatok számára. A beszerzési és szakmai szempontból jól előkészített keretmegállapodásos eljárás első részében kerülnek meghatározásra azon legfontosabb alapelvek (szakmai követelmény, potenciális ajánlattevők, értékelési szempont, szerződéstervezet), amely korábban folyamatosan visszatérő gondot és jelentős időszükségletet jelentettek.

A hivatkozott HM utasítás szerint a honvédelmi szervezetek által lefolytatandó keretmegállapodásos eljárás második részére vonatkozó követelményeket, valamint a HM VGH és honvédelmi szervezetek együttműködésének feltételeit a HM KÁT és a HVKF együttes intézkedésben[18] szabályozza.



2. ábra. Keretmegállapodás folyamata a HM KÁT-HVKF együttes intézkedés alapján

Az együttes intézkedés 11. pontja szerint – a katonai kontingensek és felszereléseik katonai feladat végrehajtására történő kitelepítése, váltása, át-, illetve hazatelepítése, utánpótlás és ellátás biztosítása érdekében katonai vagy polgári eszközökkel végzett szállítás-szolgáltatások

[16] Derzsényi Attila : Az élelmiszer ellátás hatékonyságának elemzése (Hadmérnök, VII. Évfolyam 4. szám)
[17] 48/2012. (VII. 19.) HM utasítás módosítása a 88/2012. (XII. 18.) HM utasítással
[18] 37/2013. (HK 6.) HM KÁT–HVKF együttes intézkedés: A honvédelmi szervezetek által lefolytatandó keretmegállapodásos eljárások szabályairól

– *„R1[19]. 1. melléklet XXIV. fejezet a) pontjában meghatározott szolgáltatás megrendelésére vonatkozó keretmegállapodás kezdeményezésére, valamint a megkötött keretmegállapodásos eljárás második részében történő részvételre kizárólag az MH Katonai Közlekedési központ jogosult.”*

A HM tárca belső szintű szabályzója lehetővé tette, hogy a polgári eszközzel végrehajtott légiszállítások beszerzése két szinten kerüljön biztosításra.

Álláspontom szerint a keretmegállapodásos eljárás kialakítása a honvédségi ellátásban alapos felmérést és körültekintést igényel.

A következőkben a véleményemet alátámasztandó a stratégiai légiszállításokra vonatkozó korábban megkötött komplex szállítmányozói keretszerződéseket és a bevezetendő keretmegállapodások előnyeit és hátrányait hasonlítom össze:

Keretmegállapodás előnyei:

- *Szerződő fél száma* keretszerződésnél egy, keretmegállapodás esetén több (három vagy több).
- Az *ellenszolgáltatás ára* keretszerződés esetén fix; a keretmegállapodásnál – meghatározott feltételekkel, de – változtatható.
- A *termékek és szolgáltatások* keretszerződés esetén rögzítettek, a keretmegállapodásnál változtatható.
- A keretszerződés *időtartama* egy-két év, a keretmegállapodás esetén 4 – bizonyos esetben több – év.

Összességében a keretmegállapodással meghatározott útvonalakra előre biztosítható a polgári kapacitás igénybevétele, amely nem jár előzetes kötelezettséggel, de gyorsan igényelhetővé válik.

Keretmegállapodás hátrányai:

- Amennyiben egy ajánlattevővel kerül keretmegállapodás megkötésre, a *piaci árverseny nem érvényesül.*
- Több ajánlattevővel történő keretmegállapodás megkötése esetén *felmerülhet a kartellezés lehetősége.*
- További szereplő – fuvarozó – nem vonható be, ezáltal az *eredeti igényektől eltérő útvonal vagy szállító kapacitás* – amennyiben a szerződő fél ezzel nem rendelkezik – csak külön beszerzési eljárásban biztosítható.

Összességében a keretmegállapodás esetén új fuvarozó bevonására nincs lehetőség, így a rendszer a katonai légiszállítás ellátásban csak korlátozottan alkalmazható.

DINAMIKUS BESZERZÉSI RENDSZER

Általános ismertető

A stratégiai légiszállítás beszerzésével kapcsolatosan az alábbi elvárások fogalmazhatóak meg:

- Beszerzési eljárás fajtáitól[20] függetlenül legyen alkalmazható;
  a) a hatályos „közbeszerzésekről” szóló 2011. évi CVIII. törvény (a továbbiakban: Kbt.) 3. sz mellékletében szerepel a *„légi személyszállítási és teherfuvarozási szolgáltatások”.*
  b) a hatályos *„védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról”* szóló

[19] R1.: a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló 228/2004. (VII. 30.) Korm. rendelet

[20] Kbt. 83. §, szerinti, valamint a Kbt. kivételi körébe tartozó beszerzések esetén is

228/2004. (VII. 30.) Korm. rendelet 8. sz mellékletében szintén szerepel a *„légi személyszállítási és teherfuvarozási szolgáltatások”*.

- Folyamatosan nyitott rendszer legyen. Az eddigiekben lefolytatott közbeszerzési eljárást követően már nincs mód – csak újabb közbeszerzési eljárás lefolytatásával – újabb piaci szereplők bevonására, így az olcsóbb (vagy összességében legelőnyösebb) szolgáltatóval történő szerződéskötés nem lehetséges;
- Hosszabb távon (legalább 2-4 év) a rendszer külön beavatkozás nélkül is legyen működő képes (ne kelljen évről-évre ugyanazon beszerzési eljárást ismételten lefolytatni);
- A légiszállítási szolgáltatást nyújtó cégek legyenek képesek a feladat végrehajtására, vagyis előre meghatározott jogi, pénzügyi és műszaki feltételek alapján legyenek alkalmasak. Az alkalmasság vizsgálatának minden esetben előre kell megtörténnie.
- A beszerzési eljárások lehető legrövidebb időtartam alatt történő lefolytatása a katonai célok érvényre juttatása érdekében;
- Azonnal lehessen kiválasztani a konkrét feladatnak megfelelő – optimálisabb – piaci szolgáltatót, amely a kiválasztási folyamat automatizálását is jelenti egyben;
- Közpénzek felhasználásának jogszabályban meghatározott alapelveinek biztosítása: *„nyilvánosság, verseny tisztasága, esélyegyenlőség; az egyenlő bánásmód alkalmazása a nemzeti elbánás fenntartása mellett; az átláthatóság, a rendeltetésszerű joggyakorlás követelménye, a jóhiszeműség és a tisztesség elve”*[21]

A fenti szempontok alapján belátható, hogy eleve nehézséget okoz annak meghatározása, hogy az adott beszerzést mely jogszabály alapján szükséges lefolytatni. A korábban alkalmazott beszerzési rendszerekre elmondható, hogy nem voltak képesek biztosítani az általam felsorolt elvárásokat.

- Saját légi kapacitás igénybevétele esetében más piaci szereplő bevonásával nem számolhatunk, így nincs összehasonlítási alap a gazdaságosságra, optimális kihasználtságra;
- Szállítmányozó esetén sincs lehetőség felmérni a gazdaságossági szempontot, mivel e tekintetben teljes mértékben a szállítmányozóra vagyunk utalva. Szállítmányozó cseréje pedig új közbeszerzési eljárást von maga után.
- Többnemzeti megállapodás esetén kijelenthető, hogy a kisebb kapacitást igénybe vevő nemzet a nagyobb nemzetre van utalva (a nagyobb kapacitás igénybevétele a piaci versenyben előnyben részesül)

A fenti problémák megoldására az Európai Unióban 2006-ban elfogadott és a legtöbb tagország által gyakran alkalmazott beszerzési módszert – a dinamikus beszerzési rendszert – kívánom bemutatni:

A dinamikus beszerzési rendszer olyan, mint egy keretmegállapodás, *kivéve,* hogy a „szerződés” időtartama alatt egyéb gazdasági szereplők (beszállítók) is nyújthatnak be ajánlatokat, és ha megfelelnek a közzétett kritériumoknak, csatlakozhatnak a rendszerhez.

Nemzetközi szabályozás

Az Európai Unió 2004/18/EK közbeszerzési irányelve szerint: „olyan, gyakori beszerzések lebonyolítására szolgáló, teljes mértékben elektronikus folyamat, amelynek jellemzői – a piacon általában rendelkezésre álló formában – megfelelnek az ajánlatkérő szerv által meghatározott követelményeknek, és amelynek működése határozott idejű, és érvényességi ideje alatt bármely olyan gazdasági szereplő számára nyitott, aki, illetve amely megfelel a kiválasztás szempontjainak és benyújtotta az ajánlattételhez szükséges dokumentációnak megfelelő előzetes ajánlatát.”

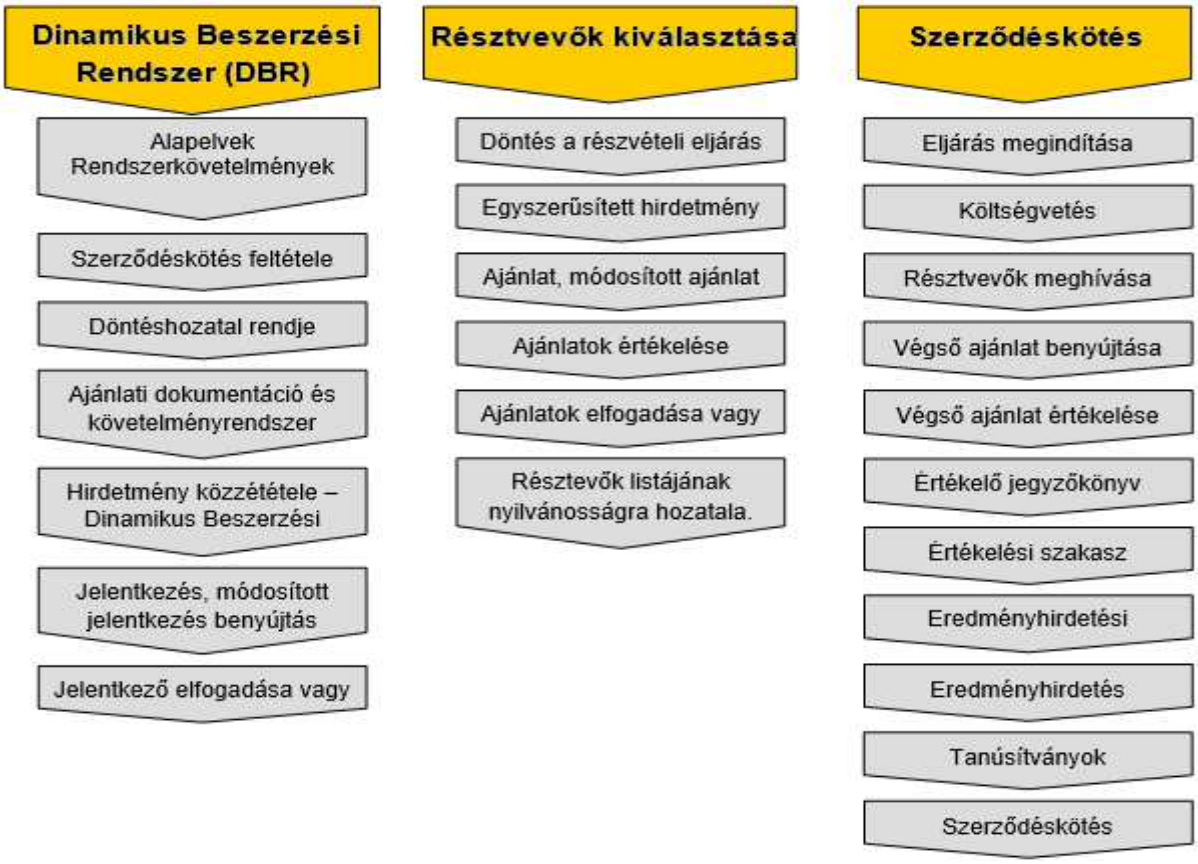
[21] Kbt. I. fejezet

A dinamikus beszerzési rendszer működése legfeljebb négy évig tarthat, kivéve a kellően indokolt, rendkívüli eseteket.

Az irányelv indoklásában kifejtették, hogy az egyes új, elektronikus beszerzési módszerek folyamatosan fejlődnek. E módszerek segítik a verseny fokozását és a közbeszerzés egyszerűsítését, különösen azáltal, hogy e módszerek alkalmazásával idő és pénz takarítható meg. Az ajánlatkérő szervek alkalmazhatnak elektronikus beszerzési módszereket, feltéve, hogy azok alkalmazása megfelel ezen irányelv szabályainak, valamint az egyenlő bánásmód, a megkülönböztetés-mentesség és az átláthatóság elvének. Ha e feltételek teljesülnek, az ajánlattevő által – különösen dinamikus beszerzési rendszer keretében – benyújtott ajánlat az adott ajánlattevő elektronikus katalógusában is megtestesülhet, amennyiben az ajánlattevő az ajánlatkérő szerv által ezen irányelv alapján kiválasztott kommunikációs eszközt használja.

Megállapítható, hogy az ajánlatkérő szervezet dinamikus beszerzési rendszert hozhat létre és működtethet, amelynek célja, hogy meghatározott közbeszerzések megvalósítása érdekében lefolytatandó eljárásokban a részvételre jogosultakat előre kiválassza.

A dinamikus beszerzési rendszer fő elemeit az alábbi ábra szemlélteti:



3. ábra. Dinamikus beszerzési eljárás elemei
(Forrás: European Vortal Academy: Dynamic Purchasing System) [22]
Fordította: Derzsényi Attila

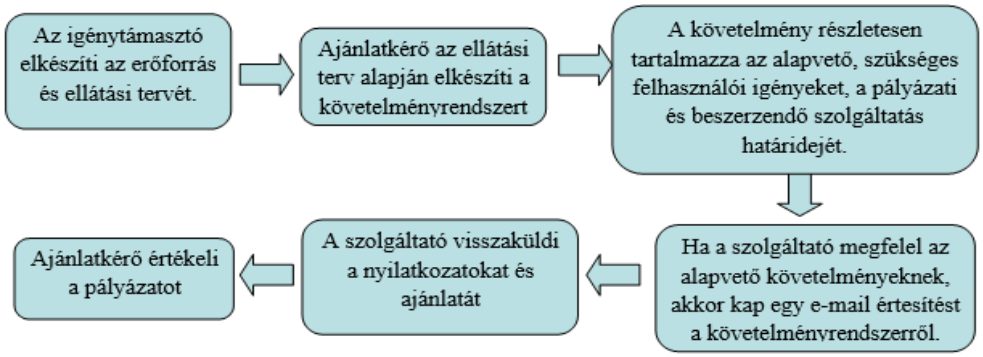
[22]European Vortal Academy: Dynamic Purchasing System
http://worldwide.vortal.biz/files/vortal_es/eVA_White_Paper_-_Dynamic_Purchasing_Systems_-_Mar2013.pdf

Az irányelv alapján a dinamikus beszerzési rendszer használatakor:

- A rendszer létrehozása és a szerződések odaítélése céljából csak elektronikus eszközöket használhat.
- Az ajánlatkérő a közbeszerzési jogszabályban rögzített nyílt eljárás szabályait alkalmazza, egészen a megkötendő szerződések odaítéléséig az alábbi kiegészítésekkel:
  a) hirdetményt tesz közzé, amelyben egyértelműen közölni kell, hogy dinamikus beszerzési rendszer kerül alkalmazásra;
  b) az ajánlattételhez szükséges dokumentációban fel kell tüntetni egyebek mellett a beszerzések jellegét, továbbá a beszerzési rendszerrel, a felhasznált elektronikus eszközökkel és a csatlakozás műszaki szabályaival és leírásaival kapcsolatos valamennyi szükséges információt;
  c) a hirdetmény közzétételétől kezdve és a rendszer érvényességének időtartama alatt, elektronikus úton korlátlan, közvetlen és teljes körű hozzáférést kell nyújtani az ajánlattételhez szükséges dokumentációhoz és minden kiegészítő irathoz, a hirdetményben pedig feltünteti azt az internetcímet, amelyen e dokumentumok megtekinthetők.
- Valamennyi, a kiválasztási szempontokat teljesítő, az ajánlattételhez szükséges dokumentációnak és az esetleges kiegészítő iratoknak megfelelő előzetes ajánlatot benyújtó ajánlattevőt fel kell venni a rendszerbe;
- Biztosítani kell valamennyi gazdasági szereplő számára annak lehetőségét, hogy előzetes ajánlatot nyújtson be, és felvételt nyerjen a rendszerbe. Az ajánlatkérő az előzetes ajánlat benyújtásától számított legfeljebb 15 napon belül elvégzi az értékelést.
- Az ajánlatkérő leghamarabb köteles értesíteni az ajánlattevőt a dinamikus beszerzési rendszerbe való felvételéről, illetve előzetes ajánlatának elutasításáról.

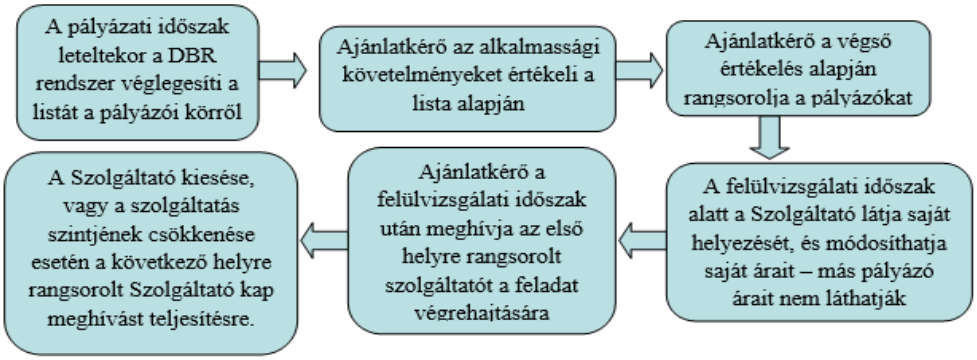
4. ábra. Dinamikus beszerzési rendszerhez (DBR) csatlakozás menete
(Forrás: Southend-on-Sea Borough Council pályázati dokumentum)
Fordította: Derzsényi Attila

- A kötelezettségvállalással járó szerződés ajánlati felhívás alapján jön létre. Az ajánlati felhívás kibocsátása előtt az ajánlatkérő szerv egyszerűsített ajánlati felhívást tesz közzé, amelyben valamennyi érdekelt gazdasági szereplőt arra hívja fel, hogy az egyszerűsített felhívás elküldésétől számított 15 napnál nem rövidebb határidőn belül nyújtsa be előzetes ajánlatát. Az ajánlatkérő szerv addig nem folytathatja az ajánlattételi felhívási eljárást, amíg valamennyi, az említett határidőn belül beérkezett előzetes ajánlat értékelését be nem fejezte.

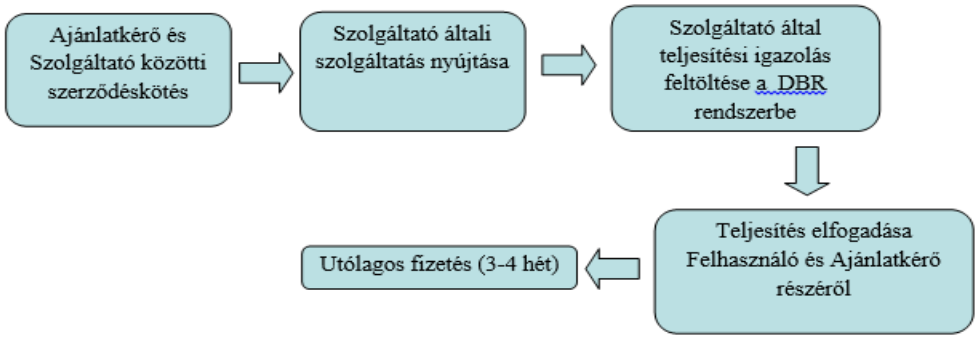


5. ábra. Ajánlatkérő pályázati felhívás elkészítése
(Forrás: Southend-on-Sea Borough Council pályázati dokumentum) [23]
Fordította: Derzsényi Attila

– Az ajánlatkérő szerv annak az ajánlattevőnek ítéli oda a szerződést, amely, illetve aki a dinamikus beszerzési rendszer létrehozásáról szóló hirdetményben megállapított bírálati szempontok alapján a legjobb ajánlatot tette.



6. ábra. Értékelés menete
(Forrás: Southend-on-Sea Borough Council pályázati dokumentum)[24]
Fordította: Derzsényi Attila



7. ábra. Kifizetés menete
(Forrás: Southend-on-Sea Borough Council pályázati dokumentum) [25]
Fordította: Derzsényi Attila

A fenti rendszer egy Angliában már alkalmazott egyedi folyamatot mutat be, azonban a lényeges elemei minden dinamikus beszerzési rendszer használata esetén megtalálható.

[23] Southend-on-Sea Borough Council pályázati dokumentum http://demand.sproc.net/pdfs/creating-requirement-flowchart.pdf
[24]Southend-on-Sea Borough Council pályázati dokumentum http://demand.sproc.net/pdfs/tender-been-submitted.pdf
[25] Southend-on-Sea Borough Council pályázati dokumentum http://demand.sproc.net/pdfs/how-you-get-paid.pdf

Nemzetközi tapasztalat

Jelenleg az Európai Unióban a dinamikus beszerzési rendszer alkalmazása igen elterjedt gyakorlat. A TED26,azaz az Európai Unió hivatalos lapjának vizsgálata alapján a cikk megírásának időpontjában27 is 84 db érvényes hirdetmény (ajánlati felhívás) jelent meg, kimondottan ezen rendszer alkalmazására. Országonkénti megoszlása a következő:

- Egyesült Királyság 23 db
- Németország 18 db
- Hollandia 16 db
- Litvánia 14 db
- Olaszország 6 db
- Cseh Köztársaság 2 db
- Franciaország 2 db
- Spanyolország 2 db
- Dánia 1 db

A rendszer alkalmazása termékenként/szolgáltatásonként (CPV kódok alapján) is eltérő képet mutat:

- Alapanyagok és Késztermékek (45). Pl (etc.): Orvosi felszerelések, gyógyszerek szállítása; irodai és számítástechnikai gépek, berendezések
- Technológia és Technika (42). Pl. (etc): Orvosi felszerelések, gyógyszerek és testápolási termékek; irodai és számítástechnikai gépek, berendezések és kellékek, a bútorzat és a szoftvercsomagok kivételével; rádiós, televíziós, hírközlési, távközlési és kapcsolódó berendezések
- Építési beruházás és Ingatlanok (16). Pl (etc): Építészeti, építési, mérnöki és vizsgálati szolgáltatások; szennyvíz- és hulladéktisztítási és környezetvédelmi szolgáltatások
- Számítástechnika és Kapcsolódó szolgáltatások (14). Pl (etc): IT-szolgáltatások: tanácsadás, szoftverfejlesztés, internet és támogatás; irodai és számítástechnikai gépek, berendezések és kellékek, a bútorzat és a szoftvercsomagok kivételével; Szoftvercsomag és információs rendszerek
- Egyéb szolgáltatások (13). Pl (etc): Egészségügyi és szociális gondozási szolgáltatások; egyéb közösségi, szociális és személyi szolgáltatások
- Nyomtatás és Közzététel (11). Pl (etc): Irodai és számítástechnikai gépek, berendezések és kellékek, a bútorzat és a szoftvercsomagok kivételével; üzleti szolgáltatások: jog, marketing, tanácsadás, munkaerő-felvétel, nyomtatás és biztonság
- Szállítás és Kapcsolódó szolgáltatások (11). Pl (etc): Szállítási szolgáltatások (kivéve szemétszállítás); szállítófelszerelések és kiegészítő szállítási cikkek (3)
- Energia és Kapcsolódó szolgáltatások (5)
- Környezetvédelem és Egészségügy (4)
- Bányászat és Nyersanyagok (3)
- Kutatás és Fejlesztés (3)
- Oktatás (3)
- Honvédelem és biztonság (1) (Megj: Ilyen típusú eljárásokban nem kerül sor a részletes tartalom nyilvánosságra hozatalára)

Az angol beszerzési gyakorlatban kiemelkedő a dinamikus beszerzési rendszer alkalmazása a szállítási szolgáltatásokra vonatkozóan.. Az oktatási, szociális ellátási, közösségi, általános

[26] Tenders Electronic Daily
[27] 2013. október 09.

szállítási és taxi szolgáltatásokra például számos város (Hampshire[28], Devon Megyei Tanács[29], Lincolnshire,[30] stb) ír ki közbeszerzési eljárást ezen rendszer alkalmazásával.

A fenti felsorolás alapján belátható, hogy a dinamikus beszerzési rendszer igen széles körben alkalmazható. Fő jellemzőjük, hogy olyan termékek, vagy szolgáltatások beszerzésére irányulnak, amelyre vonatkozó igények gyakran, visszatérően jelentkeznek.

Példát is megemlítve, elsősorban a NATO Ellátási Ügynöksége az NSPA[31] által alkalmazott eljárásmódot tartom célszerűnek kiemelni:

A NATO Ellátó Ügynökség (NSPA) - NATO fenntartási és ellátási ügynöksége (NAMSA) - a tagállamok és a NATO szervezetei részére haditechnikai és egyéb eszközök, alkatrész és szolgáltatások - haditechnikai eszköz fenntartás, javítás, raktározás, infrastrukturális beruházások, szállítmányozás, mérnök-műszaki és technikai támogatás, lőszer, robbanóanyag és kivont haditechnikai eszközök hatástalanítása, megsemmisítése - beszerzése területén nyújtja szolgáltatását.

- A NSPA csak olyan cégeket hív meg tenderre, akik szerepelnek/már regisztráltak a NAMSA adatbázisában (Source File).
- A haditechnikai eszközök és szolgáltatások esetében szükséges a „NATO Beszállítói minősítés" megléte, más kereskedelmi kategóriákban ez nem előírás.
- A regisztrált cégeknek rendszeres időközönként szükséges frissíteni a tevékenységi/képesség listájukat.

A rendszer egy állandó NATO beszállítói kör kialakítását és fenntartását tűzte célul, melyen belül a „NATO Beszállításra Alkalmas" címet nyert cégekre vonatkozóan a NATO tagország képes felelősen garanciát vállalni ezek szakmai, gazdasági, pénzügyi, és szükség esetén biztonsági megfelelőségéért.

A NATO Beszállítói Rendszer elve az, hogy létrejöjjön egy olyan stabil beszállítói bázis, melyben a résztvevő gazdálkodó szervezetek rendelkeznek hosszú távú stratégiával. Teljesítményük állandó, magas színvonalú, így egy tenderfelhívás megjelenésének pillanatában készek és képesek bekapcsolódni egy NATO érdekében történő pályázati eljárásba.

A rendszer ugyanazon elven működik, mint a dinamikus beszerzési rendszer, azzal a különbséggel, hogy itt az időtartam nincs korlátozva. Azonosság:

- Előzetes elektronikus regisztráció szükséges az alkalmassági feltételek megállapítása céljából;
- Beszerzés rövid idő alatt végrehajtásra kerül, a felhívás csak a regisztrált tagok részére kerül megküldésre;
- Nincs előzetes kötelezettségvállalás

Hazai szabályozás sajátosságai

A korábbi közbeszerzésekről szóló törvény módosításáról szóló 2005. évi CLXXII. törvény már bevezette a dinamikus beszerzési rendszer intézményét, amely 2007. január 1-jén léptette hatályba az új intézményre vonatkozó keretszabályozást.

A Kbt.-ben foglalt rendelkezések alapján azonban a dinamikus beszerzési rendszer csak akkortól alkalmazható, amikor annak részletes szabályait külön jogszabály már meghatározta.

A jogintézményre vonatkozó uniós szabályok hazai implementálását követően, a dinamikus beszerzési rendszer alkalmazás részletes szabályainak megalkotására nemzeti szinten kell sorra

[28] Ajánlati Felhívás Hampshire http://euroalert.net/en/contracts.aspx?idl=2122684
[29] Ajánlati Felhívás Devon Megyei Tanács http://tenderise.eu/notice/334702-2013
[30] Ajánlati Felhívás Lincolnshire https://www.yortender.co.uk/procontract/supplier.nsf/frm_opportunity?openForm&opp_id=OPP-HIS-YORE-93DK8L&contract_id=CONTRACT-YORE-93DJLS&org_id=ORG-YORE-8YRK33&from
[31] NATO Maintenance and Support Agency

kerülnie. A Kbt. alapján erre a Kormány kapott felhatalmazást, azonban tekintettel arra, hogy a vonatkozó jogszabály hazánkban mindezidáig nem született meg, a dinamikus beszerzési rendszerek alkalmazására jelenleg Magyarországon még nincs lehetőség[32]. Igaz ugyan, hogy az elektronikusan gyakorolható eljárási cselekményeket és az elektronikus árlejtés szabályait[33] külön kormányrendelet ugyan tartalmazza, de ezek a rendelkezések – az elektronikus jelleg ellenére – nem a dinamikus beszerzési rendszer szabályozását jelentik.

A hivatkozott[30] kormányrendelethez fűzött kommentár szerint: „*Az ún. Dinamikus Beszerzési Rendszer alkalmazására jelenleg hazánkban nincs lehetőség, mivel az ezt szabályozó végrehajtási rendelet, közösségi gyakorlat híján még nem készült el.*"

Álláspontom szerint azonban – az általam is feltárt – jelenlegi Európai Uniós gyakorlatok tükrében kijelenthető, hogy elegendő tapasztalat áll rendelkezésre a hazai szabályozás kialakítására.

Összegzés

A stratégiai légiszállítás beszerzés központú megközelítésével megállapítható, hogy számos beszerzési módszer alapján – a korábbi beszerzési eljárásoktól eltérően – gyorsabban, hatékonyabban lehetne biztosítani az ellátást.

Kutatásom során megállapítottam, hogy az Európai Unióban már régóta alkalmazott dinamikus rendszer megvalósíthatóságával, alkalmazhatóságával, hatékonyságával összefüggő tanulmányok léteznek, azonban erre vonatkozóan hazai szakirodalom még nem készült.

Annak ellenére, hogy a dinamikus beszerzési rendszer hazánkban még nem alkalmazható, az Európai Unió informatikai piaca felkészült. A katonai beszerzés vonatkozásában is célszerűnek tartom az előkészületeket, és a későbbiekben a rendszer alkalmazását.

A stratégiai légiszállítás – hasonlóan az NSPA beszerzési eljárásához, vagy az angol városi közlekedési szolgáltatások beszerzéséhez – a dinamikus beszerzési rendszer alkalmazásával:

- Képessé válik gyorsabb, hatékonyabb ellátást biztosítani;
- Az előzetes piackutatást felváltva, a lehető legszélesebb gazdasági szereplők ajánlatainak összehasonlítása válik lehetővé;
- Váratlan, azonnali szállítási helyzetekre is képes megoldást biztosítani;
- A szállítmányozó szerepét átvéve költséghatékony (idő, pénz, papír) rendszer alakítható ki;
- A rendszer működésének feltétele az erre speciálisan kialakított informatikai rendszer, amely a szoftver megvásárlásával, vagy az IT piacon szolgáltatás formájában már elérhető.

Célszerűnek tartom az általam felvázolt rendszer más tudományágak (jog, informatika) szempontjából történő kutatását, tanulmányozását is a meglévő külföldi gyakorlati tapasztalatok alapján.

32 A Közbeszerzések Tanácsa Elnökének tájékoztatója a dinamikus beszerzési rendszer alkalmazásáról (Közbeszerzési Értesítő 2007. évi 7. szám; 2007. január 17.)

33 A közbeszerzési eljárásokban elektronikusan gyakorolható eljárási cselekmények szabályairól, valamint az elektronikus árlejtés alkalmazásáról szóló 257/2007. (X. 4.) Korm. rendelet

Felhasznált irodalom

[1] MTI hírek: Állami légi szállító flottát tervez a kormány (http://www.honvedelem.hu/cikk/38640) (letöltés ideje: 2013. szeptember 17.)

[2] Szászi Gábor: A Malév felszámolásának várható hatásai a katonai légiszállítási feladatok végrehajtására; Repüléstudományi Közlemények 2012. évi 2. szám pp.1036-1045 (http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/86_Szaszi_Gabor.pdf) (letöltés ideje: 2013. szeptember 17.)

[3] Szarvas László: Stratégiai Légiszállítási Képesség – egy új többnemzeti megoldás 2008/7 Nemzet és Biztonság pp.60-76 (http://www.nemzetesbiztonsag.hu/cikkek/szarvas_laszlo-strategiai_legi_szallitasi_kepesseg___egy_uj_tobbnemzeti_megoldas.pdf) (letöltés ideje: 2013. szeptember 17.)

[4] Európai Biztonsági Stratégia: Biztonságos Európa egy jobb világban (http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568HUC.pdf) (letöltés ideje: 2013. szeptember 17.)

[5] WebLogTrade: A szállítmányozás és a fuvarozás jellemzői (http://hu.wiki.weblogtrade.eu/Sz%C3%A1ll%C3%ADtm%C3%A1nyoz%C3%A1s_%C3%A9s_fuvaroz%C3%A1s) (letöltés ideje: 2013. szeptember 28.)

[6] Magyar Logisztikai Egyesület: A közlekedés lokális fejlesztése a globalizáció tükrében (Tanulmány, 2007. szeptember)(http://www.tranzitonline.eu/cikkek/a-kozlekedes-lokalis-fejlesztese-a-globalizacio-tukreben)

[7] Honvédelmi Minisztérium: NATO Stratégiai Légiszállítási Program (http://www.kormany.hu/hu/honvedelmi-miniszterium/hirek/nato-strategiai-legiszallitasi-program-sac) (letöltés ideje: 2013. szeptember 28.)

[8] Vigh Attila A Honvédelmi Minisztérium Fejlesztési és Logisztikai Ügynökség Anyagi-Technikai és Közlekedési Igazgatóság Közlekedési Osztály helye, szerepe a missziós logisztikai támogatás rendszerében (Hadmérnök, III. Évfolyam 3. szám) (http://hadmernok.hu/archivum/2008/3/2008_3_vigh.pdf) (letöltés ideje: 2013. szeptember 17.)

[9] Derzsényi Attila : Az élelmiszer ellátás hatékonyságának elemzése (Hadmérnök, VII. Évfolyam 4. szám) (http://hadmernok.hu/2012_4_derzsenyi.pdf)

[10] Derzsényi Attila: Keretmegállapodásos eljárás alkalmazása a honvédségi ellátásban (Katonai Logisztika Online 2013/1 szám) (http://www.honvedelem.hu/container/files/attachments/39610/kl-2013-1.pdf)

[11] Dr.Tátrai Tünde: Szabályozási kérdések az elektronikus közbeszerzésben (http://www.kozbeszkut.hu/images/stories/pdf/ekozbeszerzes_szab_tamop.pdf) (letöltés ideje: 2013. október 05.)

[12] Dr. Michael Varney: E-Procurement—current law and future challenges ERA Forum July 2011, Volume 12, Issue 2, pp 185-204 (http://link.springer.com/article/10.1007/s12027-011-0217-9) (letöltés ideje: 2013. október 05..)

[13] Arrowsmith, Sue: Modernising the EU's public procurement regime: a blueprint for real simplicity and flexibility. Public Procurement Law Review, 21 . pp. 71-82. ISSN 0963-8245

(http://eprints.nottingham.ac.uk/1685/1/eprints_pplr_blueprint_for_reform_final.pdf) (letöltés ideje: 2013. október 05.)

[14] Izzet Gökhan Özbilgin: World Conference on Information Technology (Procedia Computer Science, Volume 3, 2011, Pages 1571–1575 (http://www.sciencedirect.com/science/article/pii/S1877050911000524#) (letöltés ideje: 2013. október 05.)

[15] European Vortal Academy: Dynamic Purchasing System (http://worldwide.vortal.biz/files/vortal_es/eVA_White_Paper_-_Dynamic_Purchasing_Systems_-_Mar2013.pdf) (letöltés ideje: 2013. október 06)

[16] Beuter, Rita. (2005) *European Public Procurement Reform: Main Innovations in the Public Sector Directive – A Preliminary Assessment.* EIPAScope, 2005 (3). pp. 5-11. (http://aei.pitt.edu/5952/1/Scope2005_3_1%282%29.pdf) (letöltés ideje: 2013. október 06.)

[17] Southend-on-Sea Borough Council (SBC): Southend DPS - Contract notices (http://demand.sproc.net/southend-dps.aspx) (letöltés ideje: 2013. október 12.)

[18] Southend-on-Sea Borough Council pályázati dokumentum (http://demand.sproc.net/pdfs/joining-DPS-flowchart.pdf) (letöltés ideje: 2013. október 12.)

[19] NSPO 4200 sz. rendelete: NSPO Ügynökség közbeszerzési szabályzata (NSPO AGENCY SUPERVISORY BOARD 26 June 2013) (http://translate.googleusercontent.com/translate_c?depth=1&hl=hu&prev=/search%3Fq%3Dnspa%2Bprocurement%26client%3Dfirefox-a%26hs%3DXX9%26rls%3Dorg.mozilla:hu:official&rurl=translate.google.hu&sl=en&u=http://www.nspa.nato.int/pdf/procurement/NR-4200_e.pdf&usg=ALkJrhhWHgq0iB7G8W45Ror8hSkKbZj6mg) (letöltés ideje: 2013. október 12.)

[20] A Közbeszerzések Tanácsa Elnökének tájékoztatója a dinamikus beszerzési rendszer alkalmazásáról ((Közbeszerzési Értesítő 2007. évi 7. szám; 2007. január 17.)

Hivatkozott jogszabályok jegyzéke (Complex jogtár):

[1] Európai Unió 2004/18/EK közbeszerzési irányelve;

[2] A közbeszerzésekről szóló törvény módosításáról szóló 2005. évi CLXXII. törvény;

[3] A közbeszerzésekről szóló 2011. évi CVIII. törvény;

[4] A védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló 228/2004. (VII. 30.) Korm. rendelet;

[5] A közbeszerzési eljárásokban elektronikusan gyakorolható eljárási cselekmények szabályairól, valamint az elektronikus árlejtés alkalmazásáról szóló 257/2007. (X. 4.) Korm. rendelet;

[6] A honvédelmi szervezetek beszerzéseinek eljárási rendjéről szóló 48/2012. (VII. 19.) HM utasítás módosítása a 88/2012. (XII. 18.) HM utasítással;

[7] 37/2013. (HK 6.) HM KÁT–HVKF együttes intézkedés: A honvédelmi szervezetek által lefolytatandó keretmegállapodásos eljárások szabályairól.

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Földi László – Kuti Rajmund – Sulányi Péter – Pataki János
foldi.laszlo@uni-nke.hu - kutirajmund@t-online.hu - speter@suprex.hu - bmp1k3@gmail.com

AUFGABENSTELLUNG UND ROLLE DER WERKFEUERWEHR BEI EINEM MULTINATIONALENUNTERNEHMEN

Abstrakt

Die Feuerwehr am Standort nimmt eigentlich operative Brandschutzaufgaben wahr. Auf der strategischen Ebene werden Brandschutzaufgaben vom Leiter der organisatorischen Einheit zur Wahrung der Sicherheit (Unternehmenssicherheit) wahrgenommen. Die Standortfeuerwehr muss so aufgestellt und ausgerüstet werden, dass sie in der Lage ist, jeden während ihrer Tätigkeit auf ihrem Gebiet entstandenen Brand selbständig zu löschen, mit Kräften und Mitteln gemäss der Vorschriften der erstinstanzlichen Behörde. Der Personalbestand, die Feuerwehrfahrzeuge, die Ausrüstung, individuelle und kollektive Schutzmittel, zur Löschung und Prävention von Bränden notwendige Materialien, sowie vorgeschriebene Reserven müssen bereitgehalten und bei Bedarf auf Anweisung des Operators der Standortfeuerwehr eingesetzt werden.

Egy létesítményi tűzoltóság lényegében operatív tűzvédelmi feladatokat lát el. A stratégiai szintű tűzvédelmi feladatokat a cég biztonsági osztályának szervezetszerű vezetője végzi (vállalati biztonság). A létesítményi tűzoltóságot oly módon kell felállítani és felszerelni, hogy képes legyen működése során a területén keletkezett bármilyen tűz önálló eloltására az elsőfokú hatóság előírásainak megfelelő erőkkel és eszközökkel. A személyi állományt, a tűzoltó gépjárműveket, a felszerelést, az egyéni és kollektív védelem eszközeit, a tűzoltáshoz és a tűzmegelőzéshez szükséges anyagokat valamint az előírt tartalékokat készenlétben kell tartani és szükség szerint bevetni a létesítményi tűzoltóság operátorának intézkedésére.

Kernbegriffe: *Brandschutz, Standortsicherheit, Sicherheit, Ungarn ~ tűzvédelem, létesítményi tűzoltóság, biztonság, Magyarország*

EINLEITUNG

Aufgrund von Schadensfällen und den daraus resultierenden Erfahrungen ist bekannt, dass Baustellen im Allgemeinen ein hohes Risikopotenzial für Brandschäden aufweisen können.

Deswegen sind Großbaustellen brandschutztechnisch sehr kritisch zu beurteilen. Die Gegenwart zeigt jedoch, dass mit geeigneten Schutzmaßnahmen ein entsprechender Sicherheitsstandard des Brandschutzes erreicht werden kann.

Die nachstehenden Schutzmaßnahmen– verbunden mit regelmäßigen Kontrollen durch eigene Mitarbeiter bzw. externen Stellen – dienen zur Erreichung und Erhaltung eines guten Sicherheitsstandards für die Zukunft.

Gesetzliche, behördliche, mit dem Versicherer vereinbarte oder sonstige Sicherheitsvorschriften sind einzuhalten und bleiben von diesen Empfehlungen unberührt.

Zweck

Brandgefahren stellen für jeden Industrie- und gewerblichen Betrieb eine ernste Bedrohung dar. Ein Brand kann nicht nur Gesundheit und Leben von Menschen gefährden, sondern darüber hinaus auch Lieferungsausfälle, Markteinbußen, Imageverluste oder nachteilige rechtliche Konsequenzen zur Folge haben, die für Unternehmen existenzbedrohend sein können.

Unternehmen können vor diesen Gefahren weder durch eine Feuer- noch eine brandbedingte Betriebsunterbrechungsversicherung bewahrt werden.

Zur Koordination und Durchführung von Brandschutzmaßnahmen hat sich die Ernennung einer persönlich und fachlich geeigneten Brandschutzabteilung bewährt.

Im Falle einer Werksfeuerwehr trägt das Unternehmen als Betreiber der Brandschutzanlage die Verantwortung für den Schutz der beschäftigten Arbeitnehmer und Sachgüter. Die Werksfeuerwehr muss die Menschen außerhalb des Betriebes und auch die Umwelt schützen. [1]

Versicherungsrechtlich ist das Unternehmen verpflichtet, Brandschäden abzuwenden, beziehungsweise zu mindern, ansonsten ist jeder, bei dem Unternehmen beschäftigter Arbeitnehmer, für seinen Arbeitsbereich und im Rahmen seiner Befugnisse und Aufgaben für den Brandschutz verantwortlich.

Bei Beauftragung von Fremdfirmen (Dienstleister) ist ebenfalls das Unternehmen für die Einhaltung der Brandschutzmaßnahmen verantwortlich.

Diese Verantwortung kann im Einzelfall auf die Fremdfirma übertragen werden, um die Lieferantenrisiken reduzieren zu können.

Gesetzliche Bestimmungen und behördliche Vorschriften, die in Ungarn gelten, sowie die Vereinbarungen mit dem Versicherer bleiben unberührt.

Corporate Security-Konzern (strategische) -Ebene[1]

Die Corporate Sicherheit ist eine werksübergreifende Stabsstelle des Unternehmens mit komplexen Aufgabenfeldern, wie z.B. Sicherheitslage, Lagebeurteilung, Informationsschutz, Datenschutz und Datensicherheit, Prototypenschutz, Geheimhaltung, Sicherheitsstandards, Brandschutz, Krisenmanagement, Event Security, Personenschutz.

Im Rahmen des Brandschutzes der Corporate Security wird die Zusammenarbeit der Brandschutzexperten im Unternehmen koordiniert und eine fachliche Unterstützung bei der

[1] Corporate Security=Unternehmenssicherheit: in der unternehmerischen Praxis sind mehrere Strukturmodelle zur Positionierung der Unternehmenssicherheit vorhanden, z.B. drei mögliche Organisationsmodelle:

1. als eigenständige Organisationseinheit, direkt unter der Vorstandsebene
2. als Bestandteil eines übergeordneten Bereiches Riskmanagement oder
3. als Bestandteil eines übergeordneten Bereiches Safety, Security.

Erfüllung gesetzlicher, behördlicher und versicherungsrechtlicher Auflagen gewährleistet - immer risikoorientiert und bedarfsgerecht, unter betriebswirtschaftlichen Gesichtspunkten.

Der Brandschutz ist im Unternehmen sehr genau geregelt, und gehört organisatorisch in den Bereich der Corporate Security.

Die Brandschutzregelungen wurden durch die Organisations-Richtlinie ausgefertigt und festgelegt.

Der vorbeugende Brandschutz umfasst alle Maßnahmen zur Verhinderung eines Brandausbruchs bzw. einer Brandausbreitung sowie die Sicherung der Angriffs- und Rettungswege. Der vorbeugende Brandschutz schafft darüber hinaus die Voraussetzungen für einen wirkungsvollen abwehrenden Brandschutz.

Der Brandschutz umfasst alle Maßnahmen zur Verhinderung einer Brandausbreitung - ebenso, wie die baulichen Brandschutzvorschriften und die geltenden Brandschutzrichtlinien.

Darüber hinaus müssen auch die ungarische Brandschutzgesetzgebung und die ungarischen Brandschutzrichtlinien bzw. die VdS[2] Richtlinien und Merkblätter beachtet werden.

Werksicherheit3 – operative Ebene

Die Werksfeuerwehr ist in die Werksicherheit integriert, und funktioniert als eine Teilabteilung.

Die Werksfeuerwehr ist für die eingebauten Brandschutzanlagen, Brandfrüherkennungssysteme und Brandschutzabtrennanlagen bzw. Brandschutztore, sowie Rauch- und Wärmeanlagen als Betreiber zuständig.

Der abwehrende Brandschutz umfasst alle Maßnahmen im Bereich der eingebauten Löschanlagen und Löschtechnik bzw. Werksfeuerwehrtätigkeiten.

Erfahrungen der Brandfallanalysen

Erfahrungsgemäß liegen allen Schadensereignissen entweder technische Defekte oder insbesondere menschliches Fehlverhalten zu Grunde bzw. sind diese daran zumindest beteiligt.

Dabei entstehen große Brandschäden fast immer durch das Zusammenwirken verschiedener Unzulänglichkeiten innerhalb des betrieblichen Systems. Oft handelt es sich um organisatorische oder technische Mängel, die an und für sich relativ harmlos sind, sich jedoch infolge ungünstiger Umstände zu einer Schadenskette (Kettenreaktion) verbinden.

Vor diesem Hintergrund hat der betriebliche Brandschutz über die gesetzlich geforderten Maßnahmen hinaus in den letzten Jahren immer mehr an Bedeutung gewonnen.

Brandschutzphilosophie

Diese Abhandlung kann durch bauliche, technische und organisatorische Maßnahmen des vorbeugenden und abwehrenden Brandschutzes umgesetzt werden.

Brandschutzmaßnahmen werden fast immer im komplexen betrieblichen Umfeld durchgeführt. Das reibungslose und gut aufeinander abgestimmte Zusammenwirken der verschiedenen Bereiche, wie Management, Organisation und Technik, ist eine unverzichtbare Voraussetzung für den Erfolg nicht nur jeder einzelnen Maßnahme, sondern auch kompletter Brandschutzkonzepte.

Das bedeutet konkret, dass bei dem Unternehmen zunächst eine Sensibilität für den Brandschutz vorhanden sein und eine Brandschutzpolitik, d.h. die klare Bestimmung von Brandschutzzielen, festgelegt und verfolgt werden muss.

---

[2] VdS: Vertrauen durch Sicherheit, VdS ist eine unabhängige Institution, die seit Jahrzehnten für Sicherheit und Vertrauen in den Bereichen Brandschutz und Security sorgt und fortschrittliche Sicherheitskonzepte für bedeutende Industrie- und Gewerbebetriebe, führende Hersteller und Systemhäuser sowie Fachfirmen und Fachkräfte entwickelt.

[3] Die Werksicherheit ist zuständig für die Bereiche abwehrender Brandschutz (Werksfeuerwehr), Werkschutz, Katastrophenschutz, Industriesicherheit, Ermittlungen, Sicherheitsplanung.

Es muss sichergestellt werden, dass nicht nur alle Organisationseinheiten, sondern auch alle Mitarbeiter informiert und verbindlich in die Umsetzung der Brandschutzziele einbezogen werden.

WERKSFEUERWEHR

Der abwehrende Brandschutz zur Brandbekämpfung und zur Abwendung von Gefahren für Menschen und Sachwerte muss jeweils durch die Werksfeuerwehr sichergestellt werden und stellt im Rahmen eines ganzheitlichen Brandschutzkonzeptes die letzte Verteidigungslinie gegen Brände dar.

Die Leistungsfähigkeit der Werksfeuerwehr ist allerdings auf Grund ihrer Personalstärke und Ausrüstung sowie der örtlichen Infrastruktur (z. B. Entfernung des Schutzobjektes zur Feuerwehrwache) nicht unbegrenzt.

Die Werksfeuerwehr ist eine durch das Unternehmen eingerichtete Feuerwehr mit haupt- und nebenberuflichen Kräften zum Schutz des gesamten Werkes und der verschiedenen Produktionseinrichtungen. Mit ihrer Funktion stellt sie einen wesentlichen Bestandteil des betrieblichen Gesamtbrandschutzkonzeptes dar.

Zu ihren Aufgaben gehören vor allem die Verhütung und Minderung von Schäden im Rahmen des vorbeugenden und abwehrenden Brandschutzes, die Verringerung der Hilfsfrist, die qualifizierte Bewältigung von Sondergefahren, und nicht zuletzt auch der Personenschutz.

Die Werksfeuerwehr muss jeweils gemäß der entsprechenden Gesetzgebung [2] und der VdS-Richtlinie 2034 [3] bewertet werden.

Es wird ein Schutzwert für die Werksfeuerwehr ermittelt, der sich daraus ergibt, inwieweit Grund- und Sonderanforderungen erfüllt sowie einige zusätzliche Bewertungskriterien gegeben sind.

Die Kategorisierung bzw. Einstufung der Werksfeuerwehr kann den Bewertungsergebnissen entsprechend vorgenommen werden.

Auf Grund der Einstufungsergebnisse der Werksfeuerwehr kann die Anzahl der Werksfeuerwehrmänner bzw. der Rettungsanlagen und Personalschutzausrüstungen bestimmt werden. [4]

Die ungarische Brandschutzverordnung und die Regelung des Innenministeriums stellt die wichtigste Vorschrift für die Werksfeuerwehr dar. Bemerkung: Die VdS Richtlinie ist in Ungarn nicht gültig, sie darf als Merkblatt benutzt werden.

Werksfeuerwehranforderungen

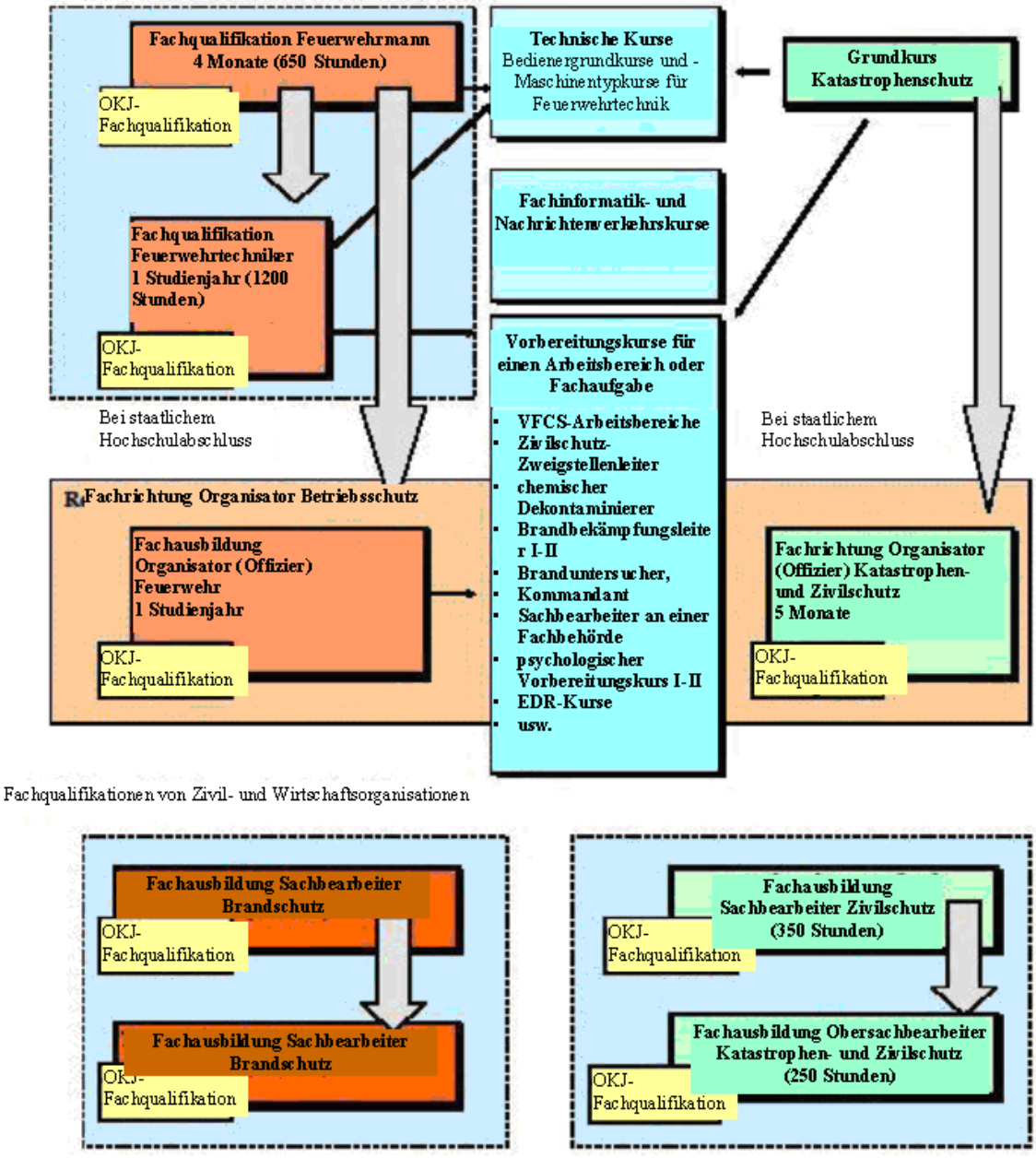
Die Werksfeuerwehr kann auf Grund gesetzlicher Anforderungen notwendig sein.

Die Verhütung und Bekämpfung von Bränden sind Gemeinschaftsaufgaben aller Werksfeuerwehrmänner, die bei dem Unternehmen beschäftigt sind. Bei dem Unternehmen sollten die Aufgaben des abwehrenden Brandschutzes von der brandschutzbehördlich zertifizierten Werksfeuerwehr wahrgenommen werden.

Werksfeuerwehr - Ausbildungskriterien [5]

Das Mitglied der Werksfeuerwehr ist eine Person, die ihre Tätigkeit als Feuerwehrmann auf Grund eines Arbeitsverhältnisses zur Erledigung der fachlichen Aufgaben eines Feuerwehrmannes in einem bereitschaftsdienstähnlichen Dienst ausübt, oder die Erledigung der fachlichen Aufgaben der Werksfeuerwehr leitet, und über die in den Rechtsvorschriften festgelegte Fachausbildung zum Feuerwehrmann verfügt und den an Berufsfeuerwehrmänner gestellten gesundheitlichen, physischen und psychischen Anforderungen entspricht.

Das nachfolgende Bild enthält die bei der Werksfeuerwehr vorgeschriebenen Qualifikationsanforderungen, Formen und Stufen nach Arbeitsbereichen gemäß der im Schulungszentrum für Katastrophenschutz des Innenministeriums verfügbaren Ausbildung.



1. quelle. Die im Schulungszentrum für Katastrophenschutz des Innenministeriums verfügbaren Fachausbildungen, Durchgearbeietet: Hr. Dr. Kuti

Fachausbildung Feuerwehrmann

Bereits erworbene Grundausbildungen, die anerkannt werden können: Die hauptamtlichen Feuerwehrleute einer Werksfeuerwehr müssen eine Feuerwehrmann-Fachausbildung oder einen vor dem 1. Januar 2003 absolvierten sechswöchigen Feuerwehrmann-Grundkurs in Verbindung mit der durch einen dreieinhalb- oder fünfmonatigen Besuch einer Unteroffiziers-Fachschule erworbenen Unteroffiziersqualifikation besitzen.

Zweck der Ausbildung ist, dass sich der Teilnehmer die zur sicheren Durchführung der Aufgaben des Arbeitsbereichs Feuerwehrmann notwendigen Fachkenntnisse in der Grundstufe aneignet.

Grundelemente der Ausbildung:

- Aufbau, Organisation und Führung der Feuerwehr;
- Rechte und Pflichten;
- Regelung des Dienstverhältnisses des Feuerwehrmanns;
- Dienstordnung und Gliederung der Feuerwehr;
- Ordnung der Feuerwehrkaserne;
- Regeln zum Tragen der Uniform, formale Regeln;
- Ausführungsordnung zu Befehlen und Anweisungen;
- Ordnung zur Bereitschaftsdienstablösung;
- Verletzungen, Unfälle;
- Nichtprofessionelle Krankenversorgung, Transport von Verletzten;
- Platzierung der an den einzelnen Kraftfahrzeugen bereitgestellten Ausrüstungen;
- Montage- und Rettungsübungen;
- Montage und Benutzung der Fachausrüstung;
- Entwicklung der körperlichen Kondition, Erfüllung der Elemente der Prüfung zur physischen Kondition;
- Entwicklung der psychischen Belastbarkeit;
- Feuerwehrsport;
- Fachausrüstung im Bereich Saug- und Druckvorrichtungen;
- Manuell montierte Leiter;
- Sonstige Fachausrüstung und Geräte;
- Funktion und Bedienung von Handlöschgeräten;
- Pumpen- und Motorenkenntnisse;
- Funktion und Bedienung der Kleingeräte der Feuerwehr;
- Funktion und Bedienung der Löschfahrzeuge;
- Funktion und Bedienung der Speziallöschfahrzeuge;
- Funktion und Bedienung der verwendeten Nachrichtentechnik;
- Aufgabensystem und Bedienung von Nachrichtenzentralen;
- Erkennung und Einstufung von Gefahrenquellen;
- Sicherheitstechnische Vorschriften zu den verwendeten Geräten;
- Funktion und Bedienung der Atemschutzgeräte;
- Aufbau und Benutzung der Schutzkleidung;
- Verwendung der sonstigen Schutzausrüstung;
- Brandarten und Brandmerkmale;
- Regelungen für die Brandbekämpfung, technische Hilfeleistung sowie;
- Katastrophenabwendung;
- Organisation und Aufgabensystem für die Brandbekämpfung;
- Brandbekämpfungsaufgaben im Freien und in geschlossenen Räumen;
- Technische Hilfeleistung und Katastrophenabwendung.

Die Dauer des Kurses beträgt 650 Stunden.

Fachkurs Feuerwehr-Kraftfahrzeugfahrer, Pumpenbediener

Die Teilnehmer des Kurses lernen den Aufbau, die technischen Parameter und die Besonderheiten der Funktion der Löschfahrzeuge kennen. Sie erhalten Kenntnisse über die Kontroll- und Wartungsaufgaben auf Bedienerebene. Sie erlangen die Fähigkeit, in Kenntnis der taktischen Möglichkeiten des Löschfahrzeuges dieses fachgerecht zu bedienen und zu betreiben.

Hydromechanische Kenntnisse:

- Die mit den Flüssigkeiten verbundenen Grundbegriffe und ihre wichtigen hydromechanischen Eigenschaften.
- Die mit dem Ruhezustand der Flüssigkeiten verbundenen Gesetzmäßigkeiten.
- Das sich auf Flüssigkeiten beziehende Erhaltungsgesetz für Material und Energie.
- Die bei der Strömung von Flüssigkeiten auftretenden Verluste.
- Gleichung der verlorengehenden Energie.

Werksfeuerwehr-Truppenführer - Ausbildungskriterium

Es ist eine abgeschlossene Ausbildung zum mittleren feuerwehrtechnischen Abschluss für hauptamtliche Feuerwehrkräfte, und eine fünfjährige Berufserfahrung notwendig.

Werksfeuerwehr-Kommandeur - Ausbildungskriterium

Personen mit abgeschlossenem Hochschul- oder Fachhochschulstudium in der Fachrichtung Brandschutz und Katastrophenschutz mit fünfjähriger Berufserfahrung.

Werksfeuerwehrausrüstungen - Grundanforderung

Ausbildung sowie Fahrzeug- und gerätetechnische Ausstattung und Ausrüstung müssen grundsätzlich unter Berücksichtigung der betrieblichen Gegebenheiten und der behördlichen Auflagen den geltenden Brandschutzvorschriften und Normen entsprechen.

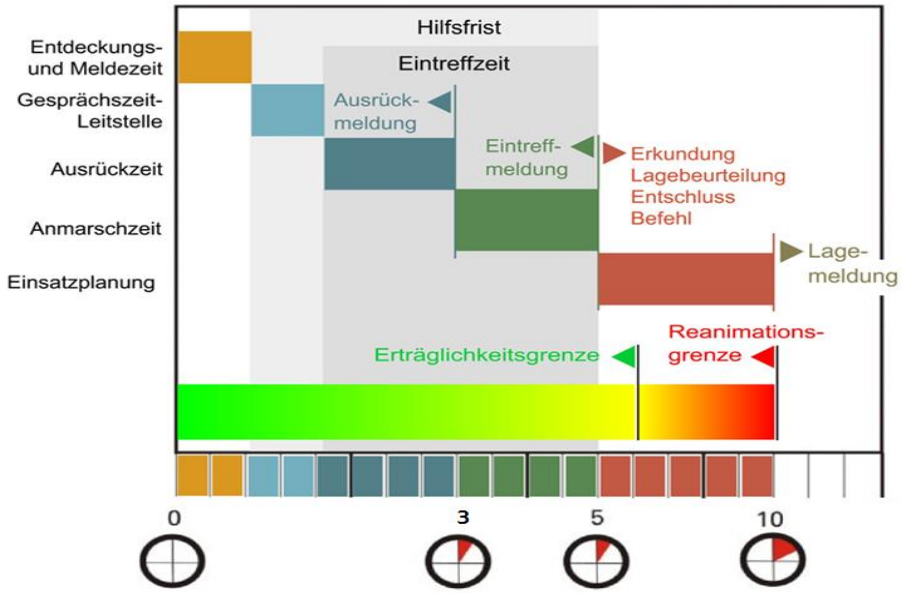
Gesundheitsanforderungen für die Werksfeuerwehr

Laut den ungarischen Brandschutzrichtlinien[4] sind die Gesundheits- und physikalischen Anforderungen der Werksfeuerwehr die gleichen, wie bei der Berufsfeuerwehr. Diese Anforderungen sind bei einem Löschangriff in der Halle von großer Bedeutung. Bei dem Auswahlprozess der Werksfeuerwehrmänner müssen nicht nur die Berufserfahrungen, sondern auch ihr Gesundheitszustand als Auswahlkriterium beachtet werden.

Feuerwehrbedarfsplan

Der Plan beinhaltet eine Aufstellung über das Unternehmensgebiet mit Rücksicht auf bauliche Eigenschaften und besondere Gefahrenmerkmale. In Verbindung mit den bekannten Hilfsfristen können die Örtlichkeit der Feuerwehrkaserne, Typ und Anzahl der Feuerwehrfahrzeuge, Personalien und die notwendigen feuerwehrtechnischen Ausrüstungen bestimmt werden. Zur Ausrüstung zählen die persönlichen Schutzausrüstungen eines jeden Feuerwehrmannes, die Spezialschutzkleidung für Gefahrguteinsätze, die zur Rettungsleistung dienenden Werkszeuge und technische Geräte sowie alle zur Brandbekämpfung notwendigen Hilfsmittel.

[4] § 5 der Verordnung Nummer 118/1996 /VII.26/ des Innenministeriums über die Anforderungen an die Werksfeuerwehr



2. quelle. Brandschutz und Sicherungstechnik, VdS-Publikationen auf CD VdS 2573: 2011–10, Durchgearbeitet: Hr. Pataki

Organisatorische Maßnahmen

Abhängig vom Personenstand der Werksfeuerwehr und den lokalen Besonderheiten können Gruppen, und aus den Gruppen Einheiten organisiert werden, die der Betreiber der Werksfeuerwehr in schriftlicher Form regeln muss. Die Gruppe besteht aus 4-6 Personen, die Einheit besteht aus 2 Gruppen. Die Gruppen der hauptberuflichen Werksfeuerwehr sind bei der Festlegung der Alarmstufe zu berücksichtigen.

Die Aufgaben

Der Brandschutz umfasst alle Maßnahmen zur Verhinderung eines Brandausbruchs bzw. einer Brandausbreitung sowie die Sicherung der Angriffs- und Rettungswege.

Der vorbeugende Brandschutz schafft darüber hinaus die Voraussetzungen für einen wirkungsvollen abwehrenden Brandschutz:

- die Geltendmachung der Bestimmungen in den Rechtsvorschriften über Brandschutz und den verbindlich anzuwendenden Normen, behördliche Vorschriften beachten und diese unterstützen, insbesondere die grundlegenden Bedingungen des Feuerlöschens und die sichernden Regelungen,
- gemäß den Bestimmungen der gesonderten Rechtsnorm auf dem Einzugsgebiet der Werksfeuerwehr die Ausübung der Aufgaben der Brandbekämpfung und der Technischen Hilfeleistung, sowie Durchführung der im Plan über Brandbekämpfung und Technische Hilfeleistung zugeordneten Aufgaben;
- bei der Vorbereitung und Schulung der Arbeitnehmer hinsichtlich des Brandschutzes,
- auf Grund der genehmigten Kooperationsvereinbarung auf Anweisung des Dienstes des Berufskatastrophenschutzorgans zu den außerhalb des Einzugsgebietes der Werksfeuerwehr entstandenen Ereignissen ausrücken, wo sie die vom Leiter der Brandbekämpfung festgelegten Aufgaben erledigen,
- Regelung des Rauchverbotes,
- Kontrolle der feuergefährlichen Tätigkeiten,
- Kontrolle der Handhabung brennbarer Abfälle. [6]

Lagezentrum und Analysezentrum [7]

Bei dem Unternehmen ist ein Lage- und Analysezentrum (im Weiteren: Lagezentrum) im Einsatz, das rund um die Uhr mit zwei Mitarbeitern von der Werkssicherheit besetzt ist. Bei einem Brandalarm oder in einem Notfall funktioniert das Lagezentrum durch EDR Rundfunksysteme als eine Steuer- und Informationszentrale. Mit diesem Lagezentrum besitzt das Unternehmen ein zentrales Organisationselement für die Werkssicherheit und den Brandschutz.

Zu den Aufgaben der Leitstelle gehören:

- Zentrale Bearbeitung von Notrufen,
- Zentrale Vergabe von Einsätzen,
- Führung von Sofortlagen, Koordination der Einsatzmaßnahmen und Durchführung erforderlicher Alarmierungen für Rufbereitschaftsdienste,
- Kontrolle von Einsätzen, Benachrichtigung weiterer Stellen bei Brand- und Notfällen bzw. bei Betriebsabbruch,
- Bearbeitung aktueller Datenabfragung,
- Führung von Lagebild, Einsatztagebuch und Einsatzbelastungsstatistik,
- Gewährleistung einer 24-stündigen Erreichbarkeit,
- Wahrnehmung von Aufgaben des FLD / Lagezentrums in Abwesenheit.

Schnelle Hilfe ist garantiert, da die Einsätze im Unternehmen von speziell dafür geschulten Kräften mit modernster Kommunikationstechnik und Unterstützung des Einsatzleitsystems MARATHON TERRA[5] (deNIS[6]) bearbeitet werden. So werden die Einsätze direkt an die Werksfeuerwehr-Einsatzkräfte[7] weitergegeben, während parallel weitere Unterstützungskräfte, Spezialeinheiten der Polizei oder beispielsweise auch Berufsfeuerwehr, Notarzt und Rettungsdienst informiert werden können.

ZUSAMMENFASSUNG, EMPFEHLUNGEN

Die Werksfeuerwehr ist eine behördlich anerkannte Berufsfeuerwehr zum Schutz von besonders brand- und/oder explosionsgefährlicher oder sonstiger Betriebe / Anlagen / Einrichtungen. Aufbau, Ausbildung und Ausrüstung sind den Erfordernissen der zu schützenden Unternehmen und den an die staatlichen Feuerwehren gestellten Anforderungen entsprechend.

Der Aufbau der Werksfeuerwehr ist in den jeweiligen Brandschutz- und Feuerwehrgesetzen von Ungarn und zum Teil in den darauf aufbauenden Werksfeuerwehrverordnungen geregelt.

Ein Großunternehmen ist nicht verpflichtet, eine Werksfeuerwehr aufzustellen. Der Aufbau einer eigenen Werksfeuerwehr wird empfohlen. Feuerwehrpersonal und -einrichtungen sowie ihre Ausrüstungen sollten den jeweiligen Unternehmensrisiken angepasst werden.

Literaturverzeichnis

[1] Kuti Rajmund: Vízköddel oltó berendezések speciális felhasználási lehetőségei és hatékonyságuk vizsgálata a tűzoltás és kárfelszámolás területén, Doktori (PhD) értekezés, 2009. ZMNE.

[5] Kommunikationssystem in Ungarn, zwischen Sicherheitsbehörden
[6] Kommunikationssystem in Deutschland, zwischen Sicherheitsbehörden
[7] Task Force

[2] Regierungsverordnung Nummer 239/2011. (XI. 18.) über die Regelungen hinsichtlich der kommunalen Feuerwehren und Werksfeuerwehren, sowie der Beiträge zum Erhalt der Berufsfeuerwehr, der kommunalen Feuerwehr und des freiwilligen Feuerwehrvereins.

[3] Brandschutz und Sicherungstechnik, VdS-Publikationen auf CD, VdS 2573: 2011 – 10.

[4] Dr. Kuti Rajmund: Komplex műszaki mentések tervezésének lehetőségei, 2010 www.vedelem.hu (Letöltve: 2013.12.02.)

[5] 10/2008. (X. 30.) ÖM rendelet a hivatásos katasztrófavédelmi szerveknél, a tűzoltóságoknál, valamint az ez irányú szakágazatban foglalkoztatottak szakmai képesítési követelményeiről és szakmai képzéseiről.

[6] Prof. Dr. Padányi József: Éghajlatváltozás és a biztonság összefüggései. HADTUDOMÁNY 1-2: pp. 33-46. (2009)

[7] Dr. Péter Sulányi – János Pataki – Attila Pongrácz : Integrierte Brandschutzeinrichtungen, Ausgabe VIII / 4 – Dezember 2013. http://hadmernok.hu/134_13_patakij.php http://hadmernok.hu/134_13_patakij.php

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Hornyacsek Júlia - Kiss Béla
hornyacsek.julia@uni-nke.hu - kiss.bela1979@freemail.hu

KATONAI ÉS CIVIL LÉGIJÁRMŰVEK ALKALMAZHATÓSÁGA A KÁRTERÜLET FELDERÍTÉSE ÉS A KÁRELHÁRÍTÁS SORÁN

Absztrakt

Napjaink biztonsági kihívásai felhívják a figyelmet arra, hogy nem csak a katasztrófák, hanem a terrorcselekmények vagy a katonai művelek során kialakult kárterületek is rendkívül összetettek, a felszámolásuk széleskörű összefogást igényel. Felmerül a kérdés, hogy a védekezésben résztvevő szervezetek képesek-e összehangoltan együttműködni ezekben az esetekben, továbbá, hogy a hagyományos felszerelések, eszközök mellett, melyek azok az új technikák, amelyek jelentősen növelhetik a lakosság és az anyagi javak mentésének, védelmének hatékonyságát. E cikkben a szerzők az új technikák és eszközök közül bemutatják azokat a légi járműveket, amelyeket sokrétűen alkalmazhatóak a kárterületen felmerülő felderítési-, kárelhárítási- és kárfelszámolási feladatok ellátása során.

The security challenges of today point to the fact that not only disasters, but terrorist acts or damage zones formed during military operations, can be extremely complex, the eradication requiring broad collaboration. The question arises whether the organisations participating in the protection are capable of coordinated co-operation in these cases, and that in addition to the traditional equipment, what are the new techniques that can significantly increase the effectiveness of saving, protecting the population and the property. From among the new techniques and tools, the authors describe those aircraft, that can be used in the detection and remediation of damage zones, in a versatile manner.

Kulcsszavak: *kárelhárítás, kárfelszámolás, helikopter, repülőgép, pilóta nélküli repülőgép, kárfelderítés, mentés ~ remediation, damage eradication, helicopter, aircraft, unmanned aerial vehicle, damage detection, rescue*

BEVEZETŐ

A Katasztrófák Előfordulását Kutató Központ (CRED) adatai szerint 1992-ben 221 jelntősebb természeti katasztrófát regisztráltak, melyek 14811 emberéletet követeltek, 78 millió személy életét befolyásolták és kb. 70 milliárd USD kárt okoztak. 2011-ben már 336 regisztrált katasztrófa 31105 halálos áldozattal járt, 209 millió ember életére volt hatással, és rekordösszegű, 366 milliárd USD anyagi vesztességet okozott.[1] A CRED természeti katasztrófának tekint minden olyan természeti eredetű esetet, amelynek során minimum 10 ember meghal, legalább 100 ember érintett, vagy amely szükségállapot kihirdetését, nemzetközi segítség igénybevételét teszi szükségessé.[2]

A számadatok szerint nem csak a katasztrófák, de a körülöttünk lévő egyéb veszélyek száma is nő, hatásuk egyre sokrétűbb, és az általuk okozott károk nagysága is emelkedik, legyen szó ezen túlmenően fegyveres összecsapásról vagy akár tömegpusztító fegyver által okozott pusztításról. A katasztrófák és egyéb tényezők következtében kialakult kárterületen számos olyan feladat adódik, amelyek végrehajtásához eszközökre, járművekre, gépekre, anyagokra és erőkre van szükség. A technikai fejlődés napjainkra már lehetővé tette, hogy a felderítést, a mentést, a kárelhárítást és a helyreállítást célzó feladatok végzéséhez légi járműveket is alkalmazzanak.

A légi járművek azokat a repülőeszközök, melyek aerodinamikai (merev és forgószárnyas repülőgépek, rakéták) vagy aerostatikus elven (léggömbök, léghajók) létrehozott felhajtó erő segítségével képesek a levegőbe emelkedni. Többnyire külön meghajtás és megfelelő kormányszervek biztosítják a levegőben történő haladást és a kívánt térbeli helyzetváltoztatást.

Ezeket a katasztrófavédelem döntően a primer mentésben alkalmazza, illetve szekunder feladatokat is elláthat.[3] Olyan területeken, ahol a terepviszonyok nem teszik lehetővé a közúton közlekedő mentők gyors helyszínre érkezését, illetve ahol a mentőlefedettség miatt ez szükséges, már a hetvenes évektől kiépült a légi mentő hálózat. Németországban például 1970 és 1998 között a mentőhelikoptereket 852 513 alkalommal vetették be, azaz évente átlagosan 47 000-szer.[4]

Felmerülő kérdések, hogy:

- a kárelhárítás- és kárfelszámolás mely területén és milyen formában alkalmazhatóak ezek az eszközöket napjainkban Magyarországon?
- mely szervezetek erői, képességei alkalmasak arra, hogy a katasztrófák felszámolásában részt vegyenek?
- a Magyar Honvédség légi járművei milyen rendszerben és módon kerüljenek alkalmazásra a kárterületeken?

Ebben a cikkben bemutatjuk a kárelhárítás- kárfelszámolás rendszerét, és az ott alkalmazható légi járművek képességeit, valamint a hatékony alkalmazás feltételeit.

KÁRELHÁRÍTÁS KÁRFELSZÁMOLÁS HELYE A KATASZTRÓFAVÉDELEMBEN

Magyarország katasztrófavédelmét a 2011. évi CXXVIII. törvény szabályozza, amely alapján az egységes katasztrófavédelmi rendszer három, - *szervezeti, erőforrás* és a *katasztrófa-elhárítási feladatok – alrendszerre* bontható.

A szervezeti alrendszerbe tartoznak a hivatásos katasztrófavédelmi szervek mellett mindazon szervek és szervezetek is, amelyek jogszabályi előírás alapján részt vesznek a katasztrófavédelemi feladatok ellátásában. (önkormányzatok, polgári védelmi, civil humanitárius szervek stb.).[5]

Az erőforrás alrendszer a fent említett szervezetek logisztikai, pénzügyi erőforrásainak biztosítását foglalja magába.

A katasztrófa-elhárítási feladatok alrendszere az 1. ábrán látható módon, a megelőzési, mentési és kárfelszámolási időszakok egymással szorosan összefüggő és el nem különíthető feladatait öleli fel.

1. ábra. A kárelhárítási és kárfelszámolási feladatok mentési időszakok szerinti kapcsolata[1]

A kárelhárítást- és kárfelszámolást alapvetően a mentési- és helyreállítási időszak feladatai közzé soroljuk, azzal a megkötéssel, hogy az előbbit elsősorban a mentési időszakban, míg a kárfelszámolást a helyreállításkor hajtják végre. Ezek mentési időszakok szerinti kapcsolata is tanulmányozható az 1. ábrán. E tevékenység meghatározásához célszerű figyelembe venni azt az összetett és komplex feladatrendszert, amely átfogja és lefedi a mentési- és helyreállítási időszak valamennyi katasztrófavédelmi tevékenységét. A kárelhárítási és kárfelszámolási feladatok értelmezése igen fontos, melyeket a szakirodalom többféleképpen is definiál. Ezek közül mi a cikkünkben az alábbi értelmezését tekintjük mérvadónak:

„A kárfelszámolási feladatok célja: a mentéshez szükséges azonnali, az ideiglenes és a teljes helyreállítási munkák végrehajtása, az alapvető életfeltételek biztosítása, továbbá a katasztrófák következményeinek részleges vagy teljes felszámolása, a kritikus esemény bekövetkezése előtti állapot teljes vagy részleges visszaállítása, továbbá a tapasztalatok összegzése."[6] A fogalomból kitűnik, hogy a végzendő feladatok szerteágazóak, és végrehajtásuk megfelelő technikai eszközöket feltételez. A kárfelszámolás rendszerint a kárelhárítás utolsó szakaszában vagy azt követően kezdődik.

„Kárelhárítási feladatoknak nevezzük mindazon, tervezési, szervezési, végrehajtási tevékenységek, rendszabályok összességét, amelyek a katasztrófák elleni védekezés „mentési" időszakában végrehajtott azonnali beavatkozások és operatív intézkedések segítségével, lehetővé teszik a kritikus események vagy káros hatásaik továbbterjedésének, a súlyos környezeti károk kialakulásának megakadályozását, a következmények mérséklését, kiküszöbölését, valamint az azonnali élet- és vagyonmentés végrehajtását."[6]

A kárelhárítási- és kárfelszámolási feladatok végrehatásához elengedhetetlen és nélkülözhetetlen a megfelelő logisztikai és technikai eszköz-támogatás, és a munkák minden oldalú biztosítása. A 2. ábrán ilyen, a 2010. október 4-én bekövetkezett vörösiszap-katasztrófa idején, a víz pH értékének a csökkentése irányuló kárelhárítási munkálat látható.

[1] Dr. Szabó Sándor, Dr. Tóth Rudolf: A kárelhárítási és kárfelszámolási feladatok értelmezése a katasztrófavédelem területén. VIth International Symposium on Defence Technology, 6-7 May 2010, Budapest, Hungary, Konferencia kiadvány, 8. oldal 3. sz. ábra ISSN 1416-1443

2. ábra. Kárelhárítási munkák a vörösiszap-katasztrófa után (Torna-patak, Marcal). 2010. október[2]

Kiemelt fontosságú, hogy az adott esemény következményeinek felszámolására kárterület-jellemzőinek megfelelő eszközöket alkalmazzanak. Ehhez, - tapasztalatok szerint a hagyományosak mellett - napjainkban egyre inkább igénybe veszik a moderneket, köztük a légi járműveket is, melyek széles spektrumban képesek segítséget nyújtani a kárelhárítás és kárfelszámolás során. Jellegükből adódóan azonban nem mindenkor és minden feladatra alkalmazhatóak, illetve bevetve sem mindig az elvárhatóan költség-hatékonyak. Ezért felhasználásuk akkor indokolt, ha hagyományos eszközökkel nem, vagy nem megfelelő hatékonysággal hajthatóak végre a szükséges feladatok.

LÉGIJÁRMŰVEK ALKALMAZHATÓSÁGÁNAK LEHETŐSÉGEI ÉS KORLÁTAI A KÁRELHÁRÍTÁS IDŐSZAKÁBAN

A kárelhárítás- és kárfelszámolás időszakában számos katasztrófavédelmi feladatban alkalmazhatóak légijárművek. Polgári és katonai repülőgépek, helikopterek, állandó készenléti szolgálatai teszik lehetővé az azonnali, szakszerű és gyors beavatkozást a katasztrófa- helyzet kialakulását követően. A civil légimentő szolgálatot az Országos Mentő Szolgálat irányítása mellett, a Magyar Légimentő Nonprofit Kft működteti, amelyet az Országos Mentő Szolgálat alapította 2006-ban. A Magyar Honvédség Katasztrófavédelmi Rendszerén belül pedig működtetik és alkalmazzák a Légi Csoportot, a Légi Sugárfelderítő Csoportot (LSFCS) és a Téli Veszélyhelyzetet Felszámoló és Mentő Csoportot, melyek szerves részét képezik az Országos Honvédségi Katasztrófavédelmi Rendszernek.

Ezeken a szervezeteken és szolgálatokon kívül a Magyar Honvédség további két 24 órás szolgálattal járul hozzá a katasztrófavédelmi feladatok ellátásához (Légi Kutató Mentő Készenléti Szolgálat, Légi Sugárfelderítő Szolgálat), melyek alkalmazhatósága ugyan bizonyos mértékig korlátozott, de ez nem csökkenti a jelentőségüket. Felmerül a kérdés, hogy mi szól a légi járművek alkalmazása mellett, és mi korlátozza azok használatát.

Az elmúlt időszak ilyen célú repüléseit elemezve megállapítható, hogy a repülőeszközök bevetésének elsődleges korlátozó tényezője a rossz időjárás, döntően a látási viszonyok erőteljes csökkenése miatt. Minden légijárműnek van egy úgynevezett időjárási minimuma, melynek jellemző - rendszerint látási távolságra vonatkozó korlátozási - értékei alatt a repülés nem hajtható végre. Kivétel ez alól a Légi Kutató Mentő Készenléti Szolgálat, ahol a hajózó gépparancsnok az időjárási viszonyok ellenére is - emberi élet megmentése érdekében - dönthet a feladat végrehajtása mellett. A másik jelentős korlátozó tényező a repülőgép hatósugara, amely az a távolság, amelyet előírt, normál üzemanyag-feltöltéssel képes megtenni céljáig, majd feladatát végrehajtva (erre további 10÷20 perc repülési idő áll rendelkezésre!) kiinduló

[2] Vízügy honlap – kárelhárítási munkák a vörös iszap katasztrófa után (Torna-patak, Marcal). 2010. október URL: http://www.vizugy.hu/gallery.php?keptarid=20#5 Letöltés: 2013. május 03.

bázisára visszatérni. A hatósugár és ezzel a végrehajtható feladat időtartama pót üzemanyagtartályok alkalmazásával növelhető. Nehézségként jelentkezik, hogy ezeknek a járműveknek magas az üzemköltségessége, illetve egyes alkalmazásukkor előfordulhat, hogy a személyzetnek nem csak a szakfeladatait, hanem az eseménnyel kapcsolatos egyéb tevékenységet is el kell látnia, amelyre speciális felkészítés nélkül nem képes. A légi járművek között speciális csoport a katonaiaké, melyek alkalmazását külön előírások is korlátozzák. A hatékony működtetés akadálya lehet az is, ha adott esetben a kárterület felderítésére-alapú döntések megkésnek és ezért a bevetés elrendelése is késik.

KATONAI LÉGIJÁRMŰVEK ALKALMAZÁSA

A Honvédelmi Miniszter által jóváhagyott Ágazati Katasztrófavédelmi Terv tartalmazza a honvédelmi szervezetekre vonatkozóan az ágazaton belüli-, illetve azon kívüli katasztrófavédelmi tevékenységgel összefüggő feladatokat és alkalmazható eszközöket, benne a légijárművekre is érvényesek a katonai rendszabályokat. Vizsgáljuk meg, melyek ezek az eszközök!

A Magyar Honvédségnél rendszeresített AN-26-os két hajtóműves, légcsavaros gázturbinás szállító repülőgép, valamint a 3. ábrán látható JAS 39 Gripen, negyedik generációs, könnyű vadászrepülőgép jól alkalmazható katasztrófavédelmi feladatok ellátására. Az AN-26-tal elsősorban személyek és különböző felszerelések, élelmiszer, védekezéshez szükséges anyagok utánpótlása szállítható, míg a JAS 39 Gripen légi felderítésre (a kárterületről légi felvételek készítésére) használható.

A Magyar Honvédségben rendszeresített forgószárnyas légijárművek közül a Mi-8/17 közepes szállítóhelikopterek, illetve a Mi-24-es harci helikopterek alkalmasak katasztrófa-védelmi feladatok ellátására. Ilyen felhasználás a szervezeten belül létrehozott Honvédelmi Katasztrófavédelmi Rendszer (továbbiakban: HKR) kereteiben történik, amely része az országos katasztrófavédelmi rendszernek. A HKR feladata egyrészt a honvédelmi ágazaton belüli katasztrófahelyzet, súlyos szerencsétlenség (baleset) megelőzése és a veszélyeztetett személyi állomány, vagyontárgyak megóvása, mentése, másrészt az MH erőinek, eszközeinek bevonását igénylő, ágazaton kívüli, valamint a nemzetközi hasonló, károsító hatások elleni védekezéshez és a segítségnyújtáshoz való hozzájárulás.

„A HKR alapvetően három feladatra (nukleáris-baleset és vízkár következményeinek elhárítására, extrém téli időjárás okozta helyzetben segítségnyújtásra) lett létrehozva, de flexibilis képességei természetesen felhasználhatóak bármely más esetben is.”[7]

3. ábra. Magyar JAS 39C EBS HU leszállás[3]

A HKR végrehajtó erői közzé tartozik *a Légi Csoport* (LCS) is, amelyet az MH 86. Szolnok Helikopter Bázis állományából jelöltek ki. Az LCS-t külön parancsra aktivizálják, a feladatát (pl. felderítés, betegek, rászorultak halaszthatatlanul szükséges gyógyintézetbe való szállítása, elzárt körzetek élelmiszerrel, gyógyszerrel történő ellátása, személyek mentése az elzárt

[3] JAS 39 Gripen URL: http://gripen.uw.hu/ készítette: nincs megnevezve, Letöltés: 2013. május 03.

életveszélyes területekről, levegőből történő gátmegerősítés, tűzoltásban való részvétel, stb.) ezt követően folyamatosan készenléti szolgálatban látja el.

Összetétele ennek megfelelően alakult ki:

- 2 db MI-8T (MI-17) helikopter,
- hajózó- és kiszolgáló állomány (2 fő első pilóta, 2 fő másodpilóta, 4 fő fedélzeti technikus, 1 fő visszaellenőrző tiszt, 2 fő SH mechanikus, 1 fő EMO mechanikus, 1 fő RTB mechanikus, 1 fő fegyver mechanikus).

Képességei alkalmassá teszik a katasztrófák következményei felszámolásában való hatékony közreműködésre, hiszen 24 fő, vagy 4t teher szállítására képes.

A Magyar Honvédség jelenleg két 24 órás készenléti szolgálatot tart fent. Ezen belül tevékenykedik a Légi Kutató Mentő Készenléti Szolgálatot (LKMSZ), melynek jogi alapjait az 1944. december 7-én, Chicagóban aláírt nemzetközi egyezmény adja. Ennek értelmében az egyezményhez csatlakozó országoknak segítséget kell nyújtaniuk az adott ország légterében bajba jutott légi járműveknek, egyben hozzá kell járulniuk, hogy a légi járművet lajstromozó ország csatlakozzon a kutatási, mentési feladatok ellátásához.

Magyarországon, az ilyen kutató-mentő feladat tekintetében példaként szolgál a 2006-ban Hejcén, pilótahiba miatt lezuhant szlovák katonai repülőgéppel (4. ábra) kapcsolatos kereső-munkálat, ahol az utasok felkutatásában és mentésében - a magyar állam hozzájárulásával - a szlovák fél is részt vehetett

„A nemzetközi trendet vizsgálva látható, hogy a fejlett országokban megkülönböztetett figyelmet fordítanak a kutatás és mentésre. Gyakorlatilag számos országban (Németország, Hollandia, Nagy-Britannia), ez a szervezet - annak ellenére, hogy katonai irányítás alatt működik - polgári személyek mentésében is részt vállal, sőt feladatai közé tartozik a mi fogalmaink szerinti légi baleseti mentés is. Németországban a katonai kutató-mentő szervezet egyes körzeteiben vegyes személyzetek, (katonák és polgáriak együtt) tevékenykednek.”[8]

4. ábra. Szlovák katonai repülőgép katasztrófa után Hejcén.[4]

Magyarország is mindent megtesz az ilyen esetekre való felkészülésért. A bajba jutott légi járművek megsegítéséről, valamint a katasztrófák elleni védekezéssel és a mentéssel összefüggő tevékenységet ellátó légi kutató-mentő szolgálat (OLKMSZ) szervezetéről, működésének, fenntartásának, riasztásának és a mentéssel járó költségek viselésének rendjéről, az e tevékenységek engedélyezésére vonatkozó szabályokról hazánkban a 267/2011. (XII. 13.) Kormányrendelet rendelkezik. Ennek értelmében a légi kutatás: a szükséges speciális berendezésekkel felszerelt, a feladatra felkészített személlyel rendelkező légijármű repülése, amelyet annak érdekében hajt végre, hogy az eltűnt légijárművet, illetve annak utasait felkutassa.[5]

[4] Nagy Sándor pv. ezredes: Szlovák katonai repülőgép balesete Hejcén. 2006. március 15. URL: http://www.vedelem.hu/letoltes/tanulmany/tan70.pdf Letöltés: 2013. május 20.

[5] értelmező rendelkezések 7.

Az OLKMSZ jelenleg két helyen települő szolgálattal, - Keleten az MH 86. Szolnok Helikopter Bázison, Nyugaton, Pápa Bázisrepülőtéren - látja el, az egész ország területére kiterjedő, 24 órás készenléti szolgálatát, amelyek hatáskörzetét a Duna folyó választja el.

Vizsgáljuk meg, hogy milyen feladatok tartoznak a légi kutatás-mentés fogalomkörébe, és milyen képességekkel kell rendelkezniük ezeknek a gépeknek!

„Az OLKMR az alábbi légi kutatás-mentéssel összefüggő feladatokat látja el:

a) Magyarország területén és légterében bajba jutott légi jármű személyzetének, utasainak felkutatása és mentése;
b) Magyarország területén bekövetkezett légiközlekedési balesetek következményeinek felderítése, és közreműködés a következmények felszámolásában;
c) a szomszédos országok területén és légterében nemzetközi szerződés vagy felkérés alapján történő légi kutatás-mentés.” [9][6]

Alkalmazhatóak tehát külföldön és belföldön egyaránt, és nemcsak kutatásra, hanem a következmények felszámolására is.

Az OLKMR légijárművei az alábbi katasztrófavédelmi feladatok ellátásában vehetők igénybe:

a) az eltűnt személyek légi úton történő felkutatása;
b) katasztrófa által érintett személyek és tárgyak légi úton történő kimenekítése.

A szolgálatoknak képesnek kell lenniük a riasztást követően nappal jó látási viszonyok között és $+5C^0$ felett, a riasztást követő 30 percen belül a kutató-mentő feladat megkezdésére. Ugyanez a normaidő éjszaka, rossz látási viszonyok között és $+5C^0$ alatt 60 percre tolódik ki. A szakszolgálati személyzet elsődleges feladata a bajba jutott légi jármű keresése, felkutatása, ezt követően az esetleges sérültek elsősegélyben részesítése és életben tartása a magasabb szintű orvosi beavatkozás megkezdéséig. A feladatok ellátásához a 6 fős személyzetnek (2 fő hajózó, 2 fő ejtőernyős, 1 fő felcser, 1 fő műszaki) minden olyan eszköz a rendelkezésére áll, ami egy vonulós tűzoltó és mentőautóban megtalálható (hidraulikus erővágók, csörlők, csigák, defibrillátor, KED mellény, stb.).

A felszerelések a feladat ellátására készenlétben tartott Mi-8-as szállítóhelikopter fedélzetére előre bemálházott állapotban vannak (5. ábra), ezzel is megrövidítve a riasztástól a felszállásig eltelt időintervallumot. A fenti képességekkel a veszélyhelyzeti figyelés, kárterület-felderítés. a kutató-mentő feladatok összehangolása, a kezdeti orvosi segítségnyújtás is megoldható.

5. ábra. Új rendszerben működik a kutató-mentő szolgálat.[7]

[6] 6. § (1)

[7] Új rendszerben működik a kutató-mentő szolgálat, Készítette: Dévényi Veronika URL**:** http://www.honvedelem.hu/cikk/35433 Letöltés: 2013. május 20.

A LÉGI JÁRMŰVEK SZEREPE ÉS KÉPESSÉGEI A NUKLEÁRIS KATASZTRÓFÁK, ÁRVIZEK, TÜZEK SORÁN

A kutató-mentő légijárművek, a bajbajutott repülőgépek balesetét követő kutatásán kívül, légi sugárfelderítésre is eredményesen alkalmazhatóak.

Napjaink egyik legnagyobb veszélyeztetettsége a *nukleáris katasztrófák bekövetkezése.* Elsődleges veszélyforrást a világon működő 156 atomerőmű és azok meghibásodása jelenti (Európában közel 150 atomreaktor). Az eddigi legsúlyosabb katasztrófa az 1986. április 26-ai csernobili atomerőműben történt robbanás, illetve a 2011. március 11-ei földrengés következményeként, a fukushimai atomerőmű balesete (6. ábra). Jelentős potenciális veszélyforrást jelenthetnek továbbá, – mindenek előtt a volt Szovjetunió felbomlásakor - eltűnt, ellopott és eladott sugárzó anyagok, nukleáris fegyverek, amelyek avatatlan kezekbe kerülve akár nukleáris katasztrófát is előidézhetnek, illetve nem zárható ki a szándékos alkalmazásuk sem. Ilyen esetek kapcsán a kárelhárítás feladatai közé sorolhatjuk a nukleáris katasztrófák bekövetkezését követő időszakban végrehajtott védekezési munkálatokat, melynek lényeges elem a kárterület felderítése.

„A légi sugárfelderítés, amely a 80-as években már vegyivédelmi harcászati eljárásként került alkalmazásra, a leggyorsabb módszer, azzal az előnnyel, hogy a kezelő állomány kisebb mértékű dózisterhelést szenved el, mint az egyéb felderítési módozatoknál."[10]

6. ábra. Nukleáris katasztrófa Japánban. Forrás:[8]

A Légi Sugárfelderítő Szolgálat elsődleges rendeltetése napjainkban egy esetlegesen ipari, vagy hadi körülmények között bekövetkezett nukleáris katasztrófát követően a szennyezett terepszakasz detektálása, felmérése, adatok továbbítása a szakemberek felé. Ezen kívül a szolgálat képes pontszerű sugárforrás keresésére, felkutatására. Hazánkban a Légi Sugárfelderítő Szolgálat az MH. 86 Szolnok Helikopter Bázison működik, 24 órás készenléti szolgálat keretein belül. A feladat egy sugármérő konténerrel felszerelt Mi-24-es harci helikopterrel hajtható végre. Napjainkra a pilóta nélküli repülőgépeket is alkalmaznak sugárfelderítésre. Ez történt a fukushimai baleset követően, ahol a Tokyo Electric Power egy T-Hawk típusú robot repülőgépet küldött a szennyezett terület fölé (7. számú ábra).

8 Nukleáris katasztrófa fenyeget Japánban, Készítette: nincs megnevezve, URL: http://vilagszam.hu/cikkek/nuklearis-katasztrofa-fenyeget-japanban-megismetlodhet-a-csernobili-eset.html/1516 Letöltés: 2013. május 20.

7. ábra. Inside the Drone Missions to Fukushima Forrás:[9]

A nukleáris eredetű veszélyeztetés ugyan nem zárható ki, de szerencsére a ritka jelenségek közé tartozik. Az egyéb katasztrófák azonban gyakran előfordulnak, pl. hazánkban az *árvíz és a belvíz* 2-3 évenként visszatérő probléma. Ezeknél is jól alkalmazhatóak a légijárművek, döntően az alábbi 3 fő területen:

- személyi szállítás, életmentés;
- a szükséges anyagok utánpótlása;
- külső függesztmények szállítása.

A személyszállítási és életmentési elsősorban a víz által körülzárt településekről történik, míg a szükséges anyagok szállítását a védekezés helyszínére és az ott dolgozók munkájának segítését gyakran távolabbról hajtják végre. Ehhez speciális eszközök is szükségesek.

Külső függesztményként a 8. ábrán látható, külön erre a célra készített 1 tonna teherbírású kemény falú zsákokat alkalmazzák, amelyet földel, homokkal vagy sóderrel tölthető meg. Feladatuk, a megindult gátszakaszon átfolyó víz útjának elzárása.

A kárelhárítási feladatokhoz sorolhatóak *a tűzoltás* is, melynek egyik legegyszerűbb és leghatékonyabb módja a felülről történő, pl. helikopter alkalmazásával. Ilyenkor, a speciális, külső függesztményként szállított víztartályból a mechanikus kioldást követően a nagy-mennyiségű, kiáramló víz szétporlad, lehűtve a levegőt csökkentve az égéshez szükséges hőmérsékletet. Napjainkban ehhez többnyire a gumifalú, összecsukható kanadai gyártmányú Bambi Bucket víztartályt használnak, mely feltölthető mesterséges víztározókból, tavakból, folyókból, de tűzoltófecskendővel is. A feladat-végrehajtás sikerességét több tényező is befolyásolja, mint például a repülési magasság, sebesség, a szélerősség és a kibocsájtás körülményei.

Ezeknek az eszközöknek az alkalmazása során a hatékonyság több tényezőtől is függ. Egyet kell értenünk azzal az állítással, miszerint: „Az egyik legfontosabb az együttműködés kérdése, hiszen a katasztrófahelyzetek bonyolultsága, a védekezésben résztvevő szervek esetenkénti nagy száma feltételezi a jó együttműködést mind a vezetés, mind a végrehajtás szintjein. Míg a megelőzés időszakában a tervezés és részben a szervezés területei igénylik elsősorban az együttműködés elmélyítését, addig a következmények felszámolása alatt a kárterületen végzett munka összehangolása a cél.”[11]

[9] Inside the Drone Missions to Fukushima, Készítette: nincs megnevezve,
URL: http://www.theatlantic.com/technology/archive/2011/04/inside-the-drone-missions-to-fukushima/237981/
Letöltés: 2013. május 25.

8. ábra. Helikopter dolgozik az Onga-Ócsalános közötti töltésszakaszon Forrás:[10]

CIVIL LÉGIJÁRMŰVEK ALKALMAZÁSA

Napjainkban, a médiából egyre gyakrabban halljuk és látjuk a civil légimentők bevetését közúti balesetek, káresetek súlyos sérültjenek elszállításánál. A légi mentés civil biztosításáért hazánk területén a Magyar Légimentő Nonprofit Kft. a felelős. Feladatai közzé tartoznak az olyan azonnali, sürgősségi feladatok, amelyek végrehajtási ideje 1 óránál kevesebb (pl. súlyos állapotú sérült személy magasabb szintű orvosi ellátást biztosító intézménybe történő szállítása is. A szolgálat szakmai irányítását az Országos Mentő Szolgálat (továbbiakban: OMSZ) végzi irányítócsoportján keresztül a 104 és a 112-es segélyhívó számokon beérkezett riasztások alapján végzi.

A szolgálat elsődleges célja a lakosság számára 15 percen belüli légi mentés biztosítása, melyet jelenleg a 9. számú ábrán látható hét állandó bázisról teljesít. E feladatokat a szakszolgálati személyzet Aerospatiale-Eurocopter AS350B gázturbinás hajtóműves (10. ábra) és Ecureuil dugattyús motoros helikopterekkel hajtja végre. Az AS350B a tartályaiba feltöltött 540 liter üzemanyaggal maximálisan 2 óra 40 percet repülhet úgy, hogy 60 liter navigációs tartaléka marad. Műszerezettsége kedvezőtlen időjárási körülmények között és éjszaka is lehetővé teszi a repülést.

9. ábra. Mentők a város felett[11]

[10] Helikopter dolgozik az Onga-Ócsanálos közötti töltésszakaszon, Készítette: nincs megnevezve, URL: http://www.origo.hu/itthon/percrolpercre/20100609-apadnak-az-eszakmagyarorszagi-folyok-arad-a-tisza-arvizi-helyzet.html?pIdx=1 Letöltés: 2013. május 25.

[11] Mentők a város felett, Készítette: Simon Péter, URL: http://repulnijo.hu/2008/02/14/mentok-a-varos-felett/ Letöltés: 2013. május 25.

10. ábra. Magyar Légimentő Nonprofit Kft. Bázisai. Forrás:[12]

A helikopterek modernizálásukkor két-képernyős, mozgótérképes GPS navigációs rendszert kaptak, amely segítségével az egészségügyi személyzet veheti a célkoordinátákat. A fedélzeti orvosi műszerezettség megegyezik a „vonulós" mentőautókéval (pl. intubáláshoz, sebellátáshoz szükséges eszközök, kapcsok, mellkas-diagnosztizáláshoz és centrális vénabiztosításhoz szükséges felszerelések, KED mellény és oxigénpalackok, alapvető gyógyszerek, infúziók, fájdalomcsillapítók, stb).

A légimentő-szolgálat személyi állománya évente általában 1400-1800 órát tölt a levegőben, amely komoly teljesítményt jelent, és megfelelő gyakorlottságot eredményez.

LÉGIJÁRMŰVEK ALKALMAZHATÓSÁGA A KÁRFELSZÁMOLÁS IDŐSZAKÁBAN

Nem csak a mentés, de a kárfelszámolás időszakában is számos olyan feladat van, amelyekben kiválóan alkalmazhatóak a különböző légijárművek (merev és forgószárnyú repülőgépek, köztük a pilóta nélküliek is). Ilyenek lehetnek a romok eltakarítása, utánpótlási felszerelések szállítása, építmények újjáépítésében való segítségnyújtás (templomtorony, vasúti híd elemeinek beemelése), kárterület felmérése (tűzkár) stb. A Magyar Honvédségben rendszeresített Mi-8/17-es közepes szállítóhelikopterek harcászattechnikai adatai alapján megállapítható, hogy alkalmasak nagyobb súlyú külső függesztmények elszállítására is.

A kárfelszámolás bonyolult és időigényes része a kárfelmérés, amihez, a légi járművek alkalmazása számottevő idő- és költségmegtakarítást eredményezhet. Pl. egy többhektáros erdőtűz után a kárhelyszín felmérésére, átvizsgálására kiválóan alkalmazhatóak a nagy felbontású HD kamerával felszerelt pilóta nélküli repülőgépek is, mivel üzemköltségük töredéke minden más eljárásnak, ráadásul a korántsem veszélytelen feladatok emberi élet kockáztatása nélkül hajthatóak végre. Különösen igaz ez kiterjedt kárterületek, vagy összetett károk esetén. Bár ezek eddig hazánkban relatíve ritkán fordultak elő, de a későbbiekben nem is zárhatóak ki. Az alkalmazásuk hatékonysága nagyban függ attól, hogy a riasztás megfelelő időpontban, módon és formában történik-e, illetve hogy a kárterületen megjelenő szervezetek együttműködése megfelelő színvonalú-e.

Ennek kialakítása nem történhet csak „papíron", hanem a valóságban is gyakorolni kell. Ezért fontos a különböző mentőszervezetek számára közös gyakorlatok szervezése, és az alapképzésükbe a katasztrófavédelmi ismeretek valamint az együttműködés kérdéseinek

[12] Magyar Légimentő Nonprofit Kft. Bázisai, Készítette: nincs megnevezve,
URL: http://www.legimentok.hu/bemutatkozunk/kuldetesunk#scrollhere Letöltés: 2013. május 25.

beépítése, készségszintűvé fejlesztése. Ennek azonban a fordítottja is igaz, a katasztrófavédelmi szakembereknek is hasznos lehet a légijárművekkel rendelkező szervezetek, és azok képességeinek ismerete.

A légijárművek beszerzése, fenntartása és üzemeltetése költségigényes. A Magyar Honvédség repülőeszközeinek fejlesztésére napjainkban politikai konszenzus van. 2013. májusában az ezzel kapcsolatos négypárti egyeztetésen Dr. Hende Csaba honvédelmi miniszter leszögezte: *„meg kell teremteni a nemzeti helikopterképességet. Ez egy, a XXI. század kihívásainak megfelelő, gazdaságosan üzemeltethető, modern flotta létrehozását jelenti, amely egyaránt alkalmas az országvédelmi és szövetségi feladatok, a katasztrófavédelem, a terrorelhárítás, a légirendészet és más nemzetgazdasági feladatok kiszolgálására."* A parlamenti pártok jóváhagyták a tanácskozást megelőző hosszas előkészítő munkát, illetve a nemzeti helikopterképesség megteremtési módjának menetrendjét*."* [12]

ÖSSZEGZÉS

Napjaink civilizációs és természeti katasztrófái, valamint az egyéb okból kialakuló veszélyeztetettség megköveteli a védelmi feladatokat ellátó szervezetektől a magas szintű szakmai felkészültséget, a szervezetek közötti hatékony együttműködést, továbbá a feladatok végrehajtásához nélkülözhetetlen technikai felszerelések meglétét és készenlétben tartását. Nem csak a katasztrófák, hanem a terrorcselekmények és a fegyveres cselekmények során kialakult emberi és anyagi károk felderítéséhez és felszámolásához is szükség van a hagyományosak mellett új eszközök és technikák alkalmazására.

A kárelhárítás és kárfelszámolás területén számos olyan feladat van, amelyek végrehajtásához elengedhetetlenek a speciális szakfelszerelések, köztük a jól alkalmazható katonai és polgári légijárművek is. Ezekkel, a nagy kiterjedésű kárterület esetén – legyen az katasztrófából, terror- vagy harci cselekményből adódó – gyorsabb, hatékonyabb, pontosabb lehet a felderítése, és a védekezési, továbbá a helyreállítási feladatok ellátása is.

A társadalom és a technika fejlődésével lehetőség nyílt a kárterületen új végrehajtási módok kifejlesztésére, alkalmazására, ilyen például a pilóta nélküli repülőgépek bevetése a légi sugárfelderítésben. A hazánkban működő, és feladatrendszerüket tekintve katasztrófavédelmi feladatok ellátását is biztosító szervezetek közül több is rendelkezik olyan légijárművel, amelyek jól alkalmazhatóak ezekben az esetekben.

A Magyar Honvédség is ezek közé tartozik, és rendszeresen részt vesz a katasztrófák következményeinek felszámolásában. Az erre a célra kialakított HKR rendszere logikus felépítésű, jól szervezett, minden szempontból alkalmas a felderítési, mentési és a kárfelszámolási feladatok ellátására. A HKR részét képező légi járművek mind felszerelésüket, mind eszközeiket, valamint személyzetük felkészültségét tekintve képesek arra, hogy a felderítést, a kárelhárítást és a helyreállítást egyaránt hatékonyabbá és gyorsabbá tegyék. Ezek között ki kell emelni a légi kutató-, mentő-, árvízvédelmi-, tűzoltási-, légi sugár-felderítési szolgálatokat, és azok képességeit.

Az ilyen jellegű feladatokat végző szervezetek tevékenységének sikere azonban nagyban függ attól is, hogy milyen az együttműködésük rendje, formája, illetve a mentő állomány együttműködési készsége és ismerete. A hatékonyság növelésére a kárterületen megjelenő szervezetek állományának alapképzésébe, továbbképzésébe célszerű lesz beleépíteni a jövőben a katasztrófavédelmi ismereteket, köztük különösen az együttműködés rendjére vonatkozó információkat, valamint az egymás képességeinek, működésének megismerését. Növelheti a kárterület felderítésének és a mentés eredményességét, ha a katasztrófavédelem állománya, valamint a védelmi igazgatás különböző szintjein dolgozó döntéshozók alapképzésében, továbbképzésében, felkészítésében helyet kapnak a civil és hivatásos szervezetek képességeit, alkalmazhatóságának területeit, módját bemutató ismeretanyagok is.

Légieszköz-parkjának alkalmazásával, a jelenleg működő katasztrófavédelmi feladatokat ellátó szolgálatok mellett, időben és megfelelő módon riasztva és alkalmazva, mind a civil szervezetek, mind a Magyar Honvédség eredményesen járulhatnak hozzá a rendkívüli események kárterületének felderítéséhez, a kutatáshoz, a mentéshez, valamint a kárelhárítás- és kárfelszámolás feladatainak hatékony, gyors végrehajtásához.

Felhasznált irodalom

[1] Csendes katasztrófák. http://csendeskatasztrofa.voroskereszt.hu/index.php/mi-az-a-csendes-katasztrofa/tenyek-es-szamok Letöltés: 2013. május 02.

[2] A Worldwatch Institute jelenti. http://www.deol.hu/main.php?c=10790 Letöltés: 2013. május 02.

[3] Einsatzarten – der Sinn der Luftrettung. http://www.rth.info/basiswissen/basiswissen.php?keyword=indikationen Letöltés: 2013. május 02.

[4] Auf einen Blick. http://www.rth.info/betreiber/betreiber.php?show=bmi Letöltés: 2013. május 02.

[5] Ujházy László: A Magyar Tartalékosok Szövetsége; In: Sereg Szemle, 2011. évi 3–4. szám, 189. old. ISSN 2060-3924

[6] Dr. Hornyacsek Júlia: A települési védelmi képességek a katasztrófa-kihívások tükrében, Budapest, 2011. Biztonságunk Érdekében OTTE, 52. oldal http://www.drhornyacsek.hu/sajat%20publikaciok/vedelmi%20kepessegek.pdf Letöltés: 2013. május 02.

[7] Benesóczky Imre – Dr. Kádár Pál: A honvédelmi tárca katasztrófavédelmi kötelezettségei és kapcsolódó igazgatási feladatok a haderő tíz éves fejlesztésének tükrében, Budapest, 2004. HM OTT 2. sz. Programbizottságánál (HM TKF) végzett tudományos munka keretében készült, 102. oldal. http://www.honvedelem.hu/files/9/4954/07.pdf Letöltés: 2013. május 14.

[8] Orosz Zoltán: Helikopterek alkalmazhatósága, a légi kutató mentő képesség technikai felszerelése és a fejlődés iránya. Repüléstudományi közlemények különszám, Szolnok, 2003., 6. oldal http://www.szrfk.hu/rtk/kulonszamok/2003_cikkek/orosz_zoltan.pdf Letöltés: 2013. május 21.

[9] 267/2011. (XII. 13.) Korm. Rendelet a bajba jutott légi járművek megsegítését, valamint a katasztrófák elleni védekezéssel és a mentéssel összefüggő tevékenységet ellátó légi kutató-mentő szolgálat szervezetéről, működésének, fenntartásának, riasztásának és a mentéssel járó költségek viselésének rendjéről, e tevékenységek engedélyezésére vonatkozó szabályokról. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100267.KOR Letöltés: 2013. május 21.

[10] Zelenák János – Nagy Gábor – Csurgai József et al.: A légi sugárfelderítés képességei alkalmazhatóságának vizsgálata elveszett, vagy ellopott sugárforrások felkutatása, illetve szennyezett terepszakaszok felderítése során. Repüléstudományi konferencia különszám, Szolnok, 2009., 2. oldal http://www.szrfk.hu/rtk/kulonszamok/2009_cikkek/Csurgai_Jozsef_stb.pdf Letöltés: 2013. május 21.

[11] Padányi József: A Magyar Honvédség lehetőségei és korlátai az árvízi védekezésben. http://www.sija.hu/wpcontent/uploads/2012/04/padanyi_jozsef_a_magyar_honvedseg_lehetosegei.pdf Letöltés: 2013. május 21.

[12] Nemzeti konszenzus a helikopter- és szállítórepülőgép-képességről. (2013. 05. 22.) http://www.honvedelem.hu/cikk/38185 Letöltés: 2013. december 21.)

Ábraforrások:

[13] Dr. Szabó Sándor – Dr. Tóth Rudolf: A kárelhárítási és kárfelszámolási feladatok értelmezése a katasztrófavédelem területén. VIth International Symposium on Defence Technology, 6-7 May 2010, Budapest, Hungary Konferencia kiadvány, 8. oldal 3. sz. ábra, ISSN 1416-1443

[14] Vízügy honlap – kárelhárítási munkák a vörös iszap katasztrófa után (Torna-patak, Marcal). 2010.október URL: http://www.vizugy.hu/gallery.php?keptarid=20#5 Nincs megjelölve, Letöltés: 2013. május 03.

[15] JAS 39 Gripen. URL: http://gripen.uw.hu/ Nincs megjelölve, Letöltés: 2013. május 03.

[16] Nagy Sándor pv. ezredes: Szlovák katonai repülőgép balesete Hejcén. 2006. március 15. URL: http://www.vedelem.hu/letoltes/tanulmany/tan70.pdf Nincs megjelölve, Letöltés: 2013. május 20.

[17] Új rendszerben működik a kutató-mentő szolgálat, Készítette: Dévényi Veronika URL**:** http://www.honvedelem.hu/cikk/35433 Letöltés: 2013. május 20.

[18] Nukleáris katasztrófa fenyeget Japánban, Készítette: Nincs megjelölve, URL: http://vilagszam.hu/cikkek/nuklearis-katasztrofa-fenyeget-japanban-megismetlodhet-a-csernobili-eset.html/1516 Letöltés: 2013. május 20.

[19] Inside the Drone Missions to Fukushima, Készítette: Nincs megjelölve, URL: http://www.theatlantic.com/technology/archive/2011/04/inside-the-drone-missions-to-fukushima/237981/ Letöltés: 2013. május 25.

[20] Helikopter dolgozik az Onga-Ócsanálos közötti töltésszakaszon, Készítette: Nincs megjelölve, URL: http://www.origo.hu/itthon/percrolpercre/20100609-apadnak-az-eszakmagyarorszagi-folyok-arad-a-tisza-arvizi-helyzet.html?pIdx=1 Letöltés: 2013. május 25.

[21] Magyar Légimentő Nonprofit Kft. Bázisai, Készítette: Nincs megjelölve, URL: http://www.legimentok.hu/bemutatkozunk/kuldetesunk#scrollhere Letöltés: 2013. május 25.

[22] Mentők a város felett, Készítette: Simon Péter URL: http://repulnijo.hu/2008/02/14/mentok-a-varos-felett/ Letöltés: 2013. május 25.

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Kátai-Urbán Lajos - Kiss Enikő
katai.lajos@uni-nke.hu - eniko.kiss@mailbox.hu

A VESZÉLYES ÁRU BELVÍZI SZÁLLÍTÁSÁVAL KAPCSOLATOS KATASZTRÓFAVÉDELMI FELADATOK VÉGREHAJTÁSI TAPASZTALATAINAK ÉRTÉKELÉSE

Abstract

A veszélyes áru belvízi szállításának hatósági ellenőrzése nem egészen két évvel ezelőtt került a katasztrófavédelem hatáskörébe. A veszélyes áru belvízi szállítására vonatkozó nemzetközi előírásokat az ADN Szabályzat tartalmazza. Az ADN ellenőrzés a fővárosban (speciális helyzete miatt) és Mohácson (schengeni határ) számítanak kiemelten fontos feladatnak. Mohácson 2012. július 4-én hozták létre a hajóellenőri szolgálatot a kikötő épületében, ahol a katasztrófavédelem munkatársai 24/48 órás szolgálati rend szerint ellenőrzik az összes Európai Unióba be- és kilépő veszélyes árut szállító hajót, valamint 2012 augusztusa óta az ADN hatálya alá nem tartozó vízi járműveket is. Jelen cikk célja az eddigi tapasztalatok értékelése, az eredmények bemutatása, valamint javaslattétel a hiányosságok pótlására.

It hasn't even been two years since disaster management took over the enforcement process of the transportation of dangerous goods by inland waterway. The international regulations of the transportation of dangerous goods by inland waterways are recorded in the ADN manual. The ADN control is a highlighted task in the capital city (due to its special situation) and in Mohács (external border of the Schengen Area). We've established our ship inspector unit in Mohács in the building of the border port on 4th July, 2012. Since that the employees of the disaster management check all the ships carrying dangerous goods entering or leaving the territory of the European Union. Furthermore, they also check the other vechicles on water since August, 2012. The main goals of this article are to evaluate the experiences, present the achievements and make proposals on how to correct the mistakes and deficiencies.

Kulcsszavak: *veszélyes áru szállítás, ADN, iparbiztonság, Magyarország, Duna ~ transportation of dangerous goods, ADN, industrial safety, Hungary, Danube*

A VESZÉLYES ÁRU BELVÍZI SZÁLLÍTÁSÁNAK SZABÁLYOZÁSA

A veszélyes anyagok vízi szállításának ellenőrzése a katasztrófavédelem számára még mindig új feladatnak számít, csupán két éve került át a katasztrófavédelem hatáskörébe. Ebből kifolyólag aránylag kevés információ áll rendelkezésünkre és kevés a tapasztalat, viszont egy nagyon fontos területről van szó és már ennyi idő alatt is jelentős fejlődés látható a veszélyes anyagok vízi szállításával kapcsolatos szabályok betartatásával kapcsolatban.

A Dunán szinte kizárólag nemzetközi viszonylatban folyik a veszélyes áru szállítása, a vízi járművek nagyrésze pedig az Európai Unió tagállamain kívülről érkezik a Duna hazai szakaszára. A hajók Mohács Határkikötőnél lépik át a schengeni határt mind a szerb, mind pedig a horvát oldalról, belépő hajók esetében ezáltal belépve az Európai Unió területére. Ahogy a közúton, úgy a vízen is megerősített, szigorított ellenőrzést végeznek az ellenőrök, így Magyarországra nagy felelősség nehezedik a hatósági feladatok végrehajtásakor.

Egy vízi járművön többnyire igen jelentős mennyiségű árut szállítanak egyidejűleg. Az alábbi kép is érzékelteti, hogy egyetlen 1500 tonnás áruszállító hajóval való áruszállítás mennyivel gazdaságosabb egy vasúti, vagy közúti szállításhoz képest. Egy 38 db 40 tonnás vasúti kocsiból álló szerelvényt még hamarabb el tudunk képzelni, mint egy 50 darab 30 tonnás ugyanazon árut szállító kamionból álló konvojt. Ebből arra is következtethetünk, hogy ha egyetlen hajó ennyi anyagot szállít egy alkalommal, akkor egy hajón elkövetett szabálytalanság mekkora veszélyt hordoz magában. Ezért is kiemelt fontosságú a veszélyes áruk vízi szállításának katasztrófavédelmi hatósági ellenőrzése, hiszen a szabálytalanságok kiszűrésével jelentős mértékben tudjuk csökkenteni a különféle kockázatokat. [1]

Szóbeli beszélgetések során igyekeztünk tapasztalatokat gyűjteni a Fővárosi Katasztrófavédelmi Igazgatóság kirendeltségeinek, a Mohácsi Kirendeltség hajóellenőri szolgálatának, a BM Országos Katasztrófavédelmi Főigazgatóság Veszélyes Szállítmányok Főosztályának, valamint a Hungária Veszélyesáru Mérnöki Iroda (HVESZ) munkatársaitól.

A veszélyes áru szállítása történhet közúton, vasúton, vízen vagy levegőben. A különféle szállítási módokra különféle nemzetközi szabályozások vonatkoznak: az ADN, az ADR, az IMSBC Kódex, az ICAO-TI (IATA DGR), az IMDG Kódex és a RID. A veszélyes áru vízi szállításával kapcsolatos katasztrófavédelmi hatósági feladatok végrehajtását mind a magyar, mind pedig a nemzetközi jogszabályok, előírások betartásával végzik. A Duna magyarországi szakaszán veszélyes árut szállító vízi járművek számára a nemzetközileg a Veszélyes Áruk Nemzetközi Belvízi Szállításáról szóló Európai Megállapodáshoz (ADN[1]) csatolt Szabályzat ismerete, alkalmazása és betartása kötelező. Az ADN, az ADR és a RID előírásai hasonlóak, illetve keresztutalásokat tartalmaznak egymásra.

AZ ADR MELLETT AZ ADN ÉS RID ELLENŐRZÉSEK A KATASZTRÓFAVÉDELEMI SZERVEK HATÁSKÖRÉBEN [2, 3]

A 2012. január 1-jével végbemenő változásokkal egyidejűleg a katasztrófavédelem új feladatokat is kapott. Így innentől már nem csak a veszélyes áruk közúti ellenőrzésével kapcsolatos feladatok, de a vasúti, vízi szállítás ellenőrzése is a katasztrófavédelem hatáskörébe tartoznak. Az új feladatok végrehajtására történő felkészülés keretén belül 2011 óta a veszélyes áruk vasúti, vízi, és légi szállítására vonatkozó jogszabályi előírások tekintetében több tanfolyami képzés is megvalósult.

A hatósági ellenőrzések és hatósági ügyek, valamint az alkalmanként jelentkező egyeztetési feladatok végrehajtása érdekében rendkívül fontos a társszervekkel való szoros együttműködés. A Veszélyes Szállítmányok Főosztály a 2012. évtől kezdődően számos, a társhatóságok által

[1] Francia: **A**ccord européen relatif au transport international des marchandises **D**angereuses par voises de **N**avigation intérieures

szervezett a veszélyes áru szállítás ellenőrzését célzó akciósorozat végrehajtásában, koordinálásában vett részt. A társhatóságok részéről az ellenőrzéssorozatok résztvevői a Nemzeti Közlekedési Hatóság, Nemzeti Adó-és Vámhivatal, az Országos Rendőr-főkapitányság és a Budapesti Rendőr-főkapitányság Dunai Vízirendészeti Rendőrkapitánysága és illetékes szervei voltak.

A BM OKF közleménye szerint a társhatóságokkal való együttműködés minden esetben megfelelő és hatékony volt, ezért az Országos Iparbiztonsági Főfelügyelőség és a Veszélyes Szállítmányok Főosztály koordinálásával az országos hatáskörű akció sorozatok a 2013-as évben is folytatódtak. Az akciók célja az illegális nemzetközi és belföldi veszélyes szállítmányok felderítése, a rejtett vagy szabálytalan veszélyes áru szállítások feltárása, valamint a szállítási alágazatonkénti nyomon követése, különös tekintettel a Magyarország területére belépő szállítmányok ellenőrzésére.

A hivatásos katasztrófavédelmi szerv eljárásai során a veszélyes áruk belvízi szállításának ellenőrzésére és a bírság kivetésére vonatkozó egységes eljárás szabályairól, továbbá az egyes szabálytalanságokért kiszabható bírságok összegéről, valamint a bírságolással összefüggő hatósági feladatok általános szabályairól a 312/2011. (XII. 23.) Korm. rendelet rendelkezik.

Az ellenőrzés lefolytatására a katasztrófavédelmi hatóság helyi szerve jogosult. Önálló ellenőrzési tevékenységet végezhet más katasztrófavédelmi hatóság illetékességi területén is a katasztrófavédelmi hatóság központi szervének előzetes jóváhagyása alapján. A 312/2011. (XII. 23.) Korm. rend. ezen módosítása 2013.07.04-én lépett hatályba, ezért a korábbi statisztikák, beszámolók alapján az akkor hatályban lévő jogszabályoknak megfelelően még a területi szerv is említésre kerül ellenőrző szervként.

A veszélyes áru szállításával kapcsolatos szabályok megsértése esetén a bírság kiszabására és egyéb hatósági intézkedés megtételére első fokon a katasztrófavédelmi hatóságnak az ellenőrzést végrehajtó helyi szerve, másodfokon pedig a katasztrófavédelmi hatóság első fokon eljárt helyi szervét irányító területi szerve jogosult.

A veszélyes áru szállításának bejelentésekor belföldi rakodás esetében a berakás, külföldi rakodás esetében a határátlépés helye szerinti katasztrófavédelmi hatóság területi szerve az illetékes.

A veszélyes áru vízi úton végzett szállításakor a katasztrófavédelmi hatóság illetékessége a folyó határ menti, szomszédos állammal közös szakaszán az államhatárig terjed.

Az eljárásrendet a 127/2012-es BM OKF főigazgatói intézkedés határozza meg, amely 2013. január 1-jén lépett hatályba. Az intézkedés hatálya kiterjed a hivatásos katasztrófavédelmi szerv központi szervére (BM OKF), területi szerveire (igazgatóságok), valamint helyi szerveire (kirendeltségek).

SZÁLLÍTMÁNYOZÁS A DUNA MAGYARORSZÁGI SZAKASZÁN

A szállítmány típusát tekintve megkülönböztetünk szárazárut és folyékony rakományt szállító hajókat. A szárazáru lehet ömlesztett (ömleszthető, szilárd anyagok csomagolás nélküli szállítása), küldeménydarabos (feladásra kész csomagolóeszközökből, nagycsomagolásból, vagy IBC-ből és tartalmából áll), és Ro-Ro (Roll on - Roll off, közúti-vízi kombinált szállítás). A folyékony árut pedig tartályhajóban szállítjuk, melynek több típusa van. A tartályhajók típusait az ADN Szabályzat határozza meg.

A vízi járművek hajtó berendezésük szerint tovább osztályozhatóak, így lehetnek géphajók, önjáró hajók, vontatóhajók, tolóhajók, gépnélküli uszályok, illetve bárkák. A hajó típusát az ellenőrzéshez azért fontos ismerni, mert különböző típusokra különböző előírások vonatkoznak, mint például a lékesedési riadó terv vonatkozó előírásai.

A Duna magyarországi szakaszán a veszélyes áruk vízi szállítása szinte kizárólagosan tartályos szállítási módon történik. Ennek oka, hogy a legnagyobb forgalom az üzemanyagok,

főként gázolaj/dízelolaj (UN 1202) és benzin (UN 1203) szállításából tevődik össze. Elvétve előfordul még ömlesztett áru szállítás is, ez leginkább az ADN hatálya alá tartozó műtrágya fogalmában merül ki. Küldeménydarabos veszélyes árut szállító vízi járművel a vizsgált időszakban hazánk területén még nem találkoztak.

ELLENŐRZÉS TERÜLETI SZINTJE

Magyarországon a veszélyes áru vízi szállításának katasztrófavédelmi hatósági ellenőrzésében a hajózhatósági adatok alapján (pl.: meder, vízállás, hajóforgalom) csak a Duna menti megyék érintettek. Ezáltal az ellenőrzések Győr-Moson-Sopron, Komárom-Esztergom, Pest, Fejér, Bács-Kiskun, Tolna és Baranya megye, valamint a főváros hatáskörébe tartoznak. Ezek közül is kiemelt jelentőségű a vízi ellenőrzés Baranya megyében, valamint a fővárosban. Baranya megyében Mohácson található a szerb-horvát-magyar hármashatár, ahol kivétel nélkül minden belépő és kilépő vízi jármű átfogó ellenőrzésen megy át, hiszen itt kezdődik és ér véget a schengeni övezet.

A főváros pedig a település katasztrófavédelmi besorolása, valamint speciális központi szerepe miatt számít kiemelt fontosságú területnek. Ennek oka - a teljesség igénye nélkül -, hogy jelentősen koncentráltan vannak jelen a fontos és védett közintézmények (pl.: minisztériumok, hivatalok, a Parlament), Seveso hatálya alá tartozó felsőküszöbértékű üzemek, védett személyek lakó- és közintézményei, a nemzetközi vízi forgalom lebonyolításában résztvevő üzemek, illetve a lakosság igen magas száma. Továbbá a vízi ellenőrzés a fuvarozás feltartóztatása nélkül kell, hogy történjen, és egyelőre kizárólag a Fővárosi Katasztrófavédelmi Igazgatóságnak van tűzoltóhajója.

ORSZÁGOS ÉVES ELLENŐRZÉSI STATISZTIKA (2012) [4]

Kutatásunk során a gyakorlati részeken túlmenően rendelkezésünkre bocsátotta a BM OKF Veszélyes Szállítmányok Főosztálya a 2012-es országos statisztikát is. A 2012-es év során összesen 43 db határozat született: 42 Baranya megyében, 1 pedig Tolna megyében. A 43 határozatból mindössze 3 jutott másodfokra, a másik negyvennek nagyrészét elismerték és befizették. 2012. során összesen 315 alkalommal volt vízi ellenőrzés. Az ellenőrzéseknek több mint fele Baranya megyében, ott 184 alkalommal, de a fővárosban is nagy számmal volt ellenőrzés, itt összesen 40 alkalommal. A pontos megyei eloszlás az alábbi táblázatban látható.

Megye	**Alkalom**
Bács-Kiskun megye	7
Baranya megye	184
Fejér megye	13
Győr-Moson-Sopron megye	31
Komárom-Esztergom megye	18
Pest megye	4
Tolna megye	18
FKI	40

1. táblázat. Ellenőrzési számok vízen (2012)

Telephelyi ellenőrzésekből jóval kevesebb volt, ennek oka, hogy nem mindenhol van ellenőrizendő telephely, tehát bizonyos megyékben ez a tevékenység egyértelműen tárgytalannak tekinthető. Országosan összesen 20 telephelyi ellenőrzés volt, ennek 25%-a a fővárosban.

Megye	Alkalom
Bács-Kiskun megye	4
Baranya megye	0
Fejér megye	0
Győr-Moson-Sopron megye	4
Komárom-Esztergom megye	3
Pest megye	1
Tolna megye	3
FKI	5

2. táblázat. Ellenőrzési számok telephelyen (2012)

A 2012-es év során országosan összesen 1995 vízi járművet ellenőriztek a katasztrófavédelem munkatársai, amelyből 1199 jármű szállított veszélyes árut. A legtöbb járművet Baranya megyében ellenőrizték, összesen 1479-et, amelyből 61%-a volt veszélyes árut szállító jármű. A fővárosban is hasonló volt az arány, itt összesen 139 járművel ellenőriztek, ezeknek 59%-a volt ADN-es.

Megye	Ellenőrzött járművek száma	
	ADN	Nem jelölt
Bács-Kiskun megye	24	21
Baranya megye	899	580
Fejér megye	54	47
Győr-Moson-Sopron megye	48	48
Komárom-Esztergom megye	38	17
Pest megye	11	4
Tolna megye	43	22
FKI	82	57

3. táblázat. Ellenőrzött ADN-es és nem jelölt járművek száma (2012)

A hatóság munkájának rendkívüliségét támasztja alá, hogy a 2012-es év során ellenőrzött járműveknek mindössze 5%-a volt belföldi. A járművek 33%-a EU tagállamból, 62%-a pedig EU tagállamon kívülről érkezett. A százalékos arányból jól látszik, hogy a magyarországi ellenőrzésnek azért is fontos szerepe van, mert az itt áthaladó járművek többségében az Európai Unión kívülről érkeznek, ezzel együtt pedig a schengeni övezetbe is itt lépnek be.

A 2002. évre vonatkozó statisztikák alapján a hibás szállítóegységeknek mindössze 3%-a belföldi, egészen nagy arányban, 44%-ban EU tagállambeli, 53%-ban pedig EU tagállamon kívüli.

Az eddigi tapasztalatok alapján elmondható, hogy éves szinten 100 millió tonna veszélyes árut szállítanak a Dunán, és átlagosan 3200, az ADN hatálya alá tartozó veszélyes árut szállító hajó jelentkezik be a NAVINFO rendszeren keresztül. Ahogy már korábban is említettem, a legtöbb hajó valamilyen üzemanyagot, gázolajat, benzint szállít. A katasztrófavédelem 2012. január 1-je óta nyolc megyei katasztrófavédelmi igazgatóság területén ellenőriz a Duna mentén.

ÖSSZEGZÉS, JAVASLATTÉTEL

Szerencsére a Duna magyarországi szakaszán nem jellemző a veszélyes áru vízi szállítása során bekövetkező baleset. Mindössze két megfeneklés miatti baleset történt az elmúlt két évben, azok során nem jutott veszélyes anyag a környezetbe.

A fővárosban és a határkikötőben szerzett tapasztalatok hasonlóságot mutatnak. Az eljárások többsége az okmányok, illetve a tűzoltó készülékek és egyéni védőeszközök teljes, vagy részleges hiányából, illetve hibáiból kerülnek elindításra, de a statisztikák javuló tendenciát mutatnak.

Összességében elmondható, hogy az elmúlt másfél évben nagy változások történtek a veszélyes áru vízi szállítására vonatkozó szabályok betartásában. Ennek oka, hogy a katasztrófavédelem a feladat átvétele óta nagy odafigyeléssel, valamint a korábban közúton szerzett tapasztalatokat hasznosítva kezdte meg és folytatja az ellenőrzéseket.

Rövid idő alatt a hajókon a biztonság jelentős mértékben javult, hiszen a legtöbb szállítmányozó cég hajói nem egy alkalommal lépnek be az országba, és ezzel az Európai Unióba, hanem heti, vagy havi rendszerességgel megfordulnak hazánk vízi útvonalán. Ezáltal a kezdetben feltárt szabálytalanságokat a szankcionálások elkerülése érdekében igyekeznek kijavítani, valamint a hiányosságok pótlása mellett az eszközöket, okmányokat folyamatosan kontroll alatt tartani, szükség esetén felülvizsgáltatni, okmányok esetében az engedélyeket időben meghosszabbítani.

Az ellenőrzéseknek nemzetközileg is híre megy, ezért ma már ritkán próbál belépni Magyarország területére olyan hajó, amelyet rendkívül rossz állapota miatt vissza kellene fordítani. Mindemellett továbbra is az újonnan, vagy esetleg kapitányváltás után érkező hajók esetében tárunk fel hiányosságokat.

Amennyiben megszűnne a folyamatos kontroll, valószínűleg a vízi közlekedés biztonsága újra visszakerülne a 2012-es évet megelőző állapotokra, mivel a szállítmányozó cégek többsége az ellenőrzéseken való megfelelés és a bírságolások elkerülése érdekében tartja be a szabályokat. Ez természetesen nem kizárólag a vízi közlekedésre vonatkozik, közúton és vasúton valószínűleg ugyanez lenne a helyzet.

Nagyon jó a társhatóságokkal való együttműködés, amely ezen a területen kiemelten fontos, hiszen a közös akciók, illetve a hajóellenőri szolgálat esetében a mindennapi munkavégzés együtt történik. Mind az információáramlás, mind pedig a feladatok során történő konkrét együttműködés kiváló.

Az ellenőrzés során problémaként merült fel a címzett elköltözése esetén a hajók feltartóztatási lehetőségének hiánya, amely a 312/2011-es Korm. rendelet módosításával megoldható lenne és a bírság kézbesítése ennek eredményeképpen minden bizonnyal megvalósulhatna.

A hatósági ellenőrök képzései és a módszertani útmutatói is rendkívül hasznosak. A katasztrófavédelem munkatársai ezekről pozitívan nyilatkoztak. Az OKJ-s képzésekre vonatkozó változások következtében az eddig alkalmazott veszélyesáru-ügyintéző tanfolyam megszűnt, azt a képzési jegyzékből törölték. Jelenleg a képzési rendszer hiányossága nem megoldott, de a szükséges ismereteket a biztonsági tanácsadói képzésekkel elvégzésével lehet pótolni. Erre minél előbb tartós megoldást kell találni akár új képzések létrehozásával, akár a régebbiek reaktiválásával.

A képzések témaköréhez kapcsolódik az IMDG hiányából adódó problematika és arra történő megoldási javaslat, amely az IMDG lefordíttatásával, illetve jogszabályokba történő adaptálását teszi szükségessé, vagy alternatívaként szakmai (angol) nyelvtanfolyamok és külföldi továbbképzésre való lehetőség biztosítását, valamint azzal egyidejűleg a kódex beszerzését kirendeltségenként legalább egy példányban, a szaknyelvi képzéssel azonos nyelven.

Az ellenőrzések szakmai színvonalának jövőbeni további erősítéséhez szükséges képzéshez kiváló alapot szolgáltat a Nemzeti Közszolgálati Egyetem iparbiztonsági szakirányán folyó képzés, illetve az egyetem Katasztrófavédelmi Intézetének gondozásában hiánypótló jelleggel megjelent az iparbiztonsági szakemberek munkáját segítő egyetemi jegyzet is. [8]

Felhasznált irodalom

[1] Loós Z.: Veszélyes Áru Szállítás - Hatósági feladatok, előadás, 2013

[2] Muhoray Á.: A katasztrófavédelem aktuális feladatai, Mindenki hadtudománya előadássorozat, előadás, 2012. október

[3] Bognár Balázs, Vass Gyula, Kozma Sándor: A BM OKF Országos Iparbiztonsági Főfelügyelőség szakterületeinek bemutatása. ÚJ MAGYAR KÖZIGAZGATÁS 5:(6) pp. 19-27. (2012)

[4] BM OKF Veszélyes Szállítmányok Főosztály adatai alapján

[5] Kozma S.: A veszélyes áru szállítás ellenőrzési és szankcionálási tevékenységének tervezése és végrehajtása, előadás, 2012. január

[6] Fővárosi Katasztrófavédelmi Igazgatóság, Közép-Pesti Katasztrófavédelmi Kirendeltség

[7] Veszélyes áruk vízi szállításának aktuális kérdései, ADN 2013 és az IMDG Code 36-12, HVESZ, 2013

[8] Bognár Balázs, Kátai-Urbán Lajos, Kossa György, Kozma Sándor, Szakál Béla, Vass Gyula: Kátai-Urbán Lajos (szerk.) IPARBIZTONSÁGTAN I.: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Budapest: Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 564 p. (ISBN:978-615-5344-12-1)

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Kátai-Urbán Lajos - Vass Gyula
katai.lajos@uni-nke.hu - gyula.vass@katved.gov.hu

SAFETY OF HUNGARIAN DANGEROUS ESTABLISMENTS – REVIEW OF THE INDUSTRIAL SAFETY'S AUTHORITY

Abstract

Storage, processing and use of dangerous substances which are present in industrial activities involve the risk of major accidents. Experiences of recent history show that accidents can result in catastrophic effects to the environment of the dangerous industrial establishment and citizens living there. Therefore, it is understandable that protection against major accidents represent one of the determinant elements in industrial safety, and is a complex activity, which includes the technical and managerial tasks of prevention, as well as the measures targeting the mitigation of the damaging effects of accidents and the protection of the population.

Az ipari tevékenységekben jelen lévő veszélyes anyagok tárolása, gyártása és használata magában hordozza a súlyos balesetek bekövetkezésének kockázatát. A közelmúlt eseményeinek tapasztalatai rámutatnak arra, hogy a balesetek katasztrofális hatással lehetnek a veszélyes tevékenység környezetére és az ott lakó állampolgárokra. Érthető tehát, hogy az iparbiztonság egyik meghatározó eleme a súlyos balesetek elleni védekezés, amely komplex tevékenység és magában foglalja a megelőzés műszaki és vezetési feladatait, a lehetséges baleseti események károsító hatásainak elhárítását, és a lakosságvédelmi intézkedések bevezetését.

Keywords: *industrial safety, industrial accidents, dangerous substances, prevention, safe operation ~ iparbiztonság, ipari balesetek, veszélyes anyagok, megelőzés, biztonságos üzemeltetés*

INTRODUCTION

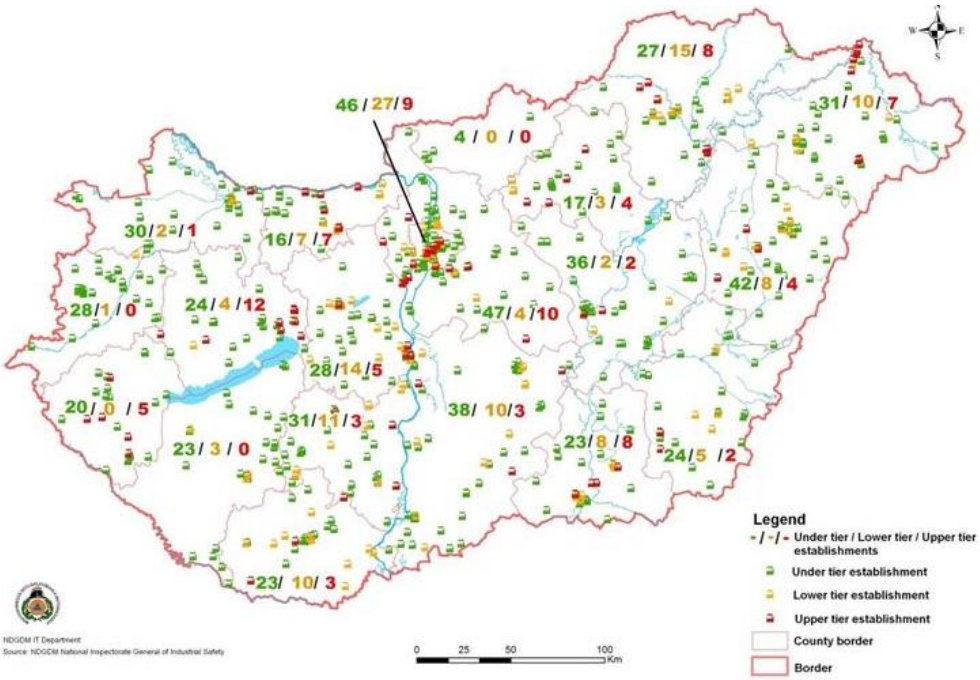
The protection against major accidents involving dangerous substances is based on Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances, that is, the Seveso II Directive. The national legislation was harmonized in 2006, according to this Directive, as amended in 2003; in 2007, the European Commission reviewed the compliance of the Hungarian legislation and deemed it to be EU-compliant. The Seveso II Directive was implemented in Hungary by Act CXXVIII of 2011 on disaster management and the amendments of related acts (hereinafter referred to as "the Disaster Protection Act") and the Government Decree No. 219/2011 (as of October 20) on the protection against major accidents involving dangerous substances.

DESCRIPTION OF HAZARD SOURCES INVOLVING DANGEROUS SUBSTANCES

General information about the dangerous establishments.

The National Directorate General for Disaster Management (Ministry of Interior, NDGDM) established and in cooperation of the 20 regional directorates operates the Industrial Safety Information System which holds data (plant name, registered office, place of business address, status, management, contact information, author of the safety report, supervisor) on more than 730 dangerous plants. The system include data about license requests, safety analyses and safety reports, external emergency plans and other public information submitted by operators of dangerous plants. The system contain all the necessary information required for the implementation of inspection (checking), damage prevention and damage elimination tasks.

Location of the dangerous plants. Hungary has joined the so-called Seveso Plants Information Retrieval System (SPIRS) related to the registration and reporting obligation according to the provisions of the Seveso II Directive. Hungary provides data on the dangerous establishments in Hungary, their activity and location, to this system on an annual basis.



1. figure. Distribution of dangerous plants by counties
(Source: NDGDM)

Classification of the dangerous plants according to their activity. According to their activity, plants subject to the Disaster Protection Act are divided into the categories specified following: gas industry (87); storage of fertilizers (56); oil industry (44); power- and heating plants (31); deposits and logistics centres (63); general chemical industry (51); manufacture of medicines (13); manufacture and storage of plant-health products (48); explosives and ammunition; pyrotechnics (15); plastics industry (35); dangerous waste (23); produce and consumption of biofuel (9), food industry (95), building industry (19), agriculture (90), heavy industry (35), waterworks, bath, swimming pool (28) and other dangerous plants (27). It appears that the plants in the gas industry and oil industry, as well as those in the domain of manufacture and storage fertilizers are in the largest number, but due to the their size and technology the pharmaceutical companies and chemical plants are also important.

Collecting information about emergency incidents and major accidents. The NDGDM registers and analyses the emergency incidents involving dangerous substances and major accidents occurring in Hungary, and in accordance with the provisions of the Seveso II. Directive forwards report to the Major Accident Reporting System (MARS). [3]

Statistical description of data sets

The NDGDM classifies the occurred dangerous events in two main categories in accordance with the legal provisions. The classification is the following:

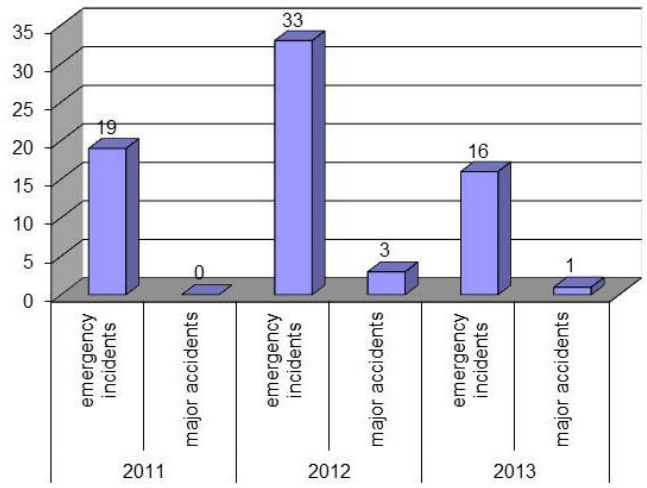
Emergency incident [1]: shall mean the occurrence of such an unforeseen event in the dangerous establishment, in the course of its routine operations or applied technological processes which requires immediate intervention, furthermore, incorporates the potential for the creation of a major accident involving dangerous substances, and has one of the following consequences:

- fire involving dangerous substances,
- explosion involving dangerous substances,
- emission of toxic, carcinogenic substances,
- emission of oxidising, flammable or eco-toxic fluid a quantity of at least 1000 kg,
- emission of other dangerous substances a quantity of at least 0,1% of the upper threshold,
- stop of a dangerous establishment.

Major accident involving dangerous substances [1]: shall mean an occurrence of such an emergency incident which involves the emission of dangerous substances in significant quantities, major fires, or explosions resulting from uncontrolled developments in the course of the operation of any dangerous establishment, and leading to major hazards or damages to human health or the environment, immediate or delayed, inside or outside the establishment.

Any major accident involving dangerous substances having at least one of the consequences described in the related annex dealing with the major accident reporting obligations of the Hungarian and Seveso regulation. [1]

The statistical overview of registered emergency incidents and major accidents illustrates the relevance of the risk area.



2. figure. Number of emergency incidents and major accidents in Hungary (Source: NDGDM)

4 major accidents occurred in 2012 and in 2013 in lower tier threshold establishments or in upper tier establishments, but not reached the level required to be reported to the European Commission.

METHODS USED IN THE RISK EVALUATION

According to the national legislation in force, the responsibilities of the NDGDM and of the 20 regional directorates, established in the protection against major accidents involving dangerous substances, include the operation of the administrative authorization system and the supervision and control system for the plants subject to the Seveso II Directive and for under tier plants (establishments under lower-tier threshold is 25%).
Pursuant to its legal obligations, the 20 Directorate for Disaster Management are responsible for the administrative authorization of dangerous establishments of an upper tier of 97 and a lower tier of 128, and of 509 establishments under lower tier threshold (data as of September 05, 2013) in Hungary, as well as for the regular official controls to be conducted in every 1, 2 or 3 years.

Requirements on the demonstration of safe operation.

The Disaster Protection Act requires the operators of dangerous establishments to demonstrate that their activities do not pose an unacceptable hazard to the population, material assets and the environment, and that they made every reasonable effort to prevent major accidents and reduce their effects. Depending on the dangerous impact, the operator can be required to provide data, prepare safety reports, safety analyses or serious damage prevention plan, and an internal protection plan for the site (as part of the safety report or safety analyses), ensure the conditions for carrying out the responsibilities specified in the internal protection plan, information of the population on the dangerous activities, potential hazards to the population and protection measures taken. [1]

The plants subject to the Disaster Protection Act shall assess the realistic possibility, probability, causes and conditions of major accidents on grounds in the documentation submitted to the authorities. These assessments shall describe the external or internal causes of accidents, and the probable stages of the course of accidents. The operator may use any method to identify the risks and assess the risk of major accidents that are used in the international practice and generally recognised by the professional community. The most widespread method used in Hungary is the quantitative risk assessment method. [1]

The operator – beyond the prompt information obligation - shall forward a preliminary report on the major accident involving dangerous substances occurred in the dangerous establishment in 24 hours after its occurring when the accident complies with at least one of the conditions above. The preliminary report shall include at least the place, date of the major accident, type, supposed reason, dangerous substances involved, immediate effects on man and the environment, and emergency measures taken. [2]

The operator in the event of reporting obligation above shall send a detailed report on the major-accident involving dangerous substances to the regional directorate within 15 days following its investigation. The operator shall send a complementary report to the authority if new fact or circumstance is revealed about the accident. The reporting obligation is independent from the participation of the regional or local bodies of the NDGDM in the response to a major accident. The operator informs the authority on the emergency incident occurred in the dangerous industrial establishment within fifteen days following its investigation. [3]

The regional directorate shall inspect if it necessary on-site the coverage of reality of the report, the circumstances of the emergency incident or major accident and requests further information from the operator. The regional directorate obliges the operator to eliminate the technical, management and control inadequacies revealed in the report by providing sufficient time frame and the operator shall inform in written the authority about the measures taken.

Necessary to carry out complex calculations involving the application of dispersion models in the performance of quantitative risk analysis. The spread of the different materials is strongly dependent on the weather situation and the material characteristics, but it is very difficult to calculate accurately known even under boundary conditions.

Since the amount of released material may not know ahead of time, hence the propagation models anticipate only very roughly the size of areas at risk from pollutants. The same is true of the dose-response models that describe the effects of various substances in man. Sensitivity to certain substances is highly dependent on the individual and very vaguely predictable concentration as well.

Different methods are used to estimate the likelihood of the accident scenarios. The method is used, when the frequency of occurrence is ordered from repository for standardized accident scenarios, which is based on experience. This method is simple, but - because of the accident sequence of events may differ significantly from our standardized study - can be a serious source of error. Other approach represents the estimating of the probability based on the accident scenarios analysis, that it uses methods such as event - tree and fault tree analysis. It is well established that the census of accidents based on frequency of occurrence allows a more complete risk assessment, as the qualitative methods. Critics of this approach state that uncertainties arise on the frequency of causal events. [3]

Prevention and preparedness requirements of safe operation

Evaluation of the risk posed by dangerous establishments. An important step in the evaluation of the risk assessments submitted in the safety documentation is to compare the risk indices calculated on the basis of these assessments with the authorization criteria defined in the legislation. The most important authorization criteria are the value for individual risk and social risk:

Individual risk: this indicates the frequency of deaths (fatal event/year) of those present at a site as a result of a major accident involving dangerous substances. In terms of acceptability, the individual risk is usually taken into account when the persons present at the site are those who are permanently there.

Social risk: this indicates the frequency of deaths (fatal event/year) of a group present at a site (area) as a result of a major accident involving dangerous substances. The acceptable level of the social risk also depends on the number of persons involved in the accident. In terms of

acceptability, the social risk is usually taken into account when large masses of people are present at the site (such as workplaces or shopping centres).

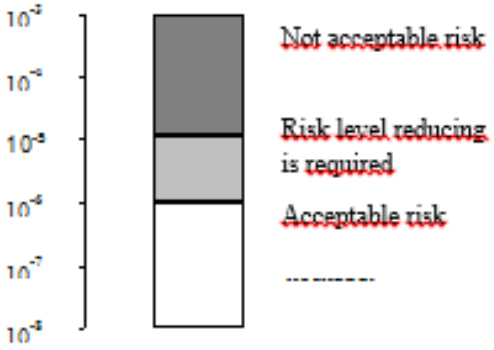
Acceptability of the individual risk. An acceptable level of risk exists if the residential area is in a zone where the individual risk of death as a result of a major accident does not exceed 10-6 event/year.

It does not indicate an acceptable level of risk if the individual risk of death in a residential area is between 10-6 event/year and 10-5 event/year. In this case, the regional directorate shall require the operator to take measures to reduce the risk associated with its activity or to ensure the conditions for safety measures (such as alarm, personal protection and isolation) to reduce the risk level.

It is not acceptable if the individual risk of death in a part of the hazard zone exceeds 10-5 event/year. If this risk cannot be reduced in the local planning procedure, the regional directorate shall require the operator to limit or terminate its activity.

This may basically involve several things:

- If one (or more) residential building(s) is (are) in a hazard zone with value exceeding 10-5 event/year, the operator of the dangerous establishment shall terminate the dangerous activity or the part of the activity which causes a specific threat;
- The operator shall transform its technology so that the buildings affected are outside that zone;
- The operator shall buy the buildings concerned and terminate their function as residential buildings (or any other function that makes them suitable to receive large masses of people). [2]



3. figure. Acceptance criterion for individual risk [2]

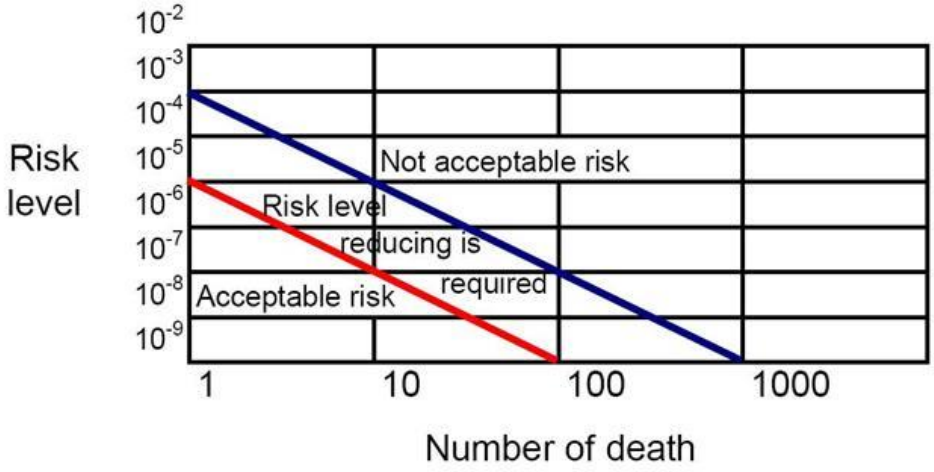
Acceptability of the social risk. The x-axis of the F-N curve shows the number of deaths (N). This number shall be displayed on a logarithmic scale so as the lowest value displayed is The y-axis of the F-N curve indicates the total frequency of accidents causing N or more deaths. This cumulated frequency should be plotted on a logarithmic scale so as the lowest value displayed is 10-9 1/year.

The social risk is acceptable without conditions if F<(10-5 x N-2) 1/year, where N>=1.

The social risk is acceptable with conditions if it is between F<(10-3 x N-2) 1/year, and F>(10-5 x N-2) 1/year, where N>=1.

In this case, in order to reduce the risk associated with the activity, the regional directorate shall require the operator to take on-site preventive safety measures (such as alarm, personal protection and isolation) to reduce the risk level.

It is not acceptable risk if F>(10-3 x N-2) 1/year, where N>=1. In this case, if the risk cannot be reduced by other means, the regional directorate shall require the operator to limit or terminate the activity. [2]



4. figure. Acceptance criterion for social risk [2]

Demarcation of the hazard zone. In order to mitigate the consequences of major accident, the regional directorate shall designate the limits of the hazard zone around the dangerous industrial establishment based on the safety report or the safety analysis.

Developments may be limited within this hazard zone, and measures to protect the population may be laid down in a specific regulation.

This hazard zone may be divided into the inner zone, the middle zone and the outer zone:

Inner zone: the individual injury risk exceeds 10-5 event/year.

Middle zone: the individual injury risk is between 10-5 and 10-6 event/year.

Outer zone: the individual injury risk is below 10-6 event/year, but is above 3x10-7.

In addition to the number of people living in the hazard zone, location, protection and environmental planning, the regional directorate shall determine whether new dangerous industrial establishments may be authorized in a hazard zone and the existing dangerous industrial establishments can be developed to an extent that requires the complementation of the safety report or the safety analysis, based on the dangerous industrial establishments or other structures or buildings in that hazard zone. The regional directorate shall deliver an opinion on the development of the road system, railway network or public utilities, and on other investments or improvements. [3]

Internal and external emergency plans. The operator of a dangerous establishment shall draw up an internal emergency plan meeting the requirements of content and form determined in national legislation to eliminate the consequences of hazards identified in the safety report and safety analysis. The operator shall provide conditions necessary for the accomplishment of tasks defined in the internal emergency plan. The task within the dangerous establishment for limiting the consequences of major accident involving dangerous substances shall be determined by the operator, while the tasks outside the dangerous establishment of the concerned state and municipal organs shall be determined in external emergency plans. The preparation of the external emergency plans is the duty of the competent local organs of the NDGDM with the cooperation of the mayors of the relevant localities endangered. The cost of the preparation of external emergency plans and their exercise are provided in the own budget of the NDGDM. [4] [5]

SUMMARY

In this article the authors introduced the possible hazard sources related to dangerous establishments in Hungary, and introduced the prevention and mitigation requirements and measures necessary for the safe operation of industrial activities.

The Hungarian industrial safety authority as part of the Hungarian Disaster Management Organisation have been applied the European regulations (Seveso II. Directive) in Hungary since 2002 (more than 12 years). In accordance with the statements of the national reports of Hungarian Competent Seveso Authority the Hungarian regulations on the major accidents protection are in full compliance with the Seveso II. Directive's regulations.

It also should also be stated that the Hungarian regulations and their appliance by the Hungarian industrial safety authority provide a high level of protection of human life and the environment in Hungary.

References

[1] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
(Act CXXVIII of 2011 on disaster management and the amendment of related acts)

[2] 219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről (Government Decree No. 219/2011 (as of October 20) on the protection against major accidents involving dangerous substances)

[3] Szakál Béla, Cimer Zsolt, Kátai-Urbán Lajos, Sárosi György, Vass Gyula. Iparbiztonság I.: Veszélyes anyagok és súlyos baleseteik az iparban és a közlekedésben. Budapest (Industrial Safety I. Dangerous Substances and their Major Accidents in the Industry and Transportation). SZIE Ybl Miklós Építéstudományi Kar - Tűzvédelmi és Biztonságtechnikai Intézet. 2012. 113 p. (ISBN:978-963-89073-3-2)

[4] Kátai-Urbán Lajos, Vass Gyula: Development of Hungarian System for Protection against Industrial Accidents. In: Jozef Ristvej (szerk.) 18. medzinárodná vedecká konferencia Riešenie krízových situácií v špecifickom prostredí. Zilina, Szlovákia, 2013.06.05-06. University of Zilina, 2013. pp. 229-239. (ISBN:978-80-554-0699-2)

[5] Bognár Balázs; Juhász István; Kátai-Urbán Lajos (szerk.); Kossa György; Kozma Sándor; Szakál Béla; Vass Gyula: „IPARBIZTONSÁGTAN I." Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához" (Industrial Safety I. Guidance on the Implementation of the Industrial Safety's Tasks of the Operator and Authority). NKE Egyetemi tankönyv. Budapest, 2013. (ISBN 978-615-5344-12-1)

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Komjáthy László - Nagy József
komjathy.laszlo@uni-nke.hu - nagyj3927@gmail.com

A TŰZOLTÓI BEAVATKOZÁSOK HATÉKONYSÁGÁNAK NÖVELÉSI LEHETŐSÉGE EGY SZÁMÍTÓGÉPES DÖNTÉSTÁMOGATÓ PROGRAM KIFEJLESZTÉSÉVEL

Absztrakt

A tűzoltók beavatkozásaik során számos esetben találkoznak váratlan eseménnyel, az információ megszerzésének korlátozottságával, valamint a közelben lévő egységek segítségének szükségességével. A kiszámíthatóság növelése érdekében a szerző egy olyan program kidolgozását kezdte meg, amely alkalmas a rövid idő alatt döntéskényszer alá kerülő parancsnokok helyzetének javítására számítástechnikai eszközök igénybevételével. A program fejlesztése nem ért véget, igény és szükség szerint folytatható, illetve bővíthető. A cikk a program készítése során elért eredményeket, valamint a további lehetőségeket mutatja be.

During the intervention firefighters can face in many cases strange or unexpected events, limited access to the relevant information or the necessity of other fire branches' help. To raise the safety of intervention author began to create software that is able to help the commander to make his decision even if he is pressed for time. The software development has not yet terminated, if required it can continue. Author gives a description of the results that have been reached and shows the possibilities and expectations.

Kulcsszavak: *döntéstámogatás, tűzoltás, katasztrófa-elhárítás, számítógép program ~ decision support, firefighting, disaster management, software*

BEVEZETÉS

A statisztikai adatok azt mutatják, hogy a tűzoltók beavatkozásainak száma szinte évről évre növekszik. Az adatokból kiolvasható az is, hogy bár a tűzesetek számának tendenciája csökken, a műszaki mentések száma ellenben növekedik. Ezért a tűzoltók munkájának megkönnyítéshez bármilyen eszköz alkalmazását meg lehet fontolni, különösen azokét, amelyek viszonylag alacsony költséggel elérhetővé tehetők a beavatkozók számára.

A feladatok hatékonyabb ellátása több szempontból is korlátokba ütközhet. A tűzoltási és műszaki mentési, katasztrófa-elhárítási munkálatok nagyon komplex feladatot jelentenek a beavatkozókra. Az irányításért felelős parancsnoknak nagyon rövid idő alatt kell gyorsan és pontosan döntést hoznia, amely sokszor csak korlátozottan teszi lehetővé a beavatkozáshoz fontos információk összegyűjtését [1]. Ezért számára minden olyan eszköz igénybevétele, amely a hatékonyabb tűzoltást, műszaki mentést és katasztrófa-elhárítást tesz lehetővé, szakmailag indokolt lehet.

Korunkra jellemző, hogy az informatikai rendszerek robbanásszerű fejlődése teljesen átalakította életünket. Ma már ott is internetezhetünk, ahol korábban elképzelhetetlen volt, sőt magát az internet használatát is csak néhány évtizede ismerjük. Ezek a lehetőségek átszövik mindennapjainkat, így a munkánkat is, ezen keresztül zajlik az információ cseréje, banki átutalásaink, sőt a tőzsdei ügyletek is. Ezért a számítógépes rendszerek tűzoltás, műszaki mentés és katasztrófa-elhárítás során történő alkalmazási lehetőségeinek vizsgálata mindenképpen célszerű és indokolt.

A szerző több évtizedes számítástechnikai ismeretei alapján, valamint az ismeretségi körében a katasztrófavédelemnél dolgozók munkájának tisztelete és megbecsüléseként a Nemzeti Közszolgálati Egyetem keretei között megvalósuló projekthez csatlakozva tanulmányozta egy döntéstámogató számítástechnikai program elkészítésének lehetőségét és alkotta meg egy program kereteit, amely célja a tűzoltói bevetések irányításának elősegítése.

A SZOFTVER CÉLJA

A szerző által készített szoftver prototípus célja az, hogy demonstrálja a lehetőségét és a használhatóságát egy olyan informatikai fejlesztésnek, amely katasztrófa helyzetekben (pl. árvíz, tűzeset, földrengés) tényleges segítséget tud nyújtani a felszámolásért felelős vezetők döntéshozatalában. A döntéshozóknak - kiemelten katasztrófa helyzetekben - saját vezetői tapasztalataikra, valamint a körülmények tényleges adataira tekintettel kell meghozniuk a lehető legjobb döntéseket, amelyek célja a különböző jogszabályokban is deklaráltan az emberi élet, a gazdasági javak, valamint a környezet védelme [2]. Ezt vezetéselméleti szempontból tekinthetjük akár helyzetfüggő vezetésnek is.

A szoftver nem tesz javaslatot, vagy ajánlásokat a kialakult helyzet konkrét megoldására, viszont egy sor olyan adattal szolgálhat, amelyek az adott szituációban a felszámolásért felelős szervezetek (pl. tűzoltóság) egységeinek vonulását, a tevékenységek megkezdését, valamint az elhárítás folyamatát döntően befolyásolhatja. Ilyen lehet például az olyan eset, amikor a riasztás beérkezése után (pl. tűzesetek, vegyi vagy biológiai katasztrófa helyzetek, de talán az árvíz kivételével minden esetben), a vonulás megkezdése előtt nincs idő felkészülni a konkrét megoldandó feladatra. A helyszínre érve a tevékenységek megkezdését még tovább hátráltathatja a szükséges információk hiánya [3]. A kutatásaim alapján arra a következtetésre jutottam, hogy a tűzoltók vonulása során kapott információk nem mindig elégségesek a megfelelő döntéshozatalhoz.

Számos esetben előfordul az is, hogy olyan egységeket és szervezeteket kell bevonni a kialakult helyzet felszámolásába, amelyek nem rendelkeznek megfelelő helyismerettel sem a megközelítési útvonalakat, sem a katasztrófa helyszínét illetően. Az együttműködés

szempontjából azonban kulcsfontosságú szerepet kap az információk minősége, különösen ott, ahol a határokon túlról érkező segítség esetén még nyelvi problémák is nehezíthetik a kommunikációt [4].

Mivel a katasztrófák jellege és helye fizikailag meghatározható jellemzőkkel bír, ezért a szoftver prototípusának kifejlesztésekor az volt az alapgondolat, hogy a szolgáltatott információk alapja mindenképpen digitális térkép, ill. térképszelvény legyen. A térkép alapvető információkat tartalmaz a környék vízrajzáról, a folyók elhelyezkedéséről és néhány további jellemzőjéről, az állóvizek, a domborzat, az útvonalak jellegéről, valamint a tereptárgyak közötti távolságokról is. A térképek digitális mivolta biztosítja továbbá azt a fajta „rugalmasságot", hogy ezeken bizonyos módosítások, plusz információk is megjeleníthetők legyenek, valamint azt is, hogy a felhasználhatósága ne legyen hely-, és mennyiségfüggő, a mentésben és katasztrófa helyzetekben résztvevő döntéshozók számára könnyen és azonnal elérhető legyen. A mobil hardver eszközök megjelenésének és elterjedésének köszönhetően ma már nem kell kizárólag a központi ügyeletek helységeiben lévő számítógépes munkaállomásokban gondolkodnunk. A digitális térképek akár a külső helyszínekre is kivihető, a vonulásban résztvevő technikai eszközökre is telepíthetők. Ennek fontosságára már egyéb fejlesztések is ráirányították a figyelmet [5].

A digitális térképek számos előnye mellett szól az is, hogy az információkat meg lehet szűrni, vagyis akár szűkíteni is az adott szükségleteknek megfelelően. Ez jelentheti pl. az adott területre vonatkoztatott adat és képi információ mennyiségének, de akár minőségi követelményeinek szűkítését is. Hétköznapi szóhasználattal élve más szemüvegen keresztül nézve mást és mást látunk a különböző térképen. A szerző a későbbiekben erre még a szűrőfeltétel címszó alatt hivatkozni fog.

Az ún. szűrők még további lehetőséget kínálnak, így egymással tetszőlegesen kombinálhatók, vagyis elemeiben is ki-, és bekapcsolhatók, vagyis elkerülhetővé válik, hogy a digitális térkép tele legyen zsúfolva jelekkel és jelölésekkel.

Könnyen elképzelhető olyan szituáció, amelynél egy időben más és más információra van szüksége a különböző szervezeteknek, illetve egységeknek. Nagyobb volumenű beavatkozásoknál belátható, hogy előbb-utóbb a már beavatkozó egységek mellett további egységek segítségnyújtására is szükség lesz. Az újonnan érkezők vonulása során - az esetleges helyismeret hiánya miatt - az egységeknek további információra lehet szüksége a megközelítési útvonalakról és a helyszínen esetlegesen a beavatkozást hátráltató tényezőkről, akadályokról, miközben a már helyszínen lévőknek a feladat elvégzéséhez szükségesek további, részletesebb információkra lehet szüksége. Ezeket a problémákat egy jól felépített, strukturált rendszerű térinformatikai adatbázis - hozzáértő kezek segítségével - könnyedén tudja kezelni.

1. ábra. Összetett tűzoltói feladatok.[6]

A digitális térképek mellett szól az a tény is, hogy a megjelenített térkép részletek tetszőlegesen kicsinyíthetők, illetve nagyíthatók (méretaránya rugalmasan változtatható). Ezzel egyrészt a térkép „részletgazdagsága” növelhető, másrészt, az előbbiekben már említett térképi információ túlzsúfoltsága is kiküszöbölhető. Természetesen a digitális térképek is tetszőlegesen elforgathatók (tájolhatók). A digitális térképek mérethűen támogatják a távolsági méréseket méretaránytól függetlenül, valamint bármely kijelölt helyhez GPS koordinátákat is lehet rendelni. A már említett, térképhez köthető adatok és maga a térkép közötti kapcsolatot szintén a GPS koordináták teremtik meg. (Az adatbázis számos elemeinek egyik a jellemző tulajdonsága a hozzárendelt földrajzi koordináta).

A digitális térképet és a hozzá tartozó adatbázist maga a szoftver teszi láthatóvá. Az erőssége mindenképpen az, hogy dinamikus információkat (időben gyorsan változókat) lehet vele ábrázolni. Az árvizek, esetleg a tavaszi hóolvadást követően a nyílt területen keletkezett bozóttüzek esetében kimondottan igaz, hogy a megközelítési útvonalakon változnak a viszonyok (pl. elönti az utat az áradás) és ilyen jellegű információk hiányában értékes percek, órák mehetnek veszendőbe kerülőút kereséssel, nem is beszélve a személyi állomány és a technikai eszközök szintén veszélybe kerülhetnek [7].

A fentieket összegezve megállapítható, hogy a prototípus szoftver a digitális térképek és adatbázisok összekapcsolására és megjelenítésére vállalkozik.

A PLATFORM HARDVER KÖVETELMÉNYEI

A szoftver alapötlete a tűzoltóságok által korábban használt riasztási és segítségnyújtási terv (RST), ma annak továbbfejlesztett változata, a műveletirányítási terv dokumentumainak alkalmazásából származtatható.

A szoftver *Embarcadero Delphi* környezetben készült *WINDOWS X86 és X64* platformon, de az alkalmazása *WINDOWS XP-7* környezetben is alkalmas. A szoftver illetve a naprakész adatbázisok rendelkezésre állásához az internet kapcsolat elengedhetetlen. A fentiekben felsorolt adatok távoli adatbázisokban, ún. *felhőben* lehetnek tárolva. *Cloud computing*-ról, avagy a felhő alapú számítástechnikáról akkor beszélünk, amikor a számítási erőforrások, hálózati sávszélesség, tárolási kapacitás és különböző szoftverek szolgáltatásként jelennek meg, amely szolgáltatás távolról, az interneten keresztül vehető igénybe. Ennek előnyei közé sorolható, hogy a futtató környezet minden tűzoltóságon rendelkezésre áll. A híradó ügyeletek fel vannak szerelve olyan PC-kkel, amelyek képesek eleget tenni a szoftver biztonságos futtatásához szükséges hardver követelményeinek.

Bár a szoftver és a különféle adatbázisok szoros konzisztens kapcsolatban vannak egymással, mégis, az adatbázisok nem feltétlenül kapcsolódnak a futtató számítógéphez. Alaphelyzetben a számítógépek lokális (helyi) adatbázisaiban rendelkezésre állnak alapvető, időben csak korlátozottan, vagy kismértékben változó információk. Amennyiben az adatbázisok bármelyikében változás keletkezik, akkor egy szinkronizálódási folyamat indul el, ami az adat tartalmak egységesítésére irányul.

Nem nehéz belátni, hogy az adatok minősége alapvetően befolyásolhatja a beavatkozás sikerét. A kutatásaim során megállapítást nyert, hogy az internet kapcsolatra képesek mobil eszközök száma és az alkalmazhatóságuk minősége továbbra is növekszik. Ezek megfelelő program adaptációval szinte valamennyi esetben képesek megjeleníteni mindazon információkat, amelyek elősegíthetik a hatékonyabb beavatkozást. Az ilyen eszközök potenciálisan képesek továbbá arra is, hogy egyfajta *input platformként* információt szolgáltassanak az olyan tevékenységekhez, amelyek terepi adatgyűjtéshez kötöttek (pl. katasztrófát megelőző tevékenységek, illetve a károk gyors felmérése). Mivel az eszközök döntően rendelkeznek GPS vevővel is, a digitális fényképezőgéppel történő adatrögzítés korrekt helymeghatározása, pontos dokumentálása is biztosítva van.

A projekt során készült prototípus alkalmas a tűzoltósági vízszerzési helyek, a tűzcsapok pontos helyeinek felmérésére és adatbázisban történő rögzítésére is. A mai gyakorlat alapján a tűzcsapok nyilvántartása a házszámok alapján történik, azok esetleges hiánya miatt nem voltak pontosan behatárolhatók. Ez akár jelentős késést, erőforrás túlzott lekötését is jelenthette egy-egy tűzoltói beavatkozás során.

2. ábra. Tűzcsapok helyének pontos meghatározása GPS készülékkel

A fenti platformok előnye a mobilitás, de hátrányként jelentkezhet az adatok elérhetőségének gyorsasága és a saját adatbázis hiányossága. A mobil eszközökre telepített alkalmazások elsősorban adatbeviteli célokat szolgálnak, a lekérdezés az *output* funkciók (térkép - adatbázis megjelenítés) jelenleg kizárólag online internet kapcsolaton keresztül, ún. WEB böngészőben érhetők el. Az input adatok a felmérés során ún. *ideiglenes állományban* foglalnak helyet, melyek a felhasználói beavatkozásra frissítik a felhőben lévő adatbázisokat.

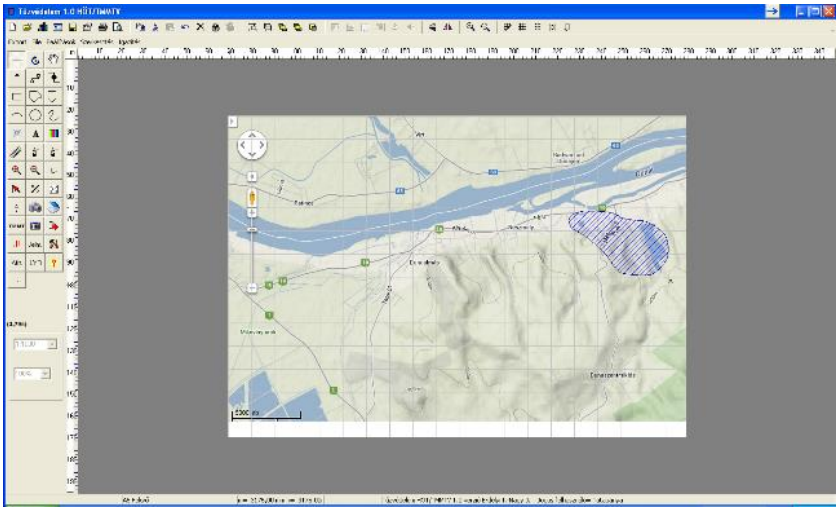
3. ábra. GPS segítségével felmért települési tűzcsap hálózat grafikus megjelenítéssel

A mobil eszközöknek fontos szerep juthat a vonulások közben is. A helyismerettel nem rendelkező, de segítségnyújtásra érkező szervezetek és egységek ugyan tisztában vannak a saját eszközeik paramétereivel, de valós idejű információ hiányában nem tudhatják a körülmények alakulását. Ilyen lehet, pl. amikor egy útszakaszon ideiglenes akadály lép fel, ami esetlegesen hátráltatja, vagy akár meg is akadályozza (veszélyezteti) a beavatkozás helyszínére történő odajutást (súly és méretkorlátozások, árvíz esetén elöntött útszakasz, stb.). A vonuló eszközök fedélzetére telepített eszközök képesek lehetnek megjeleníteni az útvonalon előforduló, és a vonulást, a későbbiekben pedig a beavatkozást érintő körülményeket.

A PROGRAMOT ALKOTÓ ÖSSZETEVŐK

A programot alkotó és az alkalmazást lehetővé tevő összetevők a következőkből elemekből épül fel:

- A futató környezet: az operációs rendszer, amely lehet WindowsXP és Windows 7 is;
- Szerkesztő szoftver: a digitális térképekhez elem információk felvitele, historikus adatok felvitele, stb.; itt van lehetőség a mobil eszközökön gyűjtött elem adatok importálására;



4. ábra. A minta program szerkesztő oldala Komárom – Esztergom Megye részletével

- A főprogram: feladata a digitális térképek és az azokhoz kapcsolódó (feltöltött) elemek megjelenítése. Az áttekintő térképen a térkép bármely pontjához lehetőség van egy jelölés (pl. zászló) letűzésére, majd a menü *szerkesztés* pontjának *eleminformáció* alpontját kiválasztva a *szerkesztő* alprogram jelenik meg. A főprogram képernyői (térképszelvények) tetszőlegesen forgathatók (tájolhatók), míg a szerkesztő program esetében ez kötött, az északi irányt a lap teteje jelzi. A szerkesztő program lehetővé teszi a távolsági méréseket.

Megjelenítéskor az egyes elemek adatai a helyi adatbázis-kezelőből kerülnek lekérdezésre a felhasználó által meghatározott szempontok szerint. A felhasználó a „kérését” párbeszédablakon keresztül állítja be, amely meghatározza a korábban említett szűrőfeltételeket is.

AZ ADATBÁZISOK SZERKEZETE

A (tér)informatikai rendszerek legnagyobb értéke az adat. A rendszer magja a központi adattároló; minden alrendszer itt tárolja a saját tulajdonú adatait. Az adatokon történő művelet végzés érdekében a szükséges adatokat a kliensek elkérik a szervertől. A cél az, hogy minden adat egyszer legyen tárolva. Az adatokhoz való hozzáférést megfelelő módon, a tűzoltóság, katasztrófavédelem belső utasításaihoz illesztve szabályozni is kell. Nagyon fontos az is, hogy az adatbázis állapota naprakész legyen, ami igen gyakran széleskörű és folyamatos adatgyűjtést jelent.

Az adattár az adatokon kívül különböző egyéb funkciókat is biztosít a felhasználók számára. Ezek az ún. *megtekintés* és a *szerkesztés*. Mindkét funkció erősen szabályozott módon érhető el, azaz egy felhasználó csak azon adatokat láthatja, illetve azokat a műveletek hajthatja végre, amelyekhez a szükséges engedélyekkel rendelkezik.

A központilag tárolt, osztott adatbázisnak köszönhető, hogy a munkacsoport tagjai egy közös adathalmazon párhuzamosan is végezhetnek műveleteket úgy, hogy egymás egyidejű tevékenységét eközben nem zavarják.

- A helyi adatbázis-kezelő egy standard MYSQL adatbázis szerverrel kiegészítve egy olyan komponens, ami a távoli adatbázissal szinkronizáltan képes a beavatkozói kéréseket kiszolgálni. Az adatbázis a feltételek kiválasztása és lekérése után az elemek (rekordok) kívánt részhalmazát jeleníti meg a térképen, mint térképobjektumot.
- A lekérdezések a *feltétel* mellett található *checkbox* kiválasztásával aktiválhatóak, vagy kikapcsolhatók.
- Az egyes elemek térképen elfoglalt pozíciója a rekordban tárolt GPS koordináták formájában található meg. 1 rekord 1 db térkép objektumot jelöl. A rekord szerkezetét az un. adatmezők alkotják.

Mezőnév	Formátuma	Leírás	Minta
ELEM_X_GPS	XX.XXXXX	Az elem X koordinátája	41.40338,
ELEM_Y_GPS	XX.XXXXX	Az elem Y koordinátája	2.17403
RAJZJEL	BLOB Bináris mező	A rajz jel maga ami megjelenik a térképen	
CSOPORT	A szűrőfeltétel alapja	Az elem csoportosítására szolgáló bejegyzés	G_VIZVE (vízvételi helyek)
TIPUSA			
LAST_MOD JELLEG	ss.min.hh:dd-mm-yyyy	Az utolsó módosítás jellege módosítás ideje	21.10.13:09-15-2013
DATETIME	ss.min.hh:dd-mm-yyyy	Adatbázisba kerülés ideje	10.13.12:17-06-2013
USER	XXXXXXX	A bekerulés módja,felhasználónév vagy eszköz azonosító	RAMIL

5. ábra. Példa a minta program rekord szerkezetének adatmezőire

A térképeken megjeleníthető különböző jelek (piktogramok) csoportosítása azok tartalmi megnevezésével a következők lehetnek:

6. ábra. A térképen megjeleníthető jelek csoportosítása

Az ábrák a csoportosítás jellegére utalnak. Az alábbiakban az egyezményes rajzjelek főcsoportjai kerülnek meghatározásra:

- Híd, átkelőhely jelölések,
- Vízi és légijárművek jelölései,
- Beépített oltóberendezések,
- Fák, erdők, jellegzetes cserjés, bozótos jelölése,
- Irányító szervek,
- Hírközlő berendezések,
- Közművek,
- Járművek, munkagépek jelölése,
- Hordozható tűzoltó készülékek jelölése,
- A tűz keletkezési helyének, a bevetett sugaraknak a jelölése,
- Tűzoltószerek, felszerelések jelölése,
- Különböző építészeti jelek,
- Vízforrások, vízellátási szerelvények, csővezetékek.

A különböző adatbázisok elérésének módja a jogosult felhasználók számára teljesen transzparens. Az adatbázisok (helyi és távoli) szinkronizáltságát a program a képernyőn körbefutó keret színével jelzi. Amennyiben a lokális és a távoli adatok konzisztensek, azaz nincs eltérés, a keret nem látható. Amennyiben a keret sárga színű, az azt jelzi, hogy a helyi adatok változtak és a távoli adatbázis frissítése folyamatban van. Ez leginkább az adatfelvitel során fordulhat elő.

A szürke színű keret a távoli adatbázis nem elérhetőségét jelzi. Ez előfordulhat mind az áttekintés (lekérdezés), mind a felvitel során. A szoftver az előre beállított időközönként próbálja a kapcsolatot felvenni a távoli adatbázissal. Alapértelmezett értéke 60 másodperc. A szinkronizálás kezdeményezhető a felhasználói felületről is.

A piros színű keret a meglévő kapcsolat esetén adatütközésre figyelmeztet. Ez abban az esetben fordulhat elő, ha azonos jelölésű azonosítóhoz más típusú elem hozzárendelése történt. Ez lehet nem felhasználói hiba is.

FELHASZNÁLÓI JÁRTASSÁGOK SZÜKSÉGESSÉGE

A beavatkozások során az információ az irányító parancsnoknál összpontosul. Amennyiben a tűzoltás, beavatkozás megköveteli (pl. nagy kiterjedésű tüzek, árvízi beavatkozások, elhúzódó raktár tüzek), olyan irányítási módban történik a felszámolás, ahol a vezetés legalább részben megoszlik. Ilyenkor az adatbázis frissítésére a vezetési törzsben bizonyára akadhat erőforrás, míg kisebb beavatkozásoknál az adatbázis frissítése a segítség szükségtelensége miatt az elsődleges feladatok ellátása után is ráérhet. A fenti feladatokat a helyszínen lévő és jogosultsággal bíró, az aktív tevékenységbe nem bevont, alapvető informatikai ismeretekkel rendelkező tűzoltó teheti meg. Ez utóbbi kritérium ma már egyre inkább teljesül, így a jövőben az ilyen jellegű korlátozó tényező egyre inkább mérséklődik.

A főprogram használatakor természetesen elvárt, hogy a használók ismerjék a különböző térképjeleket, valamint a beavatkozáshoz kapcsolódó egyezményes jeleket is.

Interaktív szerkesztő üzemmódban a felhasználónak alapvető számítógép használati jártassággal kell rendelkeznie a térkép jelölések, valamint a rajzjelek ismerete területén. A megjelenítendő elemek és adatok sokféleségének felvitele miatt hozzáférés szükséges egyéb, pl. polgári védelmi adatbázisokhoz is. Az egyéb programok (tűzcsapok felvitele mobil alkalmazással) a kezelő részéről némi betanulás után rutinszerűen végezhető.

KAPCSOLAT MÁS RENDSZEREKKEL

A szoftver prototípusként működik, ami azt is jelenti, hogy nincs felkészítve más rendszerekből, adatbázisokból történő információk, adatok automatizált fogadására. Továbbá nehezíti a kapcsolódást a meglévő adatforrások (nem feltétlenül digitális adatok és számítógépes adatbázisok) sokfélesége is, az egységes platform hiánya.

A szoftver által szolgáltatott digitális térkép ellenben alapja lehet az új műveletirányítási tervek térképvázlatainak (ami a vonulás útvonalára vonatkozik). Egy egységes formátumú bevetés irányítási adatbázis biztosíthatna olyan jellegű információkat is, amelyek a katasztrófa helyzetekben a kritikus infrastruktúrák jelenlétére is megfelelő módon ráirányítja a figyelmet. Ezáltal lehetővé válna a beavatkozási tervek hozzárendelése a digitális térképek elemihez. (Az adatbázis elemek lehetnek akár maguk a veszélyeztetett létesítmények is.) Amíg nem létezik egységes platform a szoftver un. interfészeken alkalmas arra, hogy más rendszerekből adatokat tudjon átvenni, feldolgozni, illetve megjeleníteni. Az interfész feladata az, hogy az import adatokat konvertálja a szoftver által használt adat formátumába.

A bemutató szoftvernek jelenleg nem célja, hogy más rendszereknek input adatokat szolgáltasson, viszont a digitális térképszelvényekről, a térképen megjelenített extra információról szabványos képformátumú (bmp., gif., jpg., stb.) fájlokat lehet generálni, amelyek potenciálisan alkalmasak más rendszerekhez való kapcsolódással azt biztosítani.

A PROGRAM TOVÁBBFEJLESZTÉSÉNEK LEHETŐSÉGEI

A kialakított program alapvetően már meglévő rendszerekhez illeszthetően lett megalkotva. Azonban számos olyan lehetőség is rendelkezésre áll, amely a jövőben új lehetőségeket nyithat. Ilyen a távérzékelésen alapuló információszerzés. A körülményektől függően erre lehetőség van nagy kiterjedésű erdőtüzek, de akár árvizek monitorozásánál is.

Távérzékelésnek azokat a vizsgálati módszereket nevezzük, amelyekkel a közelünkben vagy tágabb környezetünkben található tárgyakról vagy jelenségekről úgy gyűjtünk adatokat, hogy az adatgyűjtő (általában szenzornak nevezett) berendezés nincs közvetlen kapcsolatban a vizsgált tárggyal vagy jelenséggel. A távérzékelésnek több formáját is ismerjük: fix, földi berendezéshez, általában toronyhoz rögzített kamerás, valamint repülőgépre installált légi-, valamint műholdas, vagy más néven űr-távérzékelés.

Míg a légi fényképezés rendszerint csak a földfelszín által visszavert illetve a felszín saját sugárzását felhasználva készíti a felvételeket (ez az úgy nevezett passzív letapogatás), addig sok távérzékelő űreszköz saját maga által kibocsátott sugárzás segítségével is képes a földfelszín letapogatására. Ezt a módszert aktív letapogatásnak, az eredményül kapott képeket radar képeknek nevezik. A radaros módszereknek az a nagy előnye, hogy olyan hullámhosszakat használnak, melyeket a felhőzet kevéssé nyel el, e mellett függetlenek a felszín megvilágítottságától, azaz a felvételek minősége nem függ az időjárástól és a napszaktól.

A világ számos területén alkalmazzák a katasztrófavédelemben a távérzékelt adatokat, mivel azok rendszeresen és gyorsan beszerezhetőek, nagy területet lefednek, és olyan információt szolgáltatnak, amelyet a terepen, még közvetlenül a helyszínen sem tudnánk beszerezni. A légi- és űrfelvételek használatával pontosan lehatárolható egy – egy árvíz által elöntött terület, vagy szennyezés kiterjedése. Ráadásul a viszonylag könnyen és gyorsan ismételhető felvételekkel a terjedés sebessége, illetve annak várható iránya is jól meghatározható. Egy modern, katasztrófavédelmet támogató rendszerből kihagyhatatlanok a különböző távérzékelt adatok. Ezen adatok meglétének köszönhetően a katasztrófavédelmi szervek előre tudnak dolgozni és több idő marad a mentési feladatokra, mivel a digitális térképek segítségével fel tudják mérni, hogy a védelmi létesítmények hol lesznek kitéve a legnagyobb terhelésnek.

A távérzékelés nem csak megkönnyíti a katasztrófavédelem feladatát, hanem adott esetben meg akadályozhatja a katasztrófa bekövetkezését is. A védekezés és elhárítás egyik sarkalatos kérdése lehet annak költségessége. A modern pilóta nélküli repülőeszközök alkalmasak lehetnek mindazon feladatokra is, melyeket korábban csak a fenti bonyolult, sokszor igen költséges eszközpark segítségével lehetett elvégezni. A pilóta nélküli repülőgépek katasztrófavédelmi alkalmazásával kapcsolatban komoly hazai eredményekkel is rendelkezünk, így azok jövőbeni felhasználásával a program továbbfejlesztésénél a költséghatékony távérzékelés módszereként, mint input adat szolgáltató mindenképpen számolhatunk [8].

ÖSSZEGZÉS

A tűzoltási, műszaki mentési és katasztrófa-elhárítási tevékenységek nagyon összetett és bonyolult folyamatként jelenhetnek meg, amelyek felszámolásának előre tervezése, a célirányos felkészülés csak nagyon korlátozott módon valósítható meg. Ezért a helyszínen történő improvizatív döntéshozatal számos esetben domináns szerepet kap, amely szakmai szempontból nem mindig a legjobb megoldást eredményezi. A fenti problémák csökkentése, illetve a döntések hatékonyságának növelése érdekében a kutatás során célkitűzésként fogalmazódott meg egy számítógépes döntéstámogató program megalkotása.

A program megalkotásával eddig általánosan még nem alkalmazott térinformatikai elemek kerültek kidolgozásra, amelyek a beavatkozó tűzoltók tevékenységét bizonyosan elősegíthetik, így gyorsabb döntéshozatalt, pontosabb információ alapján történő helyzetmegítélést, összességében hatékonyabb beavatkozást tesz lehetővé. Ilyen, talán a legegyszerűbb megoldás a terület tűzcsap hálózatának GPS készülékkel történő felmérése és digitális térképen történő megjelenítése. További elemek, mint a különböző veszélyt jelző, vagy információt adó piktogramok, néhány további, jellemzően beavatkozást segítő elem, valamint az adatok bevitelére alkalmas interaktív felület lett kialakítva. A fejlesztés alkalmas arra, hogy demonstrálja a számítógépes döntéstámogató program előnyeit, speciálisan a tűzoltó, műszaki mentési, valamint katasztrófa-elhárítási feladatok döntéshozói szintjét a középpontba állítva. A cikkben továbbá iránymutatás történt, amely alapján a program továbbfejlesztése folytatható, külön kiemelve a kiterjesztés lehetőségét, valamint a távérzékelés alkalmazásának csatolását.

A cikk a Nemzeti Közszolgálati Egyetem, TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások” című project keretében elért eredmények alapján készült.

Results of this article are based on the research author did in the project called TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Research for Critical Infrastructure Protection”, at the National University of Public Service, Budapest, Hungary

Felhasznált irodalom

[1] Restás, Á.: A tűzoltásvezető döntései elméleti szempontból. Védelem, Katasztrófavédelmi Szemle, 3/2013, p. 5-9.

[2] Restás, Á.: A tűzoltásvezető döntéseit elősegítő mechanizmusok. Védelem, Katasztrófavédelmi Szemle, 5/2013, p. 11-14.

[3] Miskey, Tamás: Az emberi tényezők és egy új kiürítéstámogató rendszer bemutatása. In: Hadmérnök, 2/2009, p. 57.66.

[4] Komjáthy, L.: Hungarian – Slovak cross border firefighting cooperation; Annual Conference: Fire Related Research and Developments (RE13), Moreton-in-Marsh, Egyesült Királyság, 2013. november 14.

[5] Noskó, Zs.: Döntéstámogatás és vezetésirányítás a tűzoltók munkájában; Védelem, Katasztrófavédelmi Szemle, 3/2013, p. 5-9.

[6] http://tuzoltosag.info/hirkep/20131031_tuz_egy_gyomaendrodi_raklapuzemben_1383238168.jpg

[7] Restás, Á.: A pilóta nélküli repülőgépek (UAV) erdőtüzeknél történő alkalmazásának strukturált felosztása; Repüléstudományi közlemények, 2012. 2. szám, p. 622-633.

[8] Dudás, Z., Restás, Á.: Some Special Features of the Use of Unmanned Aerial Systems for Disaster Management Purposes, ICUAS 2013, Atlanta, Egyesült Államok, 2013. május 28-31.

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. január

Morvai Cintia
cintia.morvai@freemail.hu

TORONYHÁZAK MEGELŐZŐ TŰZVÉDELME - ESETTANULMÁNY

Absztrakt

Az olvasóval először a toronyház építésekor hatályos jogszabályokat ismertetem, ebből a részből kiderül. hogy mennyit fejlődtek, változtak módosultak a tűzvédelmi előírások. A toronyház aktív és passzív tűzvédelmét külön fejtettem ki, ezzel az volt a célom, hogy az olvasó még részletesebb képet kapjon a megelőző tűzvédelemről. Feltártam a toronyház létesítésekor betartandó követelmény-rendszert és összevetettem a jelenlegi követelményrendszerrel. A cikkemben ismertetem továbbá a toronyház építésének sajátosságait, hiányosságait, tervezéskor jelentkezett problémákat és végül a hatóságok engedélyezési tapasztalatait.

Firstly I present to the reader the regulations applied during the construction of the selected high-rise building. We can have a picture from this section how much have improved, changed and modified the fire prevention regulations. I explained in separate section the active and the passive fire protection system of the tower house. I explored the requirements at the time when the tower house was constructed, and compared to the current system requirements. In my article I will introduce the specialty of the high-rise building's construction, shortcomings, problems that occurred during the planning process and finally I will deal with the licensing experiences of the authorities.

Kulcsszavak: *toronyház, magas épület, aktív tűzvédelem, passzív tűzvédelem ~ tower block, high building, active fire protection, passive fire protection*

BEVEZETÉS

Az urbanizáció hatására Magyarországon egyre több középmagas és magas épület épült. Számos iparilag fejlett ország modern építészetére jellemző a részben indokolt magas építkezés. Különösen fontos, de kiemelt figyelmet érdemlő probléma a tűzesetek megelőzése és a bekövetkezett tüzek esetén az emberek és anyagi javak hatékony védelme.

A hatvanas-hetvenes években Magyarországon három "monumentális" lakóház épült, Szolnokon, Pécsett és Gyöngyösön. A gyöngyösi toronyház állapota messze túlmutat a másik két épületen, a pécsi lakóházban 1989-ben [1] három hónap alatt teljesen ki kellett költöztetni a lakókat, mivel az épület külső vasszerkezetének korrodálása olyan mértékűvé vált, hogy már veszélyeztette az épület állékonyságát, ezáltal pedig fenyegetést jelentett az emberi élet számára is. A szolnoki ház 5 évvel később a gyöngyösi beruházási tapasztalatok alapján épült, a helyi önkormányzat anyagi gondjai miatt nem tudta megfelelően elvégeztetni az állagmegóvási munkálatokat, így sokkal rosszabb műszaki állapotban van.

ÉPÍTÉSKORI TŰZVÉDELMI SZABÁLYOZÁS ÁTTKITEKINTÉSE

Mivel a toronyház a 70-es években épült, ebből adódóan az épület az akkori követelményeknek megfelelően épült. Ez bizonyos mértékben lefedi a jelenleg hatályos jogszabályi előírásokat, azonban a tűzvédelmi jogszabályok jelentős változása miatt komoly eltérések vannak az akkori és a jelenleg hatályos jogszabályi előírások között. Az 5/1965. számú BM TOP ágazati szabvány a középmagas és magas épületek tűzrendészeti előírásáról szól (továbbiakban: ágazati szabvány), amelyet alkalmaztak a ház tervezésekor és építésénél.

Az ágazati szabványban megtalálhatóak a külföldi tapasztalatok figyelembevételével azok a tűzvédelmi követelmények, amelyeket fontos élet- és vagyonvédelmi szempontok megfontolása után, tervezéskor, építéskor és üzemeltetéskor figyelembe kell venni.

Tűzoltási, felvonulási terület

Az ágazati szabvány alapján az épület megközelítését (tűzoltási felvonulási utat) legalább az épület egyik oldalán kell biztosítani, úgy hogy a megközelítési út legalább két nyomvonal szélességű legyen. A szabvány továbbá kimondja, hogy az épület szabad határoló falától mért legkisebb úttengely távolság 8 m lehet. Az utat legalább 4,2 m szélességűre kell megépíteni. Szélesebb út esetén az útpadka (járda, fellépő) és az épület szabad határoló fala közti távolság legfeljebb 6 m lehet. [2]

Tűzszakasz

Az ágazati szabványban a tűzszakaszt a jelenleg érvényben lévő jogszabálytól teljesen eltérően értelmezték. A tűzszakasz területe alatt nem a tűzszakaszhoz tartozó helyiségek összesített nettó területét értették, hanem a tűzszakaszhoz tartozó legnagyobb szint területét, függetlenül a tűzszakaszhoz tartozó szintek számától, valamint nem számították bele a tűzszakasz területébe a folyosókat. [2] A helyszíni vizsgálatok során illetve a levéltárból kikért dokumentációkat megvizsgáltam és megállapítottam, hogy az egész épület tűzszakasznak minősül.

Hő- és füstelvezetés

A létesítéskor hatályos ágazati szabvány előírta, hogy minden tűzszakasz legfelső lépcsőházának legfelső részén füstelvezető nyílást kell kiképezni. A nyílás nagysága pedig a lépcsőház alapterületének 5 %-a, de legalább 0,5 m^2 legyen. Továbbá a füstelvezető nyílás nyithatóságát üzembiztos szerkezettel kell biztosítani a földszintről. Későbbi szabályozásnak megfelelően a hő és füstelvezető méretezését úgy kellett kialakítani, hogy a hatásos

nyílásfelülete az alapterület 5 %-a legyen, de minimum 1 m^2, függőleges elhelyezésnél pedig plusz 50 %-kal növelt felületet kell létesíteni.

A hő- és füstelvezetés azért lenne nagyon fontos az ilyen magas házaknál, mivel az ilyen épületek lépcsőházai egy légteret alkotnak a közlekedő folyosókkal, így bármelyik lakásban keletkezett tűz égéstermékei bejuthatnak a lépcsőházba, meggátolva az egyetlen menekülési útvonal biztonságos használatát. Ha létezik ilyen berendezés, akkor is előfordul, hogy a megrongálásoknak köszönhetően nem működőképes, vagy nem elégséges hatékonyságú. [2]

Épületgépészet

A szellőző berendezéseket az ágazati szabvány előírásainak betartása miatt nem éghető anyagból kellett kivitelezni. A mechanikus szellőző berendezések csatornáit szintenként elzárhatóvá kellett tenni. Az elzáró szerkezeteket csatornán belül és azon kívül tűzesetre egyaránt automatikusan záródó módon kellett kialakítani. Megállapítható, hogy Magyarországon már 1965-től kötelező volt a középmagas és magas épületekben a szellőző vezetékek tűzvédelmi szakaszolása tűzhatásra automatikusan záródó szerkezetekkel nemcsak a tűzszakasz határokon, de minden szint között. Az előírást azonban nem mindig tartották be a középmagas paneles lakóépületek létesítése idején.

Az épületgépészeti aknákra az alábbiak jellemzőek:

- alumíniumból készült légtechnikai vezetékek,
- aknák a födémek vonalában nem kerültek megszakításra, szakaszolásra, tűzgátló lezárására,
- a konyhai szagelszívó vezetékben lerakódott kiszáradt olaj-, és zsírmaradékok éghető anyagként szintén hozzájárulhatnak a tűz épületszintek közötti átterjedéséhez,
- a légtechnikai vezetékek helyiségekbe történő becsatlakozásainál tűzgátló elzáró szerkezetet nem tartalmaznak.

Az ágazati szabvány alkotója tehát tisztában volt a középmagas és magas épületek esetén a gépészeti aknák tűzterjedésében játszott szerepével. Ennek ellenére a paneles technológiával létesült épületek esetén tűzterjedést gátló elzáró-szerkezetek a légtechnikai rendszerekben nincsenek. [2]

Elektromos berendezések

A lakások villamosvezetékei, az akkori igényeket elégítették ki, a mai igények ezeket természetesen már meghaladják. Az 1960-as és 70-es években általánosan használatos volt az alumínium elektromos vezeték. Jelenleg réz vezetékeket alkalmaznak általánosságban, ezért a lakásokban az elektromos hálózatok felújításánál több esetben fordult elő a réz és alumínium vezetékek szabálytalan és tűzveszélyes összekötése (sodrat-kötés).

Minden épületnek szüksége van megfelelő nagyságú villamos betáplálásra. A toronyház kiemelkedő fogyasztó Gyöngyös város villamos hálózatában, ezért ennek megfelelően a toronyház villamos ellátása kettős betáplálású, az épülethez tartozó transzformátor házban két nagyfeszültségű transzformátor biztosítja az elektromos ellátást. Ennek előnye, hogy az elektromos hálózat duplikált, azaz ha az egyik transzformátor nem működik különböző okok miatt, attól függetlenül a másik működik és a fontos berendezések, mint például a liftek is megőrzik működőképességüket.

Villámvédelem

A magas épületeknek már a toronyház építésekor is előírása volt, hogy villámvédelemmel kell ellátni. Az előírásokat betartották, azonban jellemzően a villámvédelmi rendszerekre adatátviteli vezetékeket rögzítettek, például kültéri antennákat.

Tűz esetén a kéményhatás kialakul, ami jelentősen megnöveli a tűzterjedés sebességét, ezen kívül a tűzfészektől távoli helyen is okozhat további tüzet. A menekülési lehetőségek is

korlátozottak már egy középmagas épületben, ebből adódóan ilyen esetben, a gyöngyösi toronyházban még kevesebb menekülési útvonal állna rendelkezésre probléma esetén.

AZ ÉPÜLET PASSZÍV TŰZVÉDELME

A passzív tűzvédelem azt jelenti, hogy tűzvédelmi szigeteléseket készítenek, amelyek megakadályozzák a tűz, a füst és a hő átterjedését is az épületrészekből a másik szerkezetbe. Megfelelő állékonyságot kell biztosítani az ipari berendezéseknek, azaz a tartószerkezeteknek.

A toronyház épületszerkezete

A falai monolit vasbeton falak, a födém pedig monolit vb. lemezekből készült. A válaszfalai 6 és 10 cm-es vastag égetett agyag téglából lettek kiépítve. A Gyöngyösi toronyház ajtói, a lakáson belül fából fémtokkal bevonva készültek, de a lakáson kívül önbecsukós fémajtókat helyeztek el. Az ablakok is faszerkezetűek voltak. A padlóburkolatok a lakásokban PVC és önkioltó műanyag szőnyeg, a folyosókon és a lépcsőkön mettlachi és műkő volt.

Építési technológia

A tervezési munkálatokat talajmechanikai feltárás előzte meg, ami a 70-es évek legmodernebb eszközeivel történt. A feltárások megállapították, hogy fél méter humuszos agyagréteg után 2,4 méter mélységig kövér agyag található, majd ezt követi a pleisztocén korban nyugalomba került, elég nagy teherbírással bíró andezit-görgeteg helyezkedik el, ezután levantei rétegek következnek földszíntől mért 16 méterig és ezt követi a szerves üledék és sovány agyag keveréke 22 méterig. Mivel a felszín közelében megállapították, hogy az andezit-görgeteg teherbírása elegendő a toronyház alapozására, így nem is volt szükség mély alap készítésére. A mérések szerint az épület várható süllyedése 10 centiméter, ami már az épület építésénél lejátszódik, ez egyébként a természetes konszolidáció következménye.

Az épület 80 centiméter vastag vasbetonlemez 60 centiméter vastag homokos kavics ágyazaton és 15 centiméter vastag aljzatbetonon nyugszik, ez a doboz-szerkezetnek is a részét képezi.

A toronyház csúszózsaluzással készült, Magyarországon már az 1920-as évek elején ismerték ezt a technikát és sok épület és siló épült abban az időben ilyen technikával. Másrészt nem elfelejtendő, hogy a 60-as 70-es években sok lakóépületet építettek csúszózsaluzással, ezek közé sorolhatjuk a Gyöngyösi toronyházat is.

1. ábra. A csúszózsalus betonozást befejezték
Készítette: Szendrővári György [3]

Épületgépészet

A toronyház elkészítésekor a fűtést távfűtéssel, egycsöves meleg-vizes konvektorokkal oldották meg. 1995-ben átadtak két új kazánt. A kazán működése ötszörös biztonsági tényezővel rendelkezik, azaz megtalálható öt reteszfeltétel. Ezek például: a vízhiánykapcsoló, ha nincs gáz és víz, akkor a kazán fűtése kikapcsol, használati meleg-vízhez használati vízhiány-kapcsoló és a gáznyomáscsökkentő (reduktor).

2. ábra. A toronyház jelenlegi kazántelepe

Amennyiben a lakossági vízhálózatban ellátási problémák vannak, abban az esetben az épület tetején egy 100 m^3 –es tartály biztosítja az épület vízellátását, ez a vízmennyiség a társasház mintegy 400 fős lakosságának körülbelül 2,5 napig lenne elegendő.

3. ábra. Vízhiánykapcsoló

3. sz. fotó:

A hármas számú fotón a vízhiánykapcsolót láthatjuk, a képen is jól látszik, hogy 0,8 és 1 bar között van a nyomás, a kazán letilt, amennyiben a kritikus érték alá csökken a víznyomás.

A csatornázást úgy alakították ki, hogy van belső elvezetésű szenny- és csapadékcsatorna. Az épület lakóinak a vízellátását a városi vízből oldják meg hidegvíz szivattyú segítségével, ami 350 liter/perc teljesítményű

3. AZ ÉPÜLET AKTÍV TŰZVÉDELME

A teljes körű tűzvédelemhez az épületszerkezeteken kívül beletartoznak azok a szerelvények, berendezések és eszközök melyek az épület aktív tűzvédelmét (tűzjelzés, tűzoltás) látják el. Ide tartoznak a tűzjelző berendezések, a tüzivíz hálózat, tűzoltó készülékek valamint a hő- és füstelvezető berendezések.

Tűzjelző berendezések

Tüzek esetében legfontosabb szempont a gyors észlelés és jelzés, ezért elengedhetetlen, hogy egy ilyen volumenű épület ne legyen felszerelve tűzjelző berendezéssel. A tűzjelző berendezés – megfelelő karbantartás mellett – jelentősen növeli a tűz időben történő észlelhetőségének és a lakók riasztásának hatékonyságát.

Az épületben szintenként található a fali csapoktól olyan automatikus jelzőberendezés, amely a portán található központban azonnal jelez, és azt észleli a 24 órás ügyeletet ellátó személy számára. Az akkori követelményeknek megfelelően egy MMG központ került kiépítésre, mely a kor színvonalát hűen tükrözte, illetve a mai napig megtörténik a karbantartása és megőrizte működőképességét.

A központ analóg módon jelzi, melyik emeleten keletkezett a tűz, a riasztást hangjelzés is kíséri. Előrelépést jelentett, hogy kiépítésre került a teljesen automatikus Telealarm tűzjelző rendszer, amihez hozzátartozik, hogy szintenként a szemétledobókban és az elektromos helyiségekbe ionizációs füstérzékelők vannak elhelyezve. Az ionizációs füstérzékelők olyan érzékelők melyekben egy alacsony radioaktivitású anyag által kibocsátott sugárzás intenzitását alakítja át az érzékelő elektromos jellé, ha az érzékelőbe füst kerül a jel megváltozik és riaszt a központ. Az ionizációs érzékelőket a forgalomból már kivonták, csak karbantartásuk lehetséges. Megfelelő karbantartás mellett ezek az érzékelők stabilan működnek és jó érzékenységi mutatókkal rendelkeznek, tehát a tüzet korai szakaszában képesek érzékelni.

4. ábra. MGM típusú tűzjelző hálózat

Hő és füstelvezetés

A hő- és füstelvezetők hatékony működése nagyon fontos, mivel az épületek lépcsőházainak nagy része egy légteret alkot a közlekedő folyosókkal, egy tűz során felszabaduló égéstermékek bejutnak a lépcsőházba és meggátolják az egyetlen menekülési útvonal biztonságos használatát. A toronyház létesítéskor hatályos ágazati szabvány kimondta, hogy a füstelvezető nyílás nyithatóságát üzembiztos szerkezettel kell biztosítani a földszintről.

Az építéskor a szellőztetést úgy alakították ki, hogy gravitációs úton ablakokkal és szellőzőkürtökkel. Az ablakok nyithatóságát egy mechanikus szerkezet látta el, mely a lépcsőfordulókban található és egy mozdulattal nyithatóvá tette a hő- és füst elvezetésére szolgáló nyílászárókat. Más kérdés, hogy egy pánikhangulat során, menekülés közben ki fogja

ezeket a mechanikus szerkezeteket fizikai erővel kinyitni. Megjegyzem, hogy ezek az eszközök az idő során korrodálhattak és sok esetben nehezen vagy egyáltalán nem nyithatóak.

A hő és füstelvezetés korszerűsítése céljából a négy nagyteljesítményű füstelvezető ventilátor került kialakításra, mely lényegesen javított a hő- és füstelvezetés hatékonyságán. A kazánházban az esetleges rendellenes működés következtében keletkező égéstermékek elvezetésére CO érzékelő által vezérelt ventillátorok találhatók. Az érzékelők az egészségügyileg veszélyes koncentráció 20 %-ánál jeleznek és az elszívó ventillátorok automatikusan beindulnak és a veszélyes égéstermékeket elvezetik.

Tüzivíz ellátás

A toronyház pincéjébe található a tüzivíz ellátását segítő két darab tüzivíz szivattyú, ezek Diósgyőri Gépgyár által készített szivattyúk, 4 és 5 lépcsős berendezések. Indításuk lehetséges kézi és automatikus úton is.

5. ábra. A tüzivíz szivattyú jelölve is van

6. ábra. A két tüzivíz szivattyú

A szivattyúk percenként 650 liter vizet képesek előállítani, 8 bar-os nyomáson. A toronyház áramtalanítása esetén (tűzoltó-beavatkozás esetén) a tüzivíz-hálózat működőképessége folyamatosan biztosított az épület tetején található 100 m^3-es víztározó tartályról. [4]

7. ábra. A 100 m3 tartály az épület tetején

Ebből a tározóból a víz gravitációs úton kinyerhető, a 20 emeletes magasságban a hidrosztatikai nyomás is jelentős, külön szivattyúra nincs szükség. A tartály ellátását a pincében két darab hidegvíz típusú szivattyú biztosítja, mely automatikusan vagy kézi indítással vezérelhető, ami a tartály feltöltését szolgálja, amennyiben abból fogyasztást tapasztalható, fentiek miatt a tartály mindig feltöltött állapotban található, ezért a 100 m^3-nyi vízmennyiség állandóan figyelembe vehető. A tetőtéren a tartálynak közvetlen víz-kivételezési helye van kialakítva, e mellett található egy sugárcsövet, haboldat-bekeverőt, 50 méternyi tömlőt tartalmazó tűzcsapszerelvény szekrény, továbbá a tetőn tárolnak 50 liter habképző anyagot.

8. ábra. A tartályra csatlakozó 2 db B 95-ös nyomótömlő

A fenti ábrán láthatjuk a tartályra csatlakozó 2 db B 95-ös nyomótömlőket [4].

Falitűzcsap hálózat

A ház tűzrendészeti ismertetésében foglaltak alapján minden lakószinten volt 1-1 nedves és száraz tűzcsapszekrény, közvetlenül a nyomóvezetékről leágazva. A toronyház 1971. június 14-én kiadott jegyzőkönyvében az áll, hogy a szintenként elhelyezett fali tűzcsapok nincsenek ellátva a szükséges tűzoltó felszerelésekkel, például tömlővel és sugárcsővel.

Az épületben a szintenként kiépített falitűzcsapokhoz biztosították a megfelelő felszereléseket, úgy, mint 30 méteres lapostömlőt, sugárcsövet, kapocspárkulcsot. A falitűzcsapok kialakításánál figyelembe vették, hogy az adott szint védelmét teljes területen lefedjék. [5]

9. ábra. Szintenként kialakított fali tűzcsap a hozzá tartozó szerelvényekkel

Tűzoltó készülékek

A falitűzcsap hálózaton kívül az épületben minden szinten helyeztek el porral oltó kézi tűzoltó-készülékeket, ezek a jelenlegi szabályoknak és szabványoknak megfelelő MSZ EN 3-as 6 kg-os ABC porral oltó készülékek. Szintén a jelenlegi szabályozásnak megfelelő készülékek vannak kihelyezve a felvonógépházban, itt 2 db 2 kg-os széndioxiddal-oltó készülék található, valamint a kazánhelyiségekben 2-2 db. egyenként 12 kg-os ABC porral oltó készülék. Szintenként található 1-1 db. 6 kg-os poroltó készülék. [5]

ÖSSZEGZÉS

A világ állandóan fejlődik, ezáltal napjainkban is folyamatosan épülnek újabb és újabb technikával magas épületek, amit még a 1960-as és 70-es években hatalmas megdöbbenéssel és figyelemmel kísértek az emberek, manapság pedig természetes a számunkra, hogy a fejlődő világ minden részén épülnek monumentális építmények.

A cikk elkészítése során célom volt a Gyöngyösi toronyház megelőző tűzvédelmének bemutatása és részletes ismertetése.

A magas épületekre helyeztem a hangsúlyt, a toronyház magas épület, általánosságban mindig együtt kezeljük, tanuljuk a középmagas épületekkel, azaz nem részletezzük a magas épületek sajátos tudnivalóját. A magas épületeket jól el kell különíteni a középmagas épületektől, bár nagyon sok hasonló vonásuk van és a jogszabályok megközelítése is azonos, fontos hangsúlyoznunk a magas épületek kiemelkedő jelentőségét.

Az esettanulmányban feltártam a toronyház létesítésekor betartandó követelmény-rendszert és összevetettem a jelenlegi követelményrendszerrel. Ebben segítségemre volt az a toronyház tervdokumentáció, ezáltal ismertetem az olvasóval a toronyház építésének sajátosságait, hiányosságait, tervezéskor történt problémákat és nem utolsó sorban a hatóságok engedélyezési dokumentációját is. A toronyház mai állapotát is elemeztem.

Arra a következtetésre jutottam, hogy a toronyházban vannak olyan eszközök, amik újításra vagy kiépítésre szorulnak, mert nem találhatók az épületben. A fejlesztések a közeljövőben nem fognak megvalósulni, mivel a lakók anyagi fedezet hiányában a háttérbe helyezik ezeket a fejlesztéseket. A megfelelő anyagi háttérét csak pályázat útján lehetne előteremteni, de ilyen jellegű pályázat jelenleg nem található Magyarországon.

Felhasznált irodalom

[1] Mátra Lapok Közéleti Hetilap III. évfolyam 47. szám 1998. December 2. 5 oldal ISBN: nélkül

[2] Bakaity Mónika: „Paneles lakóépületek tűzvédelme” című Tudományos Diákköri Dolgozat, Budapest, 2009, 15. oldal Konzulens: Szigeti Péter

[3] Heves megyei építők lapja, 1969. október 16. IV. évfolyam 10. szám

[4] A toronyház Használatbavételi engedélye.

[5] A toronyház tervdokumentációja, tűzrendészeti ismertetése, XV-12 134 sz. IN:573 m/ 1968 Gyöngyös város tervtára

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Pátzay György
patzay.gyorgy@uni-nke.hu

A PAKSI ATOMERŐMŰ RADIOAKTÍV NORMÁLÜZEMŰ ÉS ÜZEMZAVARI HULLADÉKOLDATAINAK SZELEKTÍV TISZTÍTÁSA

Absztrakt

Jelen cikkben ismertetem 1975-2010 között végzett kutató-fejlesztő munkánkat a Paksi Atomerőműben keletkező normál üzemű hulladékfeldolgozása terén és a bekövetkezett 2003-as üzemzavar kárelhárítási tevékenységben. Bemutatom továbbá az FHF technológia fejlesztése terén végzett fejlesztéseink eredményeit.

I present our research and development work carried out between 1975-2010 in the Paks Nuclear Power Plant, resulting in normal mode and the processing of waste occurred in 2003 incident remediation works. I also introduce the results of developments in the field of liquid radwaste treatment processing technology (LRWTT).

Kulcsszavak: *atomerőmű; folyékony hulladék; eljárás; hulladék-feldolgozás; helyreállítási munkák; radioaktív ~ Nuclear Power Plant; wastesolutions; treatment; waste occurred/processing; remediation works; radioactive*

A PAKSI ATOMERŐMŰ ÜZEMELÉSÉVEL KAPCSOLATOS KUTATÁSAINK RÖVID TÖRTÉNETE

1975-ben kutatások kezdődtek az OAB megbízásából radioaktív Cs és Sr szelektív elválasztására csurgalékvizekből ammónium ionokkal előkezelt Tokaj környéki klinoptilolitos és mordenites riolittufákkal. A kémiai előkezelés következtében a cézium kapacitás 3-szorosára nőtt (0,85 mmol/g). 1990-ben a kifejlesztett szorbenseket kipróbáltam az atomerőmű csurgalékvizeinek cézium mentesítésére. Az erőmű VK-123-as helységében összesen 272 dm^3 radioaktív oldatot tisztítottunk meg a cézium izotópoktól DF = 100 dekontaminációs faktor mellett 0.3 dm^3 szelektív ioncserélővel 366-szoros térfogatsűrítést értünk el.

1992-ben cianoferrát alapú céziumszelektív ioncserélőt dolgoztam ki, és granulált kálium-nikkel-hexacianoferrát(II) ioncserélőt állítottunk elő fagyasztásos módszerrel. Az erőműből küldött sűrítmény oldatokból a radioaktív cézium izotópokat DF > 1000 mellett 2500-3500-szoros térfogatsűrítéssel távolítottuk el. 1992-ben az erőmű VK 123-as helységében 110 dm^3 sűrítmény tisztítását végeztük el 50-100 cm^3 0,2-0,3 mm szemcseméretű ioncserélővel 15 ágytérfogat/óra áramlási sebesség mellett. A két, közel azonos tulajdonságú (01TW30B002 és 02TW30B002) oldatból a cézium izotópokat 2500-3500-szoros térfogatsűrítés mellett sikerült szelektíven eltávolítani. Ugyanakkor a 01TW30B003 jelű oldat kezelésénél komplikációk léptek fel. Komplexképzők roncsolták az ioncserélőt! Ennek eredményeként, ennél a mintánál az elérhető térfogatsűrítés csak 200-szoros volt. [1]

Ugyanebben az évben sűrítmények borát tartalmának visszanyerését vizsgáltam széndioxidos közömbösítés, nátrium-ammónium ioncsere és az ammónium-borát termikus bontásával. A német-magyar közös diplomamunka során sikeresen választottuk le a tiszta bórsavat paksi sűrítmények modelloldataiból.

1995-ben diplomamunka keretében a laboratóriumi kísérletek ellenőrzésére a paksi atomerőműben egy nagyobb méretű töltettel (75 cm^3) végeztünk kísérletet. A feldolgozott koncentrátum a 02TW30B002-es sűrítmény tároló tartályból származott, és 9 ágytérfogat/óra térfogatárammal áramlott keresztül az oszlopon. 86,7 dm^3 bepárlási koncentrátum cézium mentesítését végeztük el 25 cm^3 ioncserélővel, 1031,5-es átlagos dekontaminációs faktor mellett. Ez 3156-os térfogat sűrítési faktornak felelt meg. [2]

1999-ben ugyancsak diplomamunka keretében a kísérletek során az 01TW10B001 számú tartályban tárolt friss sűrítmény oldatot (tárolási idő < 2 év), valamint egy másik sűrítmény oldat bórsavmentesített anyalúgját (tárolási idő> 6 év) vizsgáltuk. Az ultraszűrési kísérleteket a MICRO CARBOSEP 40 típusú ultraszűrő készülék M5 (15 k Dalton) membránja segítségével, 2 bar nyomáskülönbség mellett végeztük. Majd mindegyik radioaktív izotóp előfordult ultraszűrhető formában (3-11%).

2001-ben a Paksi Atomerőmű Duna-vízzel működő hűtőrendszeri csöveinek korróziós károsodásából származó 2 db szénacélból készült, csőminta korróziós felmérésére kaptunk megbízást. Ezen túlmenően, a korróziós károk felmérési eredményeinek függvényében javaslatot kellett tennünk a jelenlegi csőrendszer kiváltásra alkalmazni kívánt ötvözött acél és titán-adagolt rozsdamentes acélcsövek 35 éves szolgálati időre tervezhető javasolt falvastagságára és a korrózió szempontjából biztonságos üzemelési feltételekre. A kutatás eredményeképpen a felmérések alapján javaslatot tettünk a csővezeték rendszer felújítására és a további mikrobiológiai korrózió hatásának csökkentésére.

2003-tól folyamatosan részt vettünk a paksi üzemzavar során keletkezett vizes oldatok ellenőrzésében, szakértési feladatokban és a kárelhárító munkák tervezésében.

2006-ban az OAH felkérése megvizsgáltuk az erőműben alkalmazott ausztenites rozsdamentes acélminták korund szemcsék által okozott eróziós korrózióját. [3]

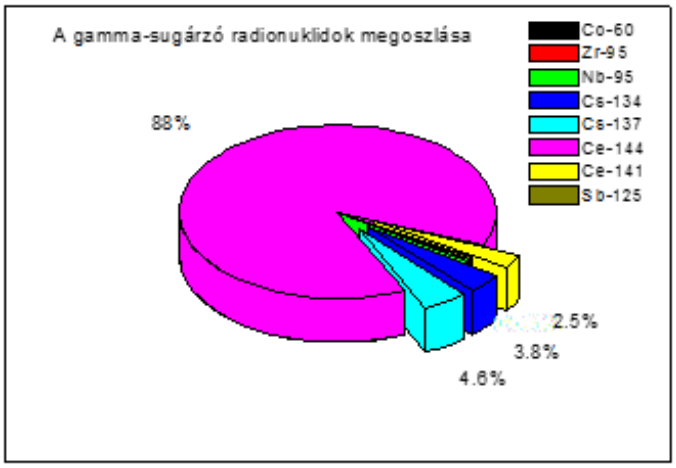
RÉSZVÉTEL A 2003-AS ÜZEMZAVAR KÁRELHÁRÍTÁSI MUNKÁIBAN [4, 5]

2003-tól folyamatosan részt vettünk az üzemzavar során keletkezett vizes oldatok radioaktivitásának értékelésében, a vízkémia és víztisztítás kialakításában. A Paksi Atomerőmű felkérésére vizsgáltuk transzuránok és aktinidák szelektív elválasztásának lehetőségeit az 1. sz. aknában lévő 20 g/l bórsav tartalmú üzemzavari oldatból. A kísérletek eredménye alapján a Mitsubishi Nuclear Fuel Co. TANNIX nevű ioncserélő szorbensét választottuk ki a feladat végrehajtására.

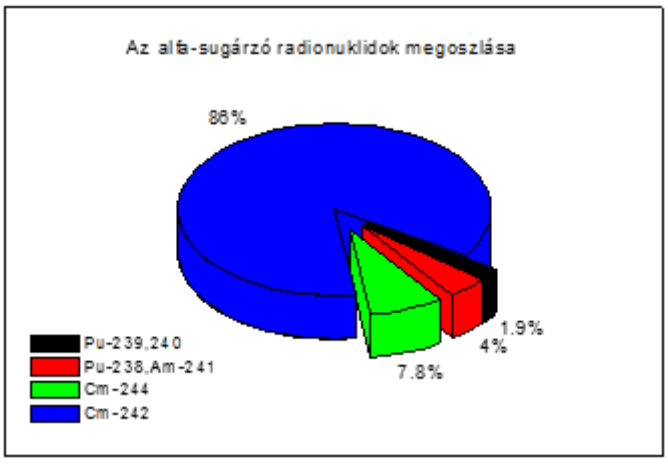
A kiválasztott szorbenssel az alábbi feladatokat hajtottuk végre:

- Transzuránok és aktinidák szorpciós megkötésének vizsgálatát a 2. blokk szennyvíz mintáiból a Mitsubishi Nuclear Fuel Co. Ltd. TANNIX szelektív szorbensével.
- Megoszlási hányados meghatározását Cm, Am, Pu és U izotópokra. Oszlopkísérleteket végeztünk a paksi 2. blokk szennyvizével az alfa-sugárzó radioaktív izotópok elválasztásának vizsgálatára.
- A kísérletek a PARt helyiségeiben történtek az influens és effluens oldatok alfa-sugárzó izotópjainak aktivitás koncentrációinak meghatározását a PARt analitikai részlege végezte.
- Kísérleteket értékeltük, a TANNIX szorbens alkalmazhatóságával kapcsolatban és javasoltuk az alkalmazását.

A kezelésre került radioaktív oldat gamma-sugárzó és alfa-sugárzó radionuklidjainak százalékos összetételét az 1. és 2. ábrákon mutatjuk be.



1. ábra. A kezelt oldat gamma-sugárzó izotópjainak százalékos összetétele [4]



2. ábra. A kezelt oldat alfa-sugárzó izotópjainak százalékos összetétele [4]

Egyensúlyi kísérletek

A laboratóriumi egyensúlyi kísérleteket a PARt segédépület expressz laboratóriumában végeztük. Az egyensúlyi kísérletekhez a TANNIX szorbens ammónium-formáját a Mitsubishi Nuclear Fuel Co. Ltd. japán cég bocsátotta rendelkezésre. Az erőmű a 2. blokk 20TG0B001 medencéjéből ~10 liter radioaktív izotópokkal szennyezett vízmintát szolgáltatott a kísérletekhez. Az egyensúlyi kísérletekben egy új, általunk kifejlesztett szorbens alkalmaztunk. A TANNIX szorbenst és a TMIX néven kifejlesztett TANNIX szorbens VARION KSN-VARION ATN kevertágyas ioncserélő gyantatöltet 1:1 térfogatarányú keverékét adott térfogatarányban az 1. sz. akna vizével 25 ^{o}C hőmérsékleten 24 órán keresztül 25 rpm lassú rázási sebességgel termosztálva rázattuk, majd az egyensúlyi idő letelte után az elválasztott folyadékfázis gamma- és alfa-sugárzó radioaktív izotópjainak aktivitás koncentrációt a PA Rt laboratóriumaiban meghatározták.

Az egyensúlyi kísérletek eredményeit az alábbiakban foglaltuk össze:

- Mikroszűréssel (0,2 mm) a cérium és kűrium izotópok kivételével jelentősen nem csökkenthető a szennyvíz radioaktivitása a vizsgált pH értékeken.
- Az egyensúlyi mérések szerint a nióbium izotópok kivételével a vizsgált pH értékeken a szennyvíz eredeti pH~4,1 értékén figyeltük meg a legjobb elválasztást úgy a gamma-sugárzó, mint az alfa-sugárzó radioaktív izotópok esetében.
- A VARION KSN-H+ és VARION ATN-OH- szerves ioncserélő gyanták 1:1 térfogatarányú kevert-ágyas töltetének (TMIX) jelenlétében a TANNIX-szerves ioncserélő gyanta keverék egyensúlyi elválasztási hatásfoka – a nióbium izotópok kivételével - jelentősen megnövekedett úgy a gamma-sugárzó, mint az alfa-sugárzó radioaktív izotópok esetében. A szorbens keverék alkalmazásával az egyes radioaktív izotópok elválasztására jellemző dekontaminációs faktorok 20-1000%-al növekedtek.

Ultraszűrési kísérletek

Az eredeti oldatból lúg adagolásával pH=6,0 és pH=8,0 oldatokat állítottunk elő és a 3 különböző pH-jú 1 liter térfogatú oldatot a TECH-SEP cég MICRO-CARBOSEP 20-40-60 típusú asztali ultraszűrő készülékének 15 kDa vágási értékű kerámia-alapú ultraszűrő berendezésén 1-,5 bar nyomásesés mellett átszűrtük. Az ultraszűrőt és a kísérleti elrendezést a 3. ábrán mutatjuk be.

3. ábra. Az ultraszűrő berendezés [4]

Az ultraszűrési kísérletek eredményeit az alábbiakban foglaljuk össze:

- A ^{60}Co radionuklid ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~4,1 értéken 96,04%-a kiszűrhető.
- A ^{95}Zr radionuklid ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~4,1 értéken 74,9%-a kiszűrhető.
- A ^{95}Nb radionuklid ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~4,1 értéken 79,7%-a kiszűrhető.

- A ^{134}Cs és ^{137}Cs radionuklidok ultraszűréssel jelentős mennyiségben nem távolíthatók el a vizsgált pH értékeken.
- A ^{144}Ce és ^{141}Ce radionuklidok ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~4,1 értéken 88,5-88,9%-uk kiszűrhető.
- A ^{125}Sb radionuklid ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~4,1 értéken 43,7%-a kiszűrhető.
- Az összes mérhető alfa aktivitás ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~4,1 értéken 89,1%-a kiszűrhető.
- A ^{239,240}Pu és a 238Pu (^{241}Am) radionuklidok ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~6,0 értéken 31,5%, illetve 54,5 %-uk kiszűrhető.
- A ^{244}Cm és ^{242}Cm radionuklidok ultraszűréssel eltávolítható mennyisége függ a vizsgált pH értékektől, pH~4,1 értéken 90,91%, illetve 93,2 %-uk kiszűrhető.

Dinamikus oszlopkísérletek

Az egyensúlyi kísérletek alapján a továbbiakban a dinamikus kísérletekben a célnak legjobban megfelelő rétegelt és kevertágyas TMIX szorbens (VARION KS-H+-VARION AT-OH-ioncserélő gyantatöltet és az ammónium-formájú TANNIX aktinidákra és transzuránokra szelektív szorbens töltet 1-1 térfogatarányú keveréke) megkötését vizsgáltuk 2 párhuzamosan üzemelő ioncserélő oszlopba töltve.

A kísérletekhez a TG medence pH~4,1 értékű ultraszűrt hulladék oldatát alkalmaztuk.

A dinamikus oszlopkísérletek alapján a következő megállapításokat tettük:

- Az ultraszűrést, majd azt követő kombinált töltettel (TANNIX+szerves kevertágyas ioncserélő gyanta) végzett tisztítás rendkívül hatásos. Ezzel a kifejlesztett eljárással eltávolítható úgy a gamma-sugárzó, mint az alfa-sugárzó radioaktív izotópok döntő többsége.
- A rétegelt-ágyas elrendezésű szorbens keverékkel elérhető térfogatsűrítések és dekontaminációs faktorok jelentősen kedvezőbb értékek, mint a kevert-ágyas elrendezés hasonló értékei.

A kidolgozott eljárás alkalmazása az üzemzavar következményeinek elhárításában

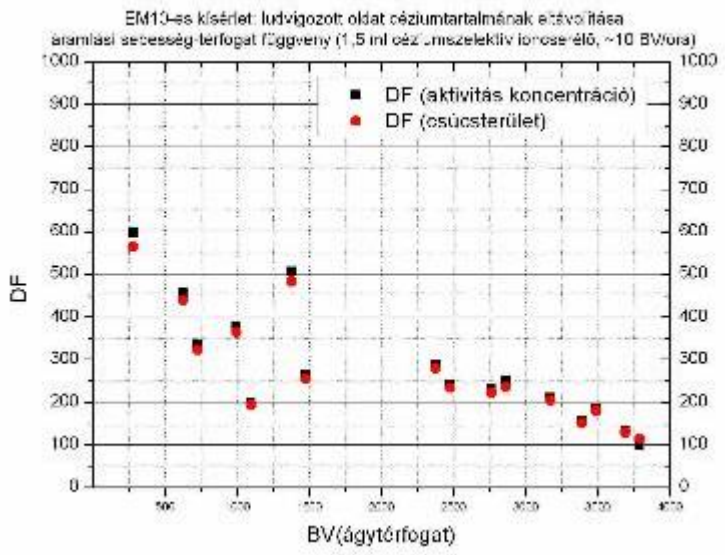
A kidolgozott TMIX szorbens technológiai megvalósítására 2006 novemberében került sor, amikor a mobil NURES konténerben a finn CsTreat és CoTreat szorbensoszlopok mellet 2 db, általunk kifejlesztett TMIX transzurán eltávolító szorbens töltet [1] is alkalmazásra került (4. ábra).

4. ábra. A NURES konténeres mobil víztisztító [4]

A kifejlesztett TMIX szorbens anyagot az erőműben továbbra is használják transzuránok szelektív eltávolítására vizes oldatokból.

AZ ERŐMŰ NORMÁL ÜZEME SORÁN KELETKEZŐ FOLYÉKONY HULLADÉKOK FELDOLGOZÁSÁT VÉGZŐ TECHNOLÓGIA (FHF) FEJLESZTÉSE

Az FHF technológia fejlesztésére cézium izotópcserén alapuló lúgálló szelektív szorbenst fejlesztettünk ki, mellyel inaktív sók oldatából szelektíven választható el ultra mikro-mennyiségű radioaktív cézium minimum 2800-szoros térfogatsűrítés és 100 fölötti dekontaminációs tényező mellett. Az 5. ábrán mutatjuk be az új lúgálló céziumszelektív szorbennsel kezelt, a paksi atomerőmű 02TW80B003 jelű sűrítményéből származó komplexbontás után kezelt oldat cézium mentesítésének áttörési görbéjét.



5. ábra. A 02TW80B003 sűrítmény cézium mentesítés a komplexbontás után [5]

A kísérleti eredmények alapján azt javasoltuk, hogy az FHF technológiát úgy kell módosítani, hogy első lépésként a meghatározó radioaktív izotópokat távolítjuk el a sűrítményből és csak ezután következik az inaktív vegyszerek (borátok, nitrátok stb.) elválasztása. A javasolt új sorrend:

1. Szerves anyagok elroncsolása, kobalt izotópok eltávolítása
2. Cézium izotópok szelektív elválasztása
3. Borátok, nitrátok leválasztása, kezelése, részleges bórsav kinyerés
4. Kis térfogatú radioaktív iszapok és szorbensek cementezése, temetése

4.ÖSSZEFOGLALÁS

A múltban sikeres kutató-fejlesztő munkával járultunk hozzá a Paksi Atomerőmű biztonságos üzemelésének biztosításához és a normál üzemelés során keletkezett folyékony hulladékok gazdaságos, biztonságos és környezetkímélő kezeléséhez, mely lehetővé tette a radioaktív sűrítmények szilárdítás utáni környezetbiztonságos elhelyezését a bátaapáti izotóptárolóban.

Az erőmű 2003-as INES 3 fokozatú üzemzavarának felszámolásában szakértőként és technológiai fejlesztőként vettünk részt és hozzájárultunk az üzemzavar következményeinek sikeres felszámolásához.

A jövőben az alábbi kutató-fejlesztő munkára számítunk a PA Rt radioaktív hulladékaival kapcsolatban:

- Az FHF technológia további fejlesztése (kobalt-komplex bontás, iszap, kristályos fázis);
- Membrántechnikai alkalmazások fokozott bevezetése;
- Korróziós kutatások.

Felhasznált irodalom

[1] Tóth, B., Pátzay, Gy.: Az atomerômûvi radioaktív hulladékok biztonságos kezelése. (The Safe Handling of the Radioactive Waste of the PWR) Magyar Kémikusok Lapja, Vol. 48., No. 10-11., 479-484, (1993)

[2] Pátzay, Gy., Weiser, L., Tóth, B., Pálmai, Gy., Feil, F.: New Technology for the Handling and Burial of MLW and LLW Evaporator Bottom of the PWR Paks, Periodica Polyechnica Ser. Chem. Eng. Vol. 39. No. 2, pp. 147-184, (1995)

[3] György Pátzay, László Weiser, Ferenc Feil, János Schunk, Gábor Patek, Radioactive wastewater treatment using a cesium selective ion exchanger and a mixture of TANNIX sorbent and VARION mixed bed ion exchange resin, J. Ion Exchange, Vol.18 No.4 (2007), 114-119

[4] G. Patzay, P. Tilky, J. Schunk, T. Pinter, F. Feil, K. Hamaguchi, L. Weiser "Radioactive wastewater treatment using a mixture of TANNIX sorbent and VARION mixed bed ion exchange resin", International Journal of Nuclear Energy Science and Technology (IJNEST), **2**(4), 328-341, 2006

[5] G. Pátzay, L. Weiser, F. Feil, G. Patek, J. Schunk, I. Gresits: Modification of Radioactive Wastewater Treatment Technology in The Hungarian PWR, WM2009 Conference, Phoenix, USA, 2009, Session 62, paper 4

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. január

Solymosi József - Solymosi Máté
solymosi.jozsef@uni-nke.hu - mate.solymosi@somos.hu

GONDOLATOK „AZ ATOMREAKTOROK BIZTONSÁGA” CÍMŰ KÖNYVRŐL

Absztrakt

Az Atomreaktorok biztonsága című könyv 2013. decemberben jelent meg a Somos Környezetvédelmi Kft. és az ELTE Eötvös Kiadó közös gondozásában. Recenzió gyanánt készült a könyvről ez a néhány gondolat a Hadmérnök olvasói számára.

In 2013 December, the Somos Environmental Protection Ltd. and the ELTE Eötvös Publishing Company published the Nuclear reactor's safety. The following thoughts are presenting a review about the book for the reader of the Hadmérnök.

Kulcsszavak: *atomreaktorok biztonsága, atomreaktorok működése és tervezése, biztonságos üzemeltetés, biztonsági elemzések, a reaktorbiztonság jogi keretei ~ safety of nuclear reactors, operation and construction of nuclear reactors, safe operation, safety assessment, legal regulation of the reactor safety*

BEVEZETŐ GONDOLATOK

A hadtudományokban és a katonai műszaki tudományokban a nukleáris biztonság terén kiemelten foglalkozunk az atomfegyverek és az ellenük való védekezés, valamint a non-proliferáció időszerű kérdéseivel. Különösen a tömegpusztító (CBRN, Chemical, biological, radiological and nuclear) fegyverek reneszánsza miatt felmerülő legújabb kori kihívásokra adandó, tudományosan megalapozott válaszok feltárásával, továbbá a nukleárisbaleset-elhárítás honvédségi feladataival.

Az Atomreaktorok biztonsága című könyv ezer szállal kötődik a honvédségi, védelmi feladatokhoz. Elsőként nyújt teljes körű elméleti és gyakorlati ismereteket a nukleáris biztonságnak a katonai műszaki tudományok számára is fontos területről, az atomreaktorok és atomerőművek biztonságáról, benne a nukleárisbaleset-elhárítás feladatairól.

Az atomenergia békés célú felhasználásának, a villamos energiatermelő atomerőművek biztonságos tervezésének és üzemeltetésének a kérdéseit veszi sorra, alaposan és kielégítő részletességgel.

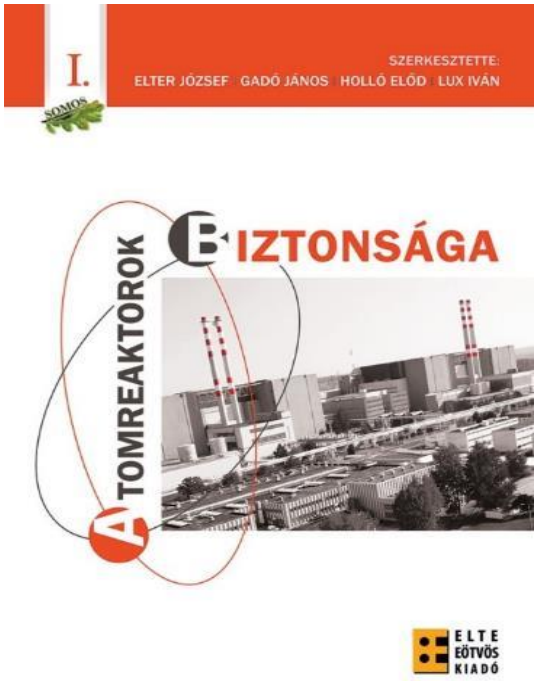
Szerzők a könyv előszavában a motivációjukat így fogalmazzák meg. „*E könyv szerzői ... úgy gondolták, hogy a társadalom számára legizgalmasabb kérdéskörben, nevezetesen az atomerőművek, atomreaktorok biztonsága terén viszonylag kevés a hozzáférhető szakirodalom. Éppen ezért az atomerőművek, atomreaktorok biztonságával foglalkozó hazai szakemberek egy csoportja elhatározta, hogy jelen könyvben megpróbálják összefoglalni a biztonsággal kapcsolatos tudnivalókat.*”[1] A könyv szerzőinek a szándéka tehát röviden a következő motivációs tényezőkkel foglalható össze: hiánypótlás, tudásátadás, az érdeklődés felkeltése, és a szakértővé válás segítése.[2] Tekintsük át a könyv tartalmát részleteiben.

ATOMREAKTOROK BIZTONSÁGA I. KÖTET

A könyv két kötetben jelent meg 750 oldal terjedelemben. Az I. kötet az 1.-3. fejezeteket tartalmazza 378 lapoldalon. A fejezetek tartalmi ismertetése az alábbiakban foglalható össze röviden, szinte csak felsorolás szerűen, a szerzőket is feltüntetve.

1. Az atomreaktorokban lejátszódó legfontosabb folyamatok

A első fejezet az alapvető magfizikai folyamatokat ismerteti, elősegítve ezzel a többi fejezet megértését: maghasadás, láncreakció, neutronfizika (Nagy László), kritikus rendszerek, kutatóreaktorok, atomerőművek (Vidovszky István), nyomottvizes reaktorok fizika alapjai (Nagy László), a termohidraulika alapjai (Házi Gábor), üzemanyagciklus, fűtőelem viselkedés (Hózer Zoltán), aktivitásterjedés, környezeti hatások (Zagyvai Péter, Sági László).



1. ábra. Az I. kötet borítója [2]

2. Az atomerőmű felépítése

Ez a fejezet az atomerőművek működési mechanizmusát mutatja be: az atomerőmű feladata, az erőművi körfolyamat, rendszerek, berendezések jellemzői (Jánosy János Sebestyén).

3. A reaktorok tervezési biztonságának alapjai

Ebben a fejezetben megismerkedhetünk a normál üzemi és a baleseti állapotokkal, és a tervezési alapokkal: üzemállapotok, a normál üzem biztonsága (Jánosy János Sebestyén, Zagyvai Péter), üzemzavarok és balesetek, biztonsági funkciók és rendszerek (Elter József), tervezési alap (Katona Tamás), determinisztikus tervezési elvek (Katona Tamás), kockázat és jellemzői/kritériumai (Bareith Attila, Holló Előd).

A reaktorok biztonsága tehát mind a tervezésnek, mind az üzemeltetésnek alapvető feladata. A reaktoroknak az atomerőmű minden üzemállapotában megfelelően biztonságosan kell működniük. Nem csak az üzemzavarok megelőzése, elhárítása, levezetése fontos az atomerőmű biztonsága szempontjából, hanem a normál üzem biztonsága, beleértve egy sor sugárvédelmi kérdést is.

Az atomerőműben üzemzavar során is garantálni kell a személyzet és a környezet biztonságát. A tervezés sokféle módon segíti elő a biztonságot az üzemzavari és baleseti helyzetekben. Ennek elemei többek között az ún. mélységi védelem, azaz az egymás mögé felsorakoztatott védelmi szintek rendszere, a radioaktív anyagokat a környezettől elzáró védelmi gátak rendszere, az atomerőműbe beépített biztonsági rendszerek és az ezek által ellátott biztonsági funkciók.

Az atomerőmű tervezése során a biztonsági filozófia összességét tervezési alapnak nevezzük, az ebbe tartozó jelenségeknek, folyamatoknak úgy kell lejátszódniuk, hogy a biztonsági követelmények messzemenően teljesüljenek (konzervatív becslés). Ebben döntő szerep jut az ún. determinisztikus tervezési elveknek és azok megvalósulásának. A biztonság megítélésének alapvető fogalma a kockázat, azaz egyszerre vagyunk tekintettel a vizsgált folyamatok veszélyességére és előfordulási gyakoriságára. A megfelelően alacsony kockázat elérésében, a tervezett vagy megépített rendszer biztonsági megítélésében nagyon fontos szerep jut a valószínűségi biztonsági elemzéseknek.

ATOMREAKTOROK BIZTONSÁGA II. KÖTET

A II. kötet a 4.-6. fejezeteket tartalmazza 372 lapoldal terjedelemben.

2. ábra. A II. kötet borítója [2]

4. A reaktorok üzemeltetési biztonsága

A fejezet tárgya az üzemeltetés biztonsága, amely a tervezés biztonsága mellett alapvető szerepet játszik. Ilyenek az üzemállapotok, a normál üzem biztonsága (Jánosy János Sebestyén, Zagyvai Péter), üzemzavarok és balesetek biztonsági funkciók és rendszerek (Elter József), tervezési alap (Katona Tamás), determinisztikus tervezési elvek (Katona Tamás), kockázat és jellemzői/kritériumai (Bareith Attila, Holló Előd).

A műszaki feltételek mellett a biztonság nagyon fontos és jelentős eleme a biztonsági kultúra, a biztonság emberi és szervezeti tényezői, amelyek lényegesen befolyásolják a már megvalósult atomerőmű biztonságát. Az üzemviteli szabályok, utasítások és eljárások teremtik meg az összhangot és koherenciát a tervezéssel. Ezeket a szabályokat az üzemeltető személyzetnek minden körülmények között be kell tartania, az atomerőmű normál üzemében, illetve üzemzavarai és balesetei esetén egyaránt. A karbantartások, a felügyeleti és ellenőrzési tevékenységek, valamint a próbák ugyancsak az üzemeltetési biztonság igen lényeges elemei. Az atomerőmű minél hosszabb, egyben biztonságos üzemidejének elérésében kulcsfontosságú az öregedéskezelés.

5. A biztonsági elemzések alapjai

A biztonsági szint megfelelőségét az ellenőrző mérések és tesztek mellett biztonsági elemzésekkel is bizonyítani kell. Ezt a célt szolgálják a DBA és BDBA elemzések (Tóth Iván, Gadó János, Keresztúri András), a súlyos baleseti elemzések (Téchy Zsolt, Lajtha Gábor), a PSA1 és PSA2 valószínűségi elemzések (Bareith Attila, Téchy Zsolt), a külső veszélyek hatásának elemzése (Katona Tamás, Bareith Attila), a forrástag, aktivitásterjedés, egészségügyi hatások (Sági László, Pázmándi Tamás, Zagyvai Péter).

6. A reaktorbiztonság jogi keretei

A jogi keretek – mint általában – az atomreaktorok alkalmazásának társadalmi beágyazását alapozzák meg, meghatározva annak feltételeit és kereteit úgy, hogy ez a tevékenység társadalmilag elfogadhatónak minősüljön. Mivel alapvetően ipari, műszaki tevékenységről van szó, lényeges kiemelni, hogy a vonatkozó jogszabályok nagymértékben támaszkodnak különböző nemzetközi szabványokra és más nemzetközileg elfogadott normákra. Ezek között a legfontosabbak a Nemzetközi Atomenergia Ügynökség biztonsági szabványai [3], valamint az Európai Unió kötelező érvényű jogszabályai és ajánlásai. A biztonság megvalósulását szavatolják a nemzetközi szervezetek, valamint a nemzetközi egyezmények rendszere.

A fejezet tartalma: a törvényi és jogszabályi háttér, felelősségek (Adorján Ferenc), biztonsági jelentések (Adorján Ferenc), nemzetközi szervezetek és egyezmények (IAEA, OECD NEA, ENSREG, WENRA) (Lux Iván).

ZÁRÓ GONDOLATOK

A könyv hazai szerzői a világon elsőként adták közre egyetlen könyvben összefogottan ezt a komplex tudásanyagot. Az elméleti kérdések mellet a könyv betekintést nyújt abba a folyamatba, hogy miként kezelik a szakemberek a gyakorlatban az atomerőművek, atomreaktorok biztonsági kérdéseit. A könyv tehát egy hiánypótló és teljesen újszerű vállalkozás, amilyen eddig nem létezett. Bátran kimondhatjuk, hogy egy új és fényes világítótorony a nukleáris biztonság tengerén. Világít és segít eligazodni az atomenergia békés célú felhasználásának túlnyomó hányadát jelentő, villamos energiatermelő atomerőművek biztonsági kérdéseiben.

Aktualitása és egyben a fontossága mindenképpen elismerésre méltó, hiszen hazánkban a villamos energiatermelés több mint 40%-át az MVM Paksi Atomerőmű Zrt. szolgáltatja, folyamatosan garantálva az ellátás biztonságát. Ugyanakkor napjainkban elengedhetetlenné vált az energiaellátás növelése, amelynek egyik fontos és környezetbarát módja lehet a paksi atomerőmű tervezett bővítése új blokk, vagy blokkok építésével. A bővítéshez is tudást és tapasztalatot meríthetnek a könyvből a fiatal szakemberek, de az adott szakterületen tanuló egyetemi hallgatók, oktatók és dolgozók egyaránt. Igen, tapasztalatot, hiszen a könyv írói a sok évtized alatt általuk megszerzett gyakorlati ismereteket is beépítették ebbe a remekműbe.

A nukleáris biztonságnak a bevezető gondolatoknál említett átfogó kérdéséhez visszatérve, azt mondhatjuk, hogy a hadtudományok és a katonai műszaki tudományok, a katasztrófavédelem, benne különösen az iparbiztonság tanulói, tanárai és gyakorlati szakemberei is hasznosan forgathatják ezt a könyvet. Örömmel tesszük közzé, hogy a Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet kötelező tananyagként felvette a könyv tartalmát szak tantárgyi programjába[1].

Holló Előd, szerkesztő a könyv bemutatóján szóbeli kiegészítőjében közölte, hogy felmerült a könyv angol nyelven történő kiadásának a komoly gondolata, rövidített változatban[2]. Ugyanott Sipos László az MVM Paksi Atomerőmű vezető mérnöke hozzászólásában elmondta, hogy a könyv tartalmát felveszi tananyagként az általa szervezett, 3-4 féléves nukleáris technikai mesteriskola tematikájába[3].

A könyv megjelenését tekintve, az igényes, keménykötéses kivitelben készült. Negatívumként lehet talán megemlíteni, hogy az illusztrációk nem minden esetben a legjobb

[1] Prof. Dr. Bleszity János ny. tű. vezérőrnagy, intézet igazgató – Katasztrófavédelmi Intézet, Nemzeti Közszolgálati Egyetem írásbeli közlése szerint, az ELTE Eötvös Kiadónak címezve

[2] Holló Előd szerkesztő: Kiegészítő bejelentés az Atomreaktorok biztonsága című könyv ismertetésén, MNT Nukleáris Technikai Szimpózium Budapest, 2013. december 5-6.

[3] Sipos László az MVM Paksi Atomerőmű vezető mérnöke: Hozzászólás az Atomreaktorok biztonsága című könyv ismertetéséhez, MNT Nukleáris Technikai Szimpózium Budapest, 2013. december 5-6.

felbontásban, illetve fekete-fehérben kerültek a könyvbe és ezért esetenként nehezen értelmezhetőek.

A könyv 24 szerző műve. Nem oktatók írták, de a szakterületük eredményes és elismert művelői, hazai és nemzetközi téren egyaránt. Ez a sokszínűség helyenként a könyv szerkezeti hiányosságait eredményezi. Nem annyira a z oktatói szemlélet hiánya, inkább az egységes felfogás és közreadás kifogásolható a könyvben.

A szerkesztők homogenitásra törekedtek azzal a célkitűzéssel, hogy az általános elveket kell ismertetni, és egyben paksi példákkal hivatkozni a gyakorlati megvalósításokra. 24 szerző egyéni látásmódja mellett a négyfős szerkesztő bizottságnak nem volt könnyű dolga a homogenitás megteremtésével. Dicséretes, hogy ez a törekvésük túlnyomó részt sikerrel járt, sajnálatos azonban, hogy szemmel láthatóan nem minden esetben.

Mivel a könyv a nukleáris biztonság témakörében alapvetően angol nyelven megjelent irodalmi forrásokat felhasználó szakembereknek szól, ezért jól jönne, ha könyv végén található lenne egy angol-magyar szakkifejezések kisszótár és egy szószedet a rövidítések jegyzéke mellé.

Megítélésünk szerint ez a könyv tovább erősíti a nukleáris biztonság területén meglévő szoros kapcsolatot és szakmai együttműködést a katonai és a civil szféra között. Emlékeztetünk arra, hogy a könyv szerzői közül többen tevékenyen vesznek részt az NKE és jogelőd intézménye, a Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskolájának a tevékenységében – mint PhD hallgató, majd PhD doktor (Sági László), mint oktató és bírálóbizottsági tag vagy opponens (Gadó János, Zagyvai Péter).

Itt emeljük ki továbbá, hogy 2013-ban a Magyar Tudományos Akadémia, az MVM Paksi Atomerőmű és a Somos Alapítvány által alapított „Hevesy György-díj a Nukleáris Biztonságért” elismerést *Gadó János*, az MTA doktora[4] vehette át kimagasló tudományos eredményeiért.[4]

Ezek alapján jó szívvel ajánljuk a könyvet a védelmi és a civil szféra minden szakemberének.

Felhasznált irodalom

[1] Atomreaktorok biztonsága I., II. kötet. Szerkesztők: Elter József, Gadó János, Holló Előd, Lux Iván, Budapest, Somos Környezetvédelmi Kft., ELTE Eötvös Kiadó, 2013. ISBN 978-312-180-1, és ISBN 978-312-182-5

[2] Holló Előd, Elter József, Gadó János, Lux Iván: Atomreaktorok biztonsága című könyv ismertetése, MNT Nukleáris Technikai Szimpózium Budapest, 2013. december 5-6. http://nuklearis.hu/sites/default/files/symposium/402.pdf (Letöltés ideje: 2013. 12. 21.)

[3] IAEA Safety Standards Series: http://www-pub.iaea.org/mtcd/publications/sss.asp (Letöltés ideje: 2013. 12. 21.)

[4] SOMOS Alapítvány – a védelmi és biztonsági oktatásért és kutatásért, Díjazottak http://mta.hu/mta_hirei/a-nuklearis-biztonsag-teruleten-elert-kutatasi-eredmenyeket-ismertek-el-az-akademian-131876/ (Letöltés ideje: 2013. 12. 21.)

[4] Gadó János MTA adatlapja: http://mta.hu/koztestuleti_tagok?PersonId=11351 (Letöltés: 2013. 12. 27.)

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Szabó Sándor
s.szabo@mil.hu

LATEST TECHNOLOGIES SUITABLE FOR CHEMICAL DECONTAMINATION OF SENSITIVE EQUIPMENT AND INTERIOR FOR THE HUNGARIAN DEFENSE FORCES

Abstract

NATO's Strategic Concept exactly determines that the proliferation of chemical weapons and other weapons of mass destruction may cause incalculable consequences for global stability and prosperity. The immediate CBRN hazard control can sustain the operational capability and preserve the survivability of troops. One of the most significant part of hazard control is the chemical decontamination which can reduce the contamination level of the military equipment, combat vehicles and personnel. The sensitive equipment and interior CBRN decontamination technologies represent modern innovation which can reduce harmful effect of chemical warfare agents effectively. The Hungarian CBRN decontamination system has not possessed these technologies yet, but their deployments are urgently needed.

A NATO stratégiai koncepciója egyértelműen meghatározza, hogy a vegyi fegyverek és más tömegpusztító fegyverek elterjedése beláthatatlan következményt jelentenek a világ gazdasági konjunktúrájára és stabilitására. Az ABV veszélyhelyzetek gyors kezelése a műveleti képesség és a csapatok túlélőképességének megőrzéséhez járul hozzá. Az ABV veszélyhelyzet kezelés egyik legmeghatározóbb része a vegyimentesítés, amely csökkenti képes a katonai felszerelések, harcjárművek és személyi állomány szennyezettségi szintjét. Az érzékeny eszköz és belső tér ABV mentesítő technológiák jelképezik azokat a modern újításokat, melyek hatékonyan csökkentik a vegyi harcanyagok káros hatásait. A magyar ABV mentesítő rendszer nem rendelkezik ezekkel a technológiákkal, de műveleti alkalmazásuk egyre sürgetőbbé válik.

Keywords: *CBRN defence, chemical decontamination, decontamination solution, vacuum based decontamination technology, sensitive equipment decontamination ~ ABV védelem, vegyi mentesítés, vákuum alapú mentesítési technológia, érzékeny eszköz mentesítés*

INTRODUCTION

If hazard control procedures and hazard precaution are not effective, decontamination of personnel, equipment and sensitive materiel can be necessary. Decontamination is the reduction or removal of chemical agents from contaminated surfaces or inner sections. Chemical decontamination may be carried out by removal of chemical warfare agents by physical means or by chemical neutralization or detoxification.

The chemical decontamination is the process which can provide safety environment for contaminated military equipment, combat vehicles and personnel by absorbing, destroying, neutralizing, and making harmless chemical contamination. [1]

The main purposes of the chemical decontamination can be for avoiding the cross contamination, controlling the spread of contamination, sustaining the operational capability, protecting support personnel and reestablishing combat assets.

New chemical decontamination technologies have appeared which can reduce the duration of decontamination and improve the effectiveness of hazard management.

The most critical parts of chemical thorough decontamination procedures are to handle sensitive equipment and vehicle interiors which capabilities are absent from the Hungarian Defense Forces' CBRN decontamination system. Some alternative modern worldwide leading chemical decontamination technologies exist which can mean trustable solution for ensuring full aspect decontamination procedures including chemical decontamination of sensitive equipment and vehicle interiors.

PROBLEM FRAMING OF SENSITIVE EQUIPMENT AND VEHICLE INTERIOR DECONTAMINATION

Traditional decontamination of chemical warfare agents means use of ''wet'' solutions, such as chemical mechanisms decontamination. Two types of chemical mechanisms have been used during the sensitive equipment[1] decontamination: oxidation and acid/base hydrolysis. Mustard[2] and the persistent nerve agent VX contain sulfur molecules that can step in oxidation reactions. VX and other nerve agents contain phosphorus groups that can be hydrolyzed. The most of the chemical decontaminants are designed to oxidize HD and VX and to hydrolyze nerve agents.

The most important category of chemical oxidative decontamination reactions is oxidative chlorination. This term covers the "active chlorine" chemicals like hypochlorite. Hypochlorite solutions can be effective universally against the organ phosphorus and mustard agents. The VX and HD contain sulfur atoms which are readily effect to oxidation.

Alkaline hydrolysis is often initiated by the nucleophilic clash of the hydroxide ion on the phosphorus atoms which can be found in VX the G agents. Hydrolysis is a chemical reaction in two possible environments, acidic or alkaline. Hydrolysis rates depend on chemical structures and reaction conditions such as pH, temperature, the kind of solvent used, and the presence of catalytic reagents. Acidic hydrolysis is less important for agent decontamination because the hydrolysis rate of most chemical agents is slow, and the sufficient acid catalysis is mostly not observed. [2]

The traditional decontamination requires storage, transport, and waste management of huge amount of hazardous chemicals. One of the typical problems, that this traditional decontamination procedures demand the release of large amounts of chemicals into the environment. Highest research efforts are going on to find environmental friendly methods to

[1] Sensitive equipment can not resist against corrosive decontamination solutions. Personal computers, GPS, radio transmitter, optics and electronics are listed here.

[2] Chemical warfare agents are usually assigned what is termed a military symbol. H - mustard gas, HD - distilled mustard, GA - tabun, GB - sarin, VX - VX nerve agent

avoid useless environmental pollution. Another major problem is that current decontamination solutions are strongly corrosive to all kinds of materials (plastic, metal, rubber) and cause severe damages on the surface and inside of sensitive equipment. For this reason ‘‘wet’’ decontamination methods are not suitable for use on sensitive equipment, restricting their use in critical mission areas, such as vehicle interiors. In addition, long decontamination chemical reaction times, typically 20 - 30 min, are needed for wet methods to be effective.

A replacement decontamination technology is needed that is capable of selective and quick destruction of chemical warfare agents, is preferably all-dry, does not require mass storage, is easily transported, does not affect sensitive equipment and does not menace with dangerous environmental pollution. [3]

Potential alternatives can be the vacuum based decontamination technologies which can meet all requirements to be safe and effective decontamination procedures.

SENSITIVE EQUIPMENT DECONTAMINATION TECHNOLOGY

A lot of military equipment and combat devices are non-protected against corrosive decontamination solution and their electronic circuits may be damaged easily. The surface and inside of sensitive equipment is generally difficult to decontaminate due to location of equipment, features of materials or construction characteristics. One of the most worldwide leading chemical decontamination technologies, as a possible solution for this problem is the vacuum based chemical decontamination technology.

The vapor pressure is the physical parameter which determines the persistency, volatility, and mobility of the chemical warfare agents. The chemical decontamination of sensitive electronic equipment can be carried out in a special vacuum chamber. This vacuum chamber can provide vacuum and thermal energy as special conditions for removing chemical warfare agents from the sensitive equipment without any corrosive or harmful effects.

1. Figure. The Kärcher Decontainment System for Sensitive Material (DSSM). [4]

The vacuum based chemical decontamination is accomplished by the following procedures:

- Temperatures: up to 70 °C which is limited by the storage temperature range of the sensitive equipment,
- Vacuum: down to 1 Pa[3] which can remove chemical warfare agents by evaporating and desorbing from the surface and interior of the equipment and electric instruments.

[3] Vapour pressure of VX: 14 Pa at 20 °C

This way, the pressure in the chamber will be reduced below the vapour pressure of the agents to enable them to desorbs and evaporate. Since desorption and evaporation is enhanced by increased temperatures and is responsible for the cooling down of the surfaces the process is supported by heating. In regard to the volatility of the agents they will be removed immediately to prevent condensation due to saturation of the atmosphere in the chamber. To ensure effective decontamination, the whole process is program controlled. The relevant parameters are kept within defined limits, temperature decrease due to evaporation is compensated and evaporating chemical warfare agent is removed out of the chamber by suitable program steps. [5]

Sensitive equipment detoxification technology

The detoxification multiphase system contains a pressurized aerosol container ready to use. This pressurized system consists of a sorbent solvent-co-solvent propellant which is part of a kit including a special vacuum device. If this system is applied directly to sensitive surfaces, it can immediately contact and absorb the contaminant, and then solidifies to form a white powder which is evacuated into the vacuum receptacle. Chemical warfare agents are neutralized by detoxification powder and the waste material is contained for disposal. There is no chemical or thermal reaction just the mechanical removal of the contaminant.

2. Figure. The CRISTANINI sensitive equipment detoxification SX34 decon vacuum in use. [6]

Advantages of detoxification technology:

- Very flexible system which can provide rapid response,
- It can remove wide range of chemical warfare agents with high efficiency,
- The product can be stockpiled without any restriction for long time duration,

Decontamination Procedure:

- Detoxification powder is sprayed directly on the surface to be decontaminated like an aerosol paint,
- The surface will be covered by a thick compact white layer of powder,
- After waiting of the reaction time (20 – 30 sec) it is possible to remove the powder layer by means of the appropriate vacuum device,

The contaminant toxic agent compound diffuses into the porous solid system of the vacuum receptacle where it becomes trapped. The chemical decontamination solution which is the part

of the kit is able to neutralize chemically the aggressive agents, thanks to its oxidation and hydrolization action.

The decontamination is successful on the surface when there are no any signs of chemical warfare agent presence which is controlled by chemical agent monitor. If the decontamination is not efficient the decontamination procedure has to be repeated.

INTERIOR DECONTAMINATION TECHNOLOGY

The most significant disadvantage is the gasoline driven jet engine decontamination technology which has limited operation possibilities in closed space, sensitive military establishments and areas with special explosion-proof restriction. The Hungarian Defence Forces CBRN Defence Battalion has been operating gasoline driven jet engine interior decontamination technology since 2012 but the operating experience is not satisfied. The portable fogging device a lightweight cold fogger without any electrical or gasoline driven engines are much more suitable for interior decontamination such as vehicle interiors, containers and buildings decontaminations because low volumes of the decontaminant can be spread homogeneously.

3. Figure. The FOGBOOSTER is the new generation of decontamination and disinfection fogging devices. [7]

The portable fogging device can be operated by the micro-film based on GD-6 decontamination solution which can be used on all surfaces, even penetrating cracks and detoxifies all common chemical warfare agents. Scientific experiments have proved the detoxification capability of GD-6 regarding highly toxic nerve agents Soman, VX and blister agent S-Mustard.

By using compressed air combined with a specially designed nozzle, the highly effective microscopically atomized decontamination fluid can produce a dry mist or fog. The aerosol produced by the OWR GmbH made “FOGBOOSTER” can cover the surface of a 20 feet ISO container within 90 seconds. The aerosol can sustain its stability for at least 15 minutes. The operation time of the “FOGBOOSTER” is approx. 30 minutes in its standard configuration. [8]

SUMMARY

The quick elimination of any contamination means remarkably high importance for deployed forces. Different kinds of highly sensitive equipment can be involved during the mission and in case of contamination this lack of capabilities is not easy to replace in the field which is critical for the highly sophisticated modern soldier and first responder. Therefore, the contaminated sensitive equipment needs to be decontaminated. But, most of the sensitive equipment is not chemically hardened and cannot be decontaminated using conventional wet-chemical or thermal decontamination methods. [9] The vacuum based decontamination technology is able to handle the contamination very effectively without corrosive effect concerning sensitive equipment. This kind of technology can provide safe environment to avoid cross contamination and the waste management difficulties are solved as well. The detoxification multiphase system is able to remove wide range of chemical warfare agent with high efficiency and the pressurized system is very flexible which can provide rapid response. The portable fogger is widely useable in military tasks and it is independent during operations. The main advantage of this technology is the absence of electrical or gasoline driven engines which makes it suitable for interior decontamination and it can use in highly dangerous dedicated environment.

These introduced decontamination technologies have not been the part of Hungarian Defense Force CBRN decontamination system yet but the participation in NATO Response Force rotation will require revising their deployment in the future. The vacuum based and the detoxification multiphase sensitive equipment decontamination technologies can replace the obsolete calcium hypochlorite decontamination method which is currently used by Hungarian Defense Force CBRN units. Unfortunately, the Hungarian CBRN decontamination system can not handle contamination inside the building or vehicle at present that is why establishing interior decontamination technology can mean a great achievement.

It should be noted that in the near future the new challenges to methods of decontamination of sensitive equipment together with the changes of military equipment modifications demand the modernization of combat methods and other operational activities and adequate training programmes for these new procedures. At the same time this decontamination process has to be introduced into the education. [10]

References

[1] ATP-3.8.1 volume I - CBRN Defence on Operations - January 2010

[2] Charles G. Hurst: M.D Medical Aspects of Chemical and Biological Warfare - Chapter 15 - Decontamination, http://www.sc-ems.com/ems/NuclearBiologicalChemical/MedicalAspectsofNBC, Download: December 1, 2013

[3] H. W. Herrmann, I. Henins, J. Park and G. S. Selwyn: Decontamination of chemical and biological warfare (CBW) agents using an atmospheric pressure plasma jet, http://scitation.aip.org/content/aip/journal/pop/6/5/10.1063/1.873480, Download: December 1, 2013

[4] http://www.armedforces-int.com/gallery/mobile-decontamination-system/mobile-decontamination-system-9_01.htmL, Download: December 1, 2013

[5] Hans-Joachim Toepfer and Markus Kostron: New Technologies and Decontaminants for highly mobile CBRN Decontamination Systems, http://www.nbcsec.fi/nbc/nbc2009/proceedings/TOEPFER.pdf, Download: December 1, 2013

[6] http://www.pointtrading.com/uploads/product_pdf/UP%201091%20-%20DESCRIPTION%20SX%2034%2007-04-08.pdf, Download: December 1, 2013

[7] http://www.owrgroup.net/index.php?article_id=109&clang=1, Download: December 1, 2013

[8] FOGBOOSTER - Advanced Portable Fogging Device for Decontamination, http://www.opecsystems.com/persistent/catalogue_files/products/fogbooster_v2-en.pdf Download: December 1, 2013

[9] Hans-Joachim Toepfer: Review of the optimized CB vacuum decontamination technologies, http://www.foi.se/Global/V%C3%A5ra%20tj%C3%A4nster/Konferenser%20och%20seminarier/CBW%20symposium/Proceedings/Toepfer.pdf, Download: December 1, 2013

[10] Dr. Berek Tamás: A jövő tisztjeinek ABV védelmi felkészítésének iránya az ABV jártasság követelményeinek tükrében, 2010. Hadmérnök, http://www.hadmernok.hu/2010_2_berek.php, Download: December 1, 2013

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Balajti István
balajti.istvan@uni–nke.hu

AZ IKER DRÓNOK ZAVARVÉDELME

Absztrakt

A polgári felhasználású drónok egyre több feladatot vesznek át a pilóták által vezetett társaiktól miközben új különleges elvárásoknak alacsony költségekkel tesznek eleget. Amíg a katonai alkalmazású drónok általában minden alkalmazási feladatra jól előkészített, ellenőrzött és kiegészítő eszközökkel felszerelt berendezések, polgári társaikról ez nem mondható el. Ezért kiemelt jelentőségű területnek számít a polgári drónok zavarvédelme, a zavarvédelmük növelésének kutatása és a drón fedélzeti adaptív szűrés lehetőségeinek elemzése. A drón fedélzeti adaptív szűrés hatékonysága kiterjeszthető iker drónok alkalmazásával. Iker drónok esetében adott feladat ellátására két teljesen azonos párban repülő és egy telemetriával vezérelt köteléket értek. Az elmélet megvalósítása elvárja a kötelékrepülés, ezen belül a drón-drón kommunikáció 97 GHz megvalósított WIFI típusú kapcsolatát. A tanulmány áttekinti, a hatékony adaptív szűréshez szükséges megoldásokat és szimulációs eredményeken keresztül értékeli az új, elméletileg még nem feldolgozott, műszaki megoldásokat.

Civilian drones have taken over tasks from their manned counterpart and they are creating new applications simultaneously for extraordinary surveillance capabilities at low cost. While military drones are usually well controlled, managed and equipped for all requirements, civilian drones are not. One of the biggest threats that is addressed in this article is the anti–jamming resistance of the civilian drones and a possible way for improvement, utilising adaptive filters on the drones. The adaptive filter's performances can be increased by extending solutions for the twin drone applications. The author's twin drone concept means that two drones are flying in formation and controlled by one remote station, while the two drone's on board telemetry and instruments are connected to each other through a WIFI like solution at 97 GHz. The study reviews the challenges of the twin drone anti–jamming performance improvement, and demonstrates solutions based on simulation results.

***Kulcsszavak**: iker drónok, fázisrács antenna, aktív zavarvédelem, adaptív szűrők ~ twin drone, phased array antenna ~ Electronic Counter–Countermeasures, adaptive filters*

BEVEZETŐ

Miért kerültek a polgári drónok az érdeklődés középpontjába? A katonai drónok mellett a polgári alkalmazások köre folyamatosan bővül, néhány felhasználási területen nélkülözhetetlenek, miközben áruk a tömegtermelés következtében folyamatosan csökken. Ennek következtében a polgári felhasználású drónok populációja gyorsan nő, és ezzel arányosan növekszik az irányítás alól elszabadult drónok okozta veszélyhelyzetek száma. [1]

A polgári drónok terjedésének legfőbb oka a felhasználási lehetőségek bővülése a befektetés/megtérülés értékarány drasztikus javulása. Napjainkra a fejlődés elérte azt a szintet, amikor a drónok feladatkörének bővülése lehetővé teszi és elvárja a kötelékrepülésből (iker drón koncepció) eredő előnyök kihasználását. Ezek az előnyök:

- a feladat végrehajtás biztonsága;
- az érzékelők hatótávolságának és felbontóképességének növekedése;
- az irányítás, tájékozódás valamint az érzékelők zavarvédelmi lehetőségeinek fokozása. Ez utóbbi e cikk tárgya.

A cikk első része a drónok feladataival, fedélzeti eszközeinek jellemzőivel és a leggyakoribb interferenciaforrások értékelésével foglalkozik.

A második részben a drón fedélzeti adaptív szűrés rövid elméleti áttekintése, és az iker drón fedélzeti zavarszűrés hatékonyságának szimulációs eredményekkel való szemléltetése olvasható. Foglalkozni kell a szűrési algoritmusuk feladatfüggő optimalizálásával.

A harmadik rész a kötelékrepülés megvalósításának elvárásait elemzi. Ezen belül a drón–drón kommunikáció és a hatékony adaptív szűréshez szükséges antenna pozíciók és az ezt támogató repülési formációk vizsgálata emelendő ki.

A POLGÁRI DRÓNOK FŐBB JELLEMZŐI

A polgári drónok kb. 2 óra alatt elvégezhető feladatait, fedélzeti műszerezettségét, jelentősen behatárolja a szállítható hasznos tömeg nagysága. Ez a képen látható kb. 2x2 m–es nagyságú drón esetén kb. 4 kg, mely általában a drón alsó vagy orr gondolájában található. Az 1. ábrán példaként bemutatott drón legfontosabb feladatai:

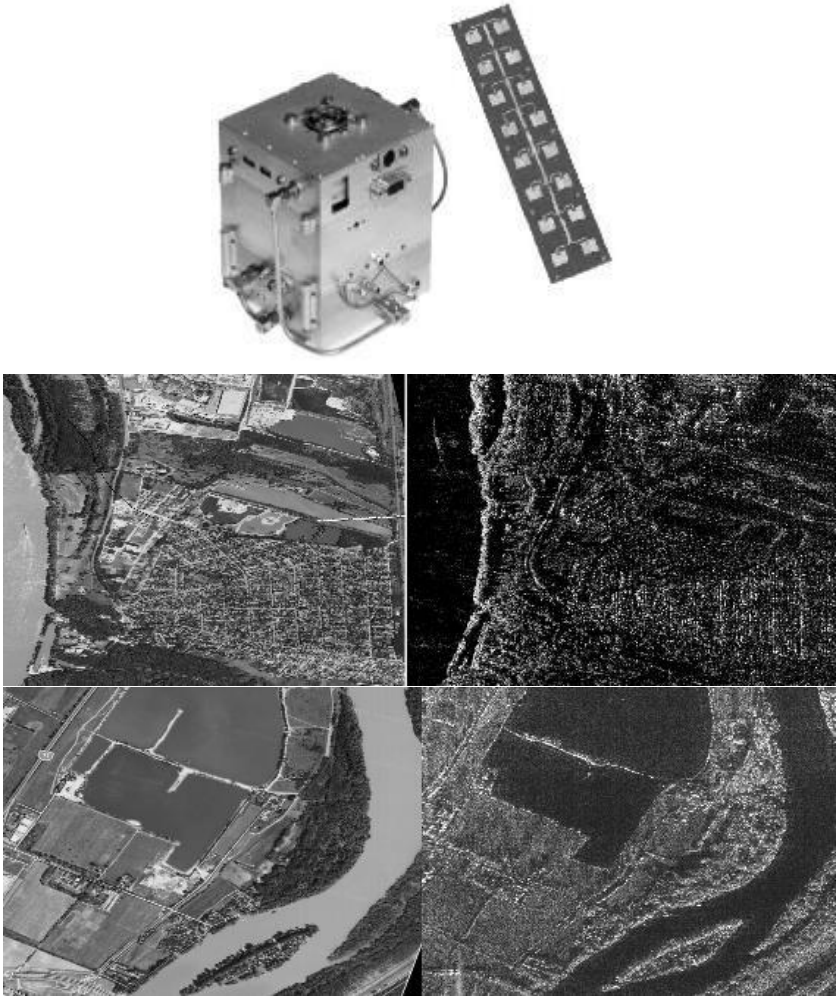
- természeti katasztrófák (földrengések, árvizek és erdőtüzek) megfigyelése, hatásuk felmérése illetve a keletkezek károk továbbterjedésének megakadályozásához szükséges információ gyors összegyűjtése;
- nagykiterjedésű logisztikai bázisok biztonságtechnikai célú monitorozása;
- agrokulturák fejlődésének és állapotának pontos felmérése;
- vadgazdálkodási feladatok optimalizálásához szükséges adatszolgáltatás;
- térképészeti és egyéb geodéziai információszolgáltatás;
- professzionális hobbi tevékenység támogatása.

1. ábra. Polgári alkalmazásra szánt drón
(UAV http://www.bonn–hungary.hu/ letöltés ideje: 2014. 11.26)

A csatolt linken megfigyelhetők az optikai rendszerek, melyek jól bevált érzékelők, kiegészülnek az infravörös tartományban éles képet szolgáltató hőkamerákkal.[2] Ez utóbbiak különösen árvizek és erdőtüzek esetén szolgáltathatnak nélkülözhetetlen, a katasztrófa elhárítást segítő információkat. Napjainkban egyre fontosabb, hogy a polgári felhasználású

drónok feladataik ellátására hatékony SAR (szintetikus apertúrájú radar) eszközökkel rendelkezzenek. Ezt szemlélteti a 2. ábra, mely az 1. ábrán látható drón fedélzet eszközkészletének része.

A kép tetején látható X–sávú SAR radar és antennája együtt kevesebb, mint 2 kg tömegű. Az alatta található baloldali képek az optikai tartományban, míg a jobb oldaliak, ugyanarról a területről, az X–sávú radarral készült SAR képek. A több mint 2 m–es felbontással rendelkező radar képeket az optikai tartományban készültekkel összehasonlítva megállapítható, hogy a vizsgált területekre jellemző, növényzet/vizek/épületek elnyelési és/vagy jel visszaverődési sajátossága, melyek fontosak a felsorolt feladatok minőségi adatainak minőségi végrehajtásához. A felbontóképesség tovább növelhető iker drónokra telepített SAR alkalmazásával.



2. ábra. Drón fedélzeti SAR (fent), SAR képek (jobb oldalt) optikai képek (bal oldalt)

A drónok elvárt hatékonysága csak a különböző műszercsoportok feladathoz optimalizált, modulárisan cserélhető alkalmazásával oldható meg. Így elérhető, hogy a műszerek rendkívül kis tömeggel és teljesítményfelvétellel rendelkezzenek, míg az érzékelők antennáinak mérete kicsi, de érzékenységük és a kapcsolódó digitális jelfeldolgozás teljesítménye nagy legyen. Ha a drón fedélzeti vevő rendszerek érzékenysége nagy, megnő a nem szándékos interferencia jelek hatása a fedezeti telemetriai, kommunikációs és érzékelő rendszerekre. A feladatok végrehajtásának további sajátossága, hogy azokat földközeli magassági tartományokban a légtér–felügyeleti rádiólokátorok céltárgy–detektálási lehetőségein kívül hajtják végre, közel a természetes (vagy mesterséges, de nem szándékos, pl. TV tornyok, GSM átjátszók, magas feszültségű távvezetékek, nagyteljesítményű transzformátorok) elektromágneses zavaró

hatásokhoz. A polgári felhasználású elektronikai eszközök közötti elektromágneses kompatibilitás törvényes előírások által szabályozott, de az elvárások betartása és betartatása körülményes, költséges és néha nem lehetséges. [3]

Egyre gyakrabban olvashatunk „csendes terek" kialakításának szükségességéről pl. iskolák, éttermék számára és az ezt lehetővé tevő zavaró eszközök piaci jelenlétéről. A 3. ábra a zavaró eszközök, mint üzleti vállalkozások keretében beszerezhető eseteket szemlélteti. A kép a polgári gyártású zavaró eszközök széles skálájának meglétére mutat rá. Megállapítható, hogy a GPS/GSM/WIFI „Anti–Jam Technology" egyre bővülő piaccal rendelkezik és a drónok fedélzetén elhelyezhető hasznos tömeg nagysága és a polgári életben gyorsan terjedő interferencia források terjedése jelentős veszélyforrás a drónok megbízható üzemeltetésére és az elvárható minőségű feladat végrehajtás kivitelezhetőségére. Bár a polgári gyártású zavaró eszközök nem tűnnek olyan veszélyesnek, mint a 10–20 kW kimenő átlagteljesítménnyel rendelkező katonai társaik, de mint látni fogjuk így is hatékonyak és rendkívül veszélyesek a drónok feladatatainak végrehajtása vonatkozásában.

3. ábra. A GPS, WIFI és GSM berendezések zavarására szolgáló polgári eszközök

A DRÓNOK ZAVARVÉDELEMÉNEK ELVÁRÁSAI

A drónok, zavarvédelem szempontjából legérzékenyebb rendszerei a telemetriai adatszolgáltatáshoz szükséges helymeghatározás, a vezérlést biztosító kommunikáció és az érzékelők vevőrendszerei. A valós idejű helymeghatározás GPS alapú, fejlettebb rendszereknél ez kiegészül a GSM tornyok nyújtotta statikus és különböző inerciális navigációs rendszerekkel.

Az adó–vevő pontok közelsége miatt, legalább 30–50 dB–lel jobb helyzetben vannak a telemetriai adatokat továbbító rádiók. A vezérlés, a telemetriai adatok továbbítása föld – levegő – föld vagy költségesebb rendszereknél (pl. az Irídium műholdak felhasználásával) föld – műhold – drón – műhold – föld – rádiókapcsolattal valósul meg.

Teljesen vegyes a kép a passzív érzékelők területén, hiszen az optikai és lézeres eszközök védettnek tűnnek aktív zavarás ellen, de az 1980–as években folytatott rendkívül sikeres HM HTI „ÁLOM" fedőnevű téma már akkor bebizonyította sebezhetőségüket. A feladat végrehajtásra használt passzív érzékelők köre magába foglalja az optikai kamerákat, videó felvevőket, a lézer távmérőket, az infravörös tartományban működő hőkamerákat. Zavarérzékenyek a különböző típusú és hullámtartományban működő radarok: magasságmérők, ütközés előrejelzők, SLAR (oldalra néző) és SAR radarok. A drón fedélzeti radarok, magasságmérők, ütközés előrejelző, SLAR/SAR radarok zavarvédelme gyártó

specifikus, hiszen értékelni kell, hogy mi a célszerűbb: felkészülni a radar (pl.: SAR) zavarvédelemére, vagy megismételni a mérést, amikor nincs interferencia a környéken?

A drónok zavarvédelmének mélyebb értékeléséhez ismernünk kell a drón fedélzetére ésszerűen telepíthető antennák, adó–vevő és jelfeldolgozó rendszerek főbb műszaki elvárásait, illetve a megvalósítás lehetőségeit, hiszen a drónok által szállított hasznos tömeg rendkívüli mértékben behatárolja az alkalmazható megoldások körét. Ennek következtében megállapítható, hogy a drón fedélzetén, a feladat végrehajtása szempontjából alkalmazható:

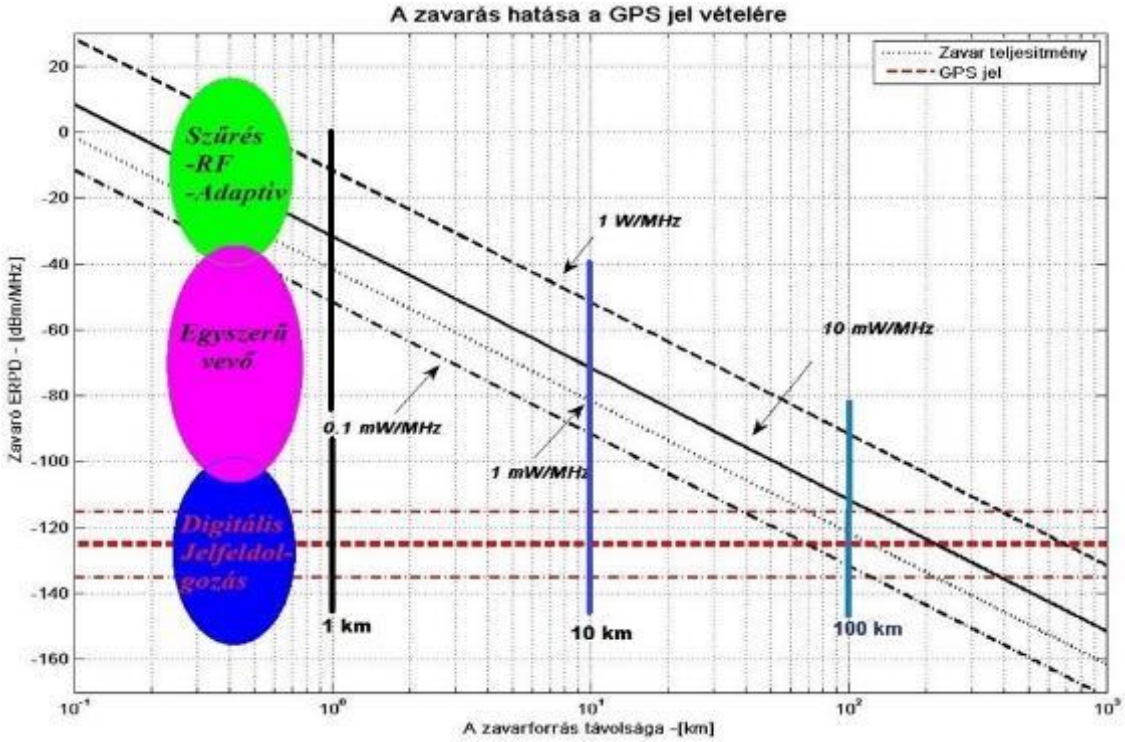
- antennák mérete elégséges minimum;
- az adóteljesítmény minimális;
- a vevőérzékenység az elérhető maximum;
- a jelfeldolgozás rendkívül korszerű, feladatorientáltan flexibilis és maximális teljesítményű legyen.

Ezért a drónok zavarvédelmi képességének értékelése és növelése napjainkra kiemelkedően fontos gazdasági–műszaki paraméter illetve a balesetek valószínűségének csökkentése miatt életvédelmi elvárás. A kérdés megválaszolásában segít a 4. ábra, ahol a rendkívül kis teljesítményű (0.0001–1 Watt) zavarforrás 100 km távolságra található a dróntól.

A drónok zavarvédelmi elvárásainak szemléltetését a polgári felhasználások területén széleskörűen elterjedt Globális Helymeghatározó Rendszer (Global Positioning System–GPS) sebezhetőségének bemutatásával célszerű kezdeni, mivel minden drón fedélzeti műszerébe beépült. Hasonló elven és műszaki paraméterekkel jellemezhetők az orosz–indiai GLONASS, az Európai Unió által fejlesztett Galileo és a kínai Beidou–2 rendszerek.

A GPS műholdak főbb polgári felhasználásra szánt műszaki jellemzői: két jogilag védett frekvencián (1227,6 MHz és 1575,42 MHz) szórt spektrumú jelet sugároznak a Föld felszíne felett kb. 3 Föld–sugárnyi (20200 km) magasságú kör alakú pályáról. A GPS műholdak polgári felhasználásra szánt kódeleme ezred másodpercenként 1023 jelet tartalmaz, míg a katonai társa 10230–at tizezred másodpercenként, melynek következtében a jel–zaj viszony jelentősen növelhető. A katonai rendszerek kihasználhatják a komplexebb kódolás feldolgozása és a hosszabb ideig fenntartható jelkorreláció nyújtotta 30–50 dB jel–zaj viszonynövekedésben rejlő előnyöket. A polgári felhasználású drónok számára is rendelkezésre áll viszont a szélessávú interferencia jelek ellen alkalmazható hatékony adaptív térbeli szűrés technológiája.

Általános esetben (4. ábra) egy GPS zavaró ERPD (Effective Radiated Power Density) Effektív Teljesítmény Sűrűsége: 0,1 mW/MHz – 1 W/MHz közötti érték. A GPS műhold műszaki paraméterei és pályája miatt a kisugárzott jel erőssége úgy van meghatározva, hogy a Föld felszínén a jelszint elérje a –125±10 dBm/MHz jelteljesítményt a 0 dB–s körpolarizált antenna kimeneten. A drónon elhelyezhető GPS antenna nyeresége általában 0–3 dB, míg az alkalmazható RF szűrők és a kiszajú előerősítők érzékenysége gyártó specifikus paraméter. GPS zavarás esetén további problémát jelent, hogy a helyzetkoordináta mérés nem egyszerre szűnik meg, hanem pontossága folyamatosan romlik (100–500 m), miközben lehetetlen lesz az új műholdakra való szinkronizálás. Eközben a rendszer újra éledési idő tovább növekedhet akár 1–2 percre. Tény, hogy a telemetriai adatszolgáltatás számítógépes hálózat kommunikáción nyugszik, mely szinten megszűnhet vagy instabillá válhat a GPS időjelek hibaszórásának növekedésével.



4. ábra. GPS jel zavarásával kapcsolatos jelszintek, jellemzők

Megoldhatatlan problémát jelent, hogy a katonai rendszerek bonyolult jelfeldolgozási és hosszabb jelintegrálási lehetőségei nem alkalmazhatók polgári rendszerekben azok nyilvánossá tétele előtt, de a dinamika tartomány növelés adaptív szűrők által sikeresen kiterjeszthető a polgári drónok zavarvédelmének fokozására is. Az elképzelések megvalósításánál, számunkra előnyös lehet, hogy a magyar légtérellenőrző rádiólokátor–rendszer jelentős tapasztalatokkal rendelkezik a korszerű zavarvédelemmel ellátott rádiólokátorok üzemeltetése területén, mely információk jelentős mértékben adaptálhatók a drónok zavarvédelmi megoldásainak kidolgozásánál. Igaz, hogy a gyakorlatban bevált megoldások katonai és üzleti okok miatt csak körültekintően dolgozhatók fel, de a többletmunka megéri, hiszen az ismeretek kritikus elemzése segíthet feltárni a polgári drónok zavarvédelme szempontjából fontos szempontokat.

ADAPTÍV ZAVARSZŰRÉS

A drónok zavarvédelmének növeléséhez döntő szempont a hatékonyság, mely elérhető korszerű szoftver rádió alapú algoritmusok nagyfrekvenciás áramkörökkel való rendszerintegrálásával. Megvizsgálva a drónok fedélzetén alkalmazható adaptív zavarszűrés lehetőségeit a megoldások a koherens jelfeldolgozások digitális megvalósításai köré csoportosíthatók. A tudományosan leggyakrabban vizsgált, az általam is kutatott esetekre az elméleti kiindulási modellekre vonatkozó egyszerűsítő megkötések az alábbiak [4]:

- rendelkezzen az interferenciaforrás (a zavar forrás) pontszerű térbeli helyzettel és fehérzajhoz hasonló teljesítmény sűrűségű spektrummal;
- legyen a zavar forrás jele az antennabemeneteken erősen korrelált;
- a zavaróadó és a drón/drónok mozgásából származó Doppler–frekvenciacsúszások automatikusan kiegyenlítődjenek (gaussi bistatikus Doppler);
- az iránymérés felbontása legyen olyan nagy, hogy ne befolyásolja az adaptív zavarelnyomás hatékonyságát.

Az antennarács technológia elméletéből következik, hogy a koherens antennanyaláb előállítás elvárásainak betartásával, több antennarács csoport alakítható ki egy nagy

antennarácson belül, illetve tetszőleges számú antennarács helyezhető egymás mellé. Az antennák geometriai elhelyezése, a „kiterjesztett apertúra” alkalmazásfüggő és optimalizálása az antenna nyereség valamint az adás–vételi irány karakterisztika elvárásaihoz igazodik. Az iker drónokra szerelhető antennák (általános esetben fázisrács antennák) legfontosabb jellemzői és sajátosságai az apertúra amplitúdó és fáziseloszlás függvényeiből kiindulva az FFT (Fast Fourier Transformation – Gyors Fourier Transzformáció) térbeli hullámokra történő alkalmazásával számított iránykarakterisztikákon keresztül vizsgálható.

A rendszer által determinált jel[1] a lineáris (ekvidisztáns) antennarácson (Uniform Linear Array –ULA) „n” szerint mintavételezve számítható. Iker antennarács esetén, 5. ábra, az adási irány karakterisztika kialakítása két teljesen azonos (R_1 és R_2) antenna fázis és amplitúdó eloszlásfüggvényeiből és a köztük lévő, iker alkalmazás esetén néhányszor tíz méteres távolság által meghatározott eloszlásfüggvénnyel történik. Az antennák kimenetén megjelenő jelek az (1) és (2) egyenletek szerint számíthatók. Adaptív zavarszűrés esetén a különböző irányokból érkező interferencia jelek fázis– és amplitúdói a (3) szerint csökkenthetők. [5]

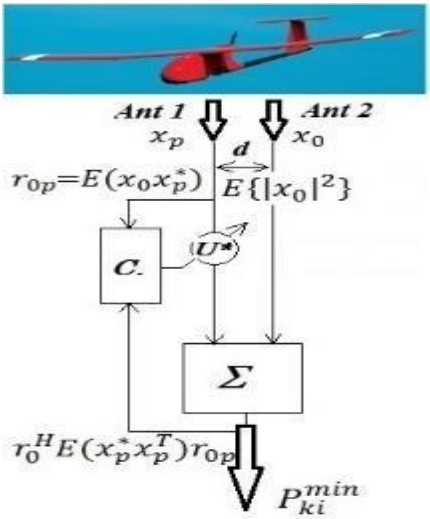
Az 5. ábra egy drón fedélzeti GPS, rádiókommunikációs és radar rendszereinek adaptív térbeli zavar szűrésének általános elvét szemlélteti. A megoldás előnye az egyszerűen kivitelezhető jelstabilitás növelés, hátránya viszont, hogy meg kell duplázni a drónra szerelt vételi antennák és RF egységek számát.

Zavarviszonyok között a főcsatornában mintavételezett jel $x_0 = x(n)$ [6]:

$$x(n) = \sqrt{M}v(\phi)s(n) + w(n) \qquad (1)$$

Ahol:

- $v(\phi) = \frac{1}{\sqrt{M}}\left[1 \;\; e^{-jk_o dsin(\phi)} \ldots e^{-jk_o dsin(\phi)(M-1)}\right]^T$ – antenna irányvektor;
- Φ – a keskenysávú jel iránya, ($-\pi/2 < \phi < +\pi/2$);
- $1/\sqrt{M}$ – M antenna elemszám,√– a számítási műveletek egyszerűsítésére;
- $d \leq \lambda_o/2$ – a szomszédos antenna elemek közötti távolság;
- k_o – térhullámok esetén értelmezett hosszegységre eső hullámszám, analógiája, az időegységre eső hullámszám;
- $w(n)$ – a vevőrendszer zajhőmérséklet vektora (korrelálatlannak tekintjük, ezért a mintavételezés „n” előtti szűrők átfedéseiből és az érzékelő elemek kölcsönös egymásra hatásából eredő ideiglenes korreláció értéke elhanyagolható);
- $s(n)$ – a vett keskenysávú jel vektora.



5. ábra. Adaptív térbeli szűrésen alapuló drón zavarvédelem

[1] Lásd részletek MATLAB Phase Array Toolbox

Ennek analógiájára a segédantennán (vagy al–antennarács csoporton) vett jel:

$$x_p(n) = s(n)v(\Phi_o) + \sum_{p=1}^{P} i_p v(\Phi_p) + w(n) \qquad (2)$$

Ahol:

- $s(n)$ – értéke legalább 20–30 dB–lel (oldalnyaláb szint) kisebb**,** mint a főcsatornában;
- i_p – interferencia (zajzavar) erőssége Φ_p irányában;
- $v(\Phi_o)$ és $v(\Phi_p)$ – az interferencia iránya a „*o*" fő és a „*p"* segédantennához viszonyítva.

Az adaptív szűrő kimenetén mérhető jelteljesítmény:

$$P_{ki}^{min} = E\{|x_0|^2\} - r_0^H R_p^{-1} r_{0p} = E\{|x_0|^2\} - r_0^H E(x_p^* x_p^T) r_{0p} \qquad (3)$$

Ahol:

- $E\{|x_0|^2\}$ – a főcsatorna bemenetén mérhető interferencia és vevőzaj teljesítmény;
- r_0^H– a főcsatorna bemenetén mérhető interferencia és vevőzaj kovariancia (kereszt–korreláció) Hermitant–mátrix;
- $R_p^{-1} = E(x_p^* x_p^T)$– a szűrő kimenetén mért interferencia és vevőzaj kovariancia (korrelációs) mátrix, $E(\cdot)$ – statisztikai elvárás, * komplex konjugált, x_p^T– transzpóz vektora x_p–nek;
- $r_{0p} = E(x_0 x_p^*)$ – statisztikai mátrix kapcsolat a fő– és a segédcsatorna bemenetén mérhető interferencia (+vevőzaj) kovariancia (kereszt–korreláció) között. A főcsatorna bemenetén $\rho_{00} = 1$. Általános esetben:

$$r_{0p} = \begin{vmatrix} 1 & \dot{\rho}_{01} & \dot{\rho}_{02} & . & \dot{\rho}_{0(P-1)} \\ \dot{\rho}_{10}^* & 1 & \dot{\rho}_{12} & . & \dot{\rho}_{1(P-1)} \\ \dot{\rho}_{20}^* & \dot{\rho}_{21}^* & 1 & . & . \\ . & . & . & 1 & . \\ \dot{\rho}_{(P-1)0}^* & \dot{\rho}_{(P-1)1}^* & \dot{\rho}_{(P-1)2}^* & . & 1 \end{vmatrix} \qquad (4)$$

Megjegyzés: A (4) egyenletnek csak akkor van megoldása, ha a zavaró jelforrások száma kevesebb, mint a segédcsatornák száma.

A zavarelnyomási tényező *(„K_z")* (Jammer Cancellation Ratio – JCR) a vizsgált rendszer bemeneti és kimeneti jelteljesítményeinek arányából származtatható [7]:

$$K_z = \frac{P_{be}}{P_{ki}^{min}} = \frac{E\{|x_0|^2\}}{E\{|x_0|^2\} - r_0^H R_p^{-1} r_{0p}} \qquad (5)$$

Legegyszerűbb esetben *p=1*, – csak egy segédcsatorna aktív.

$$K_z = {}^{1}/_{(1 - r_{01}^2)} \qquad (6)$$

Ahol: $r_{01} = E\{|x_0 x_1^*|^2\} = \left(\left|\overline{\dot{U}_{be0} \dot{U}_{be1}^*}\right|\right) / \sqrt{\overline{\left|\dot{U}_{be0}\right|^2 \left|\dot{U}_{be1}\right|^2}}$ – a fő– és segédcsatorna bemenete között számított zajzavar keresztkorreláció.

Megjegyzés: a korrelációs mátrix ergodikus folyamatok esetén pontosan számítható a megvalósítás időállandójával, de a valós mérési környezet csak véges darabszámú mintavektor előállítását teszi lehetővé. Ezért véges dimenziójú autókorrelációs mátrixból kell megbecsülni a térbeli spektrum értékét, mely több szempontból is korlátozott.

A zavarelnyomás hatékonyságát meghatározó tényezők

A korrelációt romboló legfontosabb összetevők [8]:

1. *A fő– és a referenciacsatornák jelkésleltetés különbsége:*

$$\partial\tau \leq {}^{1}/_{2B_n\sqrt{K_z}} \qquad (7)$$

Ha a vevő sávszélessége Bn=5 MHz és Kz= 40 dB, akkor $\partial\tau \leq$ 10–9s.

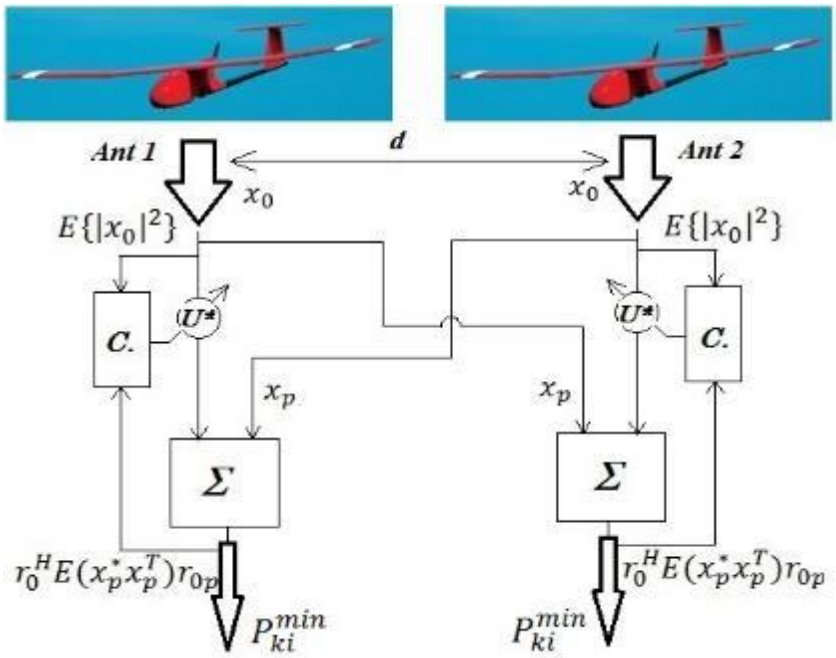
2. *A segédcsatornák érzékenysége:* Alapvetően a fő– és a segédcsatornák bementén mért zavarteljesítmény és saját zajteljesítmények korrelációromboló értéke határozza meg. Elvárás, hogy a segédcsatornák érzékenysége elérje a főcsatorna érzékenységét. A korreláció fenntartása érdekében azonosak a fő– és segédcsatornák RF szűrői, kábelezése, kis zajú erősítői, keverői és analóg digitális átalakítói.
3. *A segédantenna erősítési tényezője:* Rádiólokátorok esetén a főantenna vételi oldalnyaláb szintjeinél nagyobb és magas keresztkorrelációs értéket kell biztosítania, melyet a zajzavar–teljesítmény egységnyi antennaerősítéséhez viszonyított értéke behatárol. Ideális esetben értéke megegyezik a főnyalábéval, mely elvárás iker rádiólokátor koncepció esetén teljesül.
4. *A segédantennák iránykarakterisztikájára vonatkozó elvárás:* A segédantenna irány karakterisztika amplitúdó– és/vagy fázisközéppontja különbözzön a főantennáétól. Ez az elvárás hasonló a monopulzusos iránymérés elvárásaihoz, de ez esetben a segédantenna fázisközéppontjának elmozdítása a jelkésleltetésre vonatkozó követelményt (7) rontja: $\partial\tau_{FázisKözp} = dcos\Phi/c$, ahol: d – a két antenna fázisközéppont közötti távolság.
5. *Az adaptivitás sebességére* vonatkozó követelmény: Az elvárt hasznos jelre (radarok esetén a saját adójelére) nem szabad reagálnia, viszont a zajzavar változásait időben adaptívan követnie kell. Radarok esetén a megvalósításhoz általában az impulzus kompresszió kimenetén megjelenő jel sávszélességét 2–3 szorosára csökkentik, annak figyelembe vételével, hogy így is jelentősen nagyobb legyen a zavarójel sávszélességénél.

A (6) egyenlet szerint az adaptív szűrés hatékonysága csökken az interferenciajelek korrelációjának csökkenésével. Leggyakrabban ez az eset akkor fordul elő, ha a fehérzajszerű nagy kitöltési tényezővel rendelkező zavarójelek változó teljesítményű impulzusokkal keverednek. Az ilyen típusú zavarás elleni védelem, kombinált SLB (Side Lobe Blanking) / SLC (Side Lobe Cancellation) technológia alkalmazását várja el, mely napjainkra már beépült néhány korszerű rádiólokátorba.

AZ ADAPTÍV ZAVARELNYOMÁS DRÓNFEDÉLZETI MEGVALÓSÍTÁSA

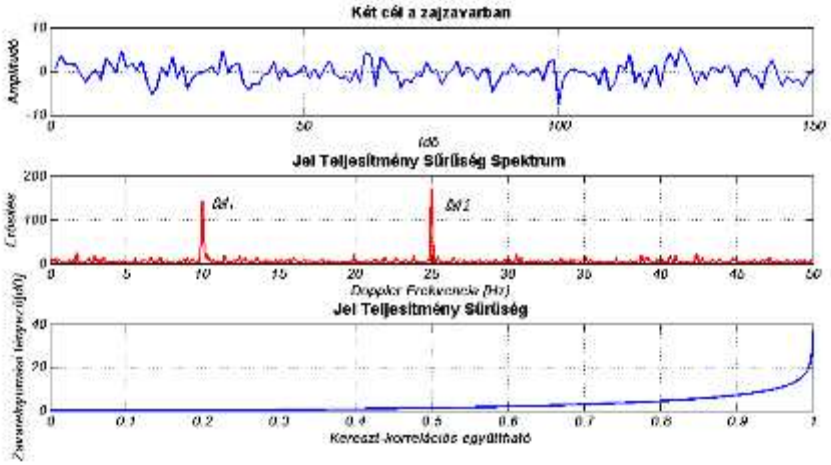
A 6. ábra az iker drón koncepció fedélzeti GPS, rádiókommunikációs és radar rendszereinek adaptív térbeli szűrésen alapuló általánosan alkalmazható, kiterjesztett képességekkel rendelkező zavarvédelmének vázlata. Ez a koncepció az adaptív szűrők hatásfokának javítására további elvi és gyakorlati lehetőségeket kínál. A megoldás előnye, hogy jelentősen kiterjeszti az egy drónra szerelt érzékelő egységek performanciáját. Hátrány viszont a drónok közötti jelstabilitás megoldásának és a bonyolultabb adaptív algoritmusok megvalósításának költsége.

A zavarvédelmi lehetőségek közül kiemelendő a vételi antennák főnyaláb védelme. Ez egy olyan adaptív szűrő, ahol a bemeneti jeleket, a fő és a kisegítő csatornák számára elvben teljesen azonos antennák szolgáltatják. Mivel az antennák erősítése, minden irányban nagyon hasonló, az adójel spektruma pontosan ismert, a zavaró adók iránya nagy pontossággal adaptívan meghatározható és az általuk injektált interferenciák (pl. doppler sebessége, mely ez esetben 10 és 25 Hz) nagy zavarelnyomással csökkenthetők.



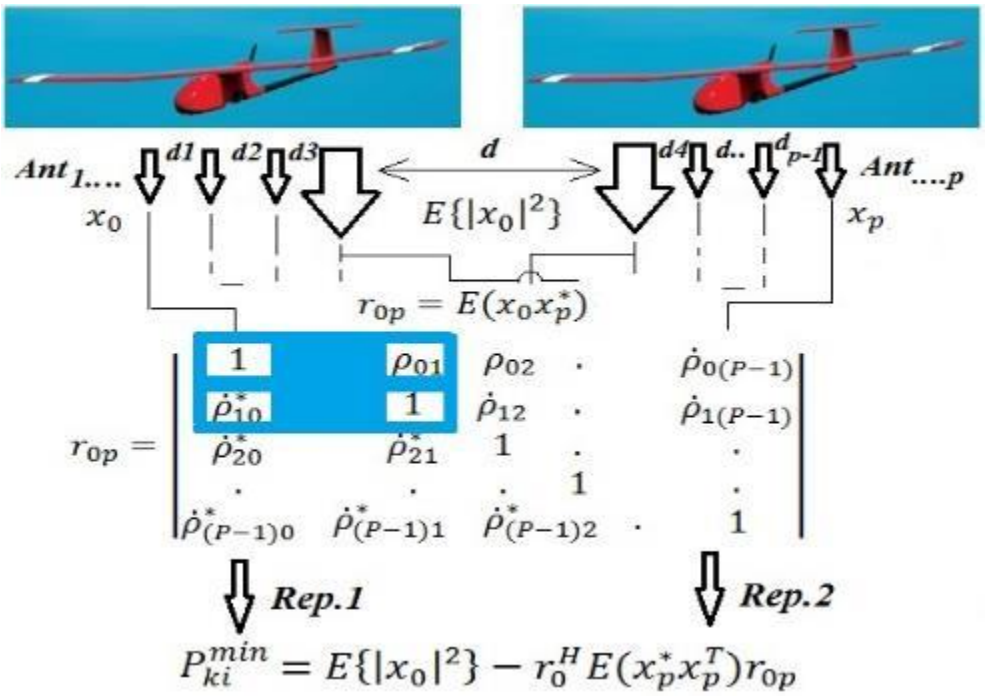
6. ábra. Iker drónokkal megvalósítható kiterjesztett zavarvédelem

A 7. ábra szemlélteti az egyszerű keresztkorrelációt kihasználó zavarszűrés hatékonyságát. Az iker drónok R_1 és R_2 főantennáin megjelenő jel normál eloszlású zajzavar, melyben a két céljel ugyanabban a távolsági cellában található és radiális sebességük eltér egymástól. Így a két cél Doppler–frekvenciája FFT–vel számítható, melyet az ábra középső része szemléltet. Ez esetben is a zavarelnyomási tényező hatékonyságát a keresztkorreláció értéke határozza meg. Az ábra alsó része a zavarelnyomási tényező keresztkorrelációs tényezőtől való függését mutatja. Mivel a korrelációs tényező („ρ”) a vizsgált rendszer bemeneti és kimeneti jelteljesítményeinek arányából származtatható (5), egy adott, pl. K= 20 dB zavar elnyomási érték eléréséhez ρ=0.99 korrelációs érték realizálása szükséges, mely már a 70–es, 80–as évek technológiai szintjén is elérhető volt. A 40 dB zavarelnyomási érték eléréséhez ρ =0.9999 korrelációs érték realizálása az elvárás, mely még napjaink technológiai lehetőségei tükrében is komoly kihívás.



7. ábra. Főcsatorna–védelem és a keresztkorreláció kapcsolata

A 8. ábra az iker drón zavarvédelem kiterjesztése sokcsatornás üzemmódra, a hozzá tartozó keresztkorrelációs mátrixszal. Ez utóbbi a zavarelnyomást legjobban befolyásoló, korrelációs együttható, csatornák közötti komplex konjugált értékeit tartalmazza. [9]



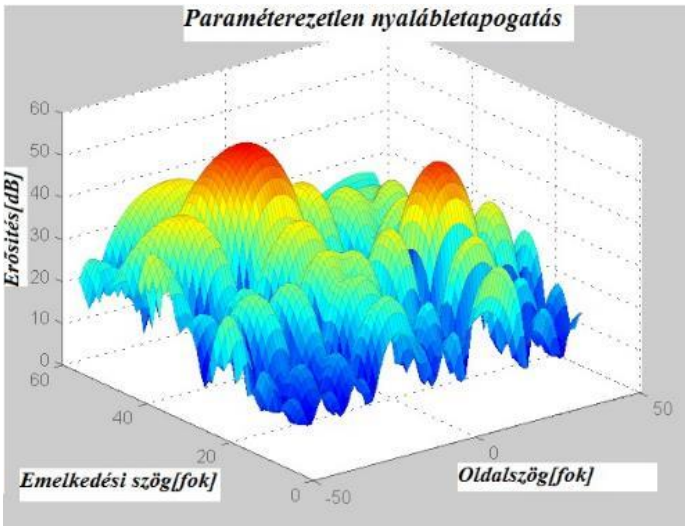
8. ábra. Az adaptív szűrők alkalmazásának szabadságfoka megnő

Általános esetben az elemi sugárzók egymáshoz viszonyított távolsága eltérő és változó, hiszen a két drón egymáshoz viszonyított helyzetének ingadozása befolyásolja. Az eltérő antenna fázisközéppontok miatt a számítások bonyolultsága a sugárzók számának négyzetével nő. A számítási igény csökkentése érdekében célszerű behatárolni az elemi sugárzók egymáshoz viszonyított távolságát és lehetőség szerint rögzíteni azt.

A ZAVARELNYOMÁS HATÉKONYSÁGÁNAK SZÖGFELBONTÁS FÜGGÉSE

A tanulmány elején elvárást fogalmaztunk meg az iránymérés felbontására, melyet gyakran nem lehet teljesíteni a drónokra szerelhető antennarendszerek méretei miatt. A lehetőségeket viszont célszerű felmérni. A 9. és 10. ábrák az iránymérési szögfelbontás fontosságát egy szimulációs példán keresztül mutatják be. A 1,227 GHz védett frekvencián üzemelő GPS antenna URA[2] (4x2 elemű) 0,08 és 0.16 m elemtávolsággal rendelkezik vízszintes és függőleges síkban. Legyen a drónokhoz viszonyított ismeretlen zavaradók iránya (–15º, 45º), (20º, 25º), és (–13º, 43º) oldalszögben és helyszögben. Az antennarács bemenetén a zavarójel erőséggé 0.01 watt.

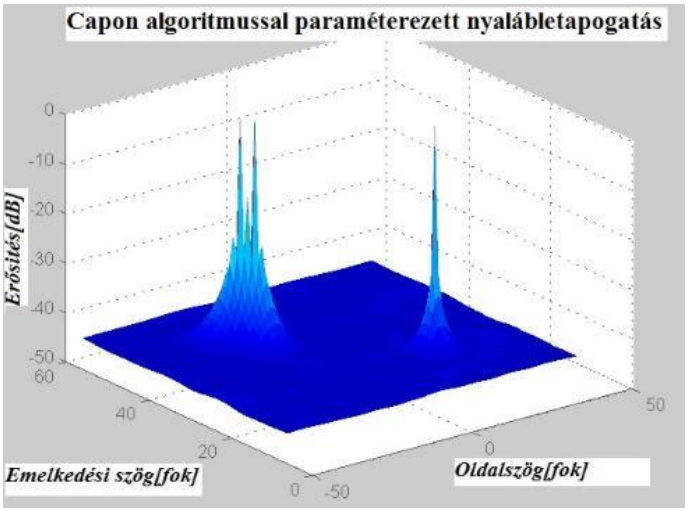
[2] URA (Uniform Rectangular Array), lásd további részletek: MATLAB Direction of Arrival Estimation with Beamscan and MVDR (Letöltés ideje: 2013. 10. 12)



9. ábra. Hagyományos FFT–alkalmazó térletapogatás esetén elérhető szögfelbontása

A feladat a zavarójelek irányának minél pontosabb megállapítása, majd a zavarójelek kompenzálása. Mivel a zavarójelek hatékony kompenzálása a zavarójel irányának pontos ismeretén alapszik a lehetőségek felmérésére összehasonlításra kerül a hagyományos FFT–alkalmazó térletapogatás és a pontosabb iránymérést lehetővé tevő Capon–módszer (algoritmus)[3]. A 9. ábra bal felső részén mutatott elméleti jelszintek szerint az egymáshoz közeli irányokban a hagyományos FFT–alkalmazó becslés bizonytalansága még nagy. Ez esetben a zavaró jelek a főnyaláb szélességén belül vannak, (–15º, 45º) és (–13º, 43º) irányban. A zavarelnyomás még akkor is problematikus a kis értékű SINR miatt, ha a zavarók egymáshoz viszonyítva távolsága nagy (–15º, 45º), (20º, 25º).

Megoldást jelenthet a számítástechnikailag bonyolultabb és némileg költségesebben megvalósítható Capon iránymérési algoritmus alkalmazása. (További 10 – 16 hasonló hatásfokkal rendelkező algoritmus ismert, így ennek bemutatásán keresztül értékelhető a többi algoritmus is.) Ennek segítségével az egymáshoz közeli zavarforrások iránya becsülhető és a zavarelnyomás növeléséhez szükséges SINR érték is nő. Ezt szemlélteti a 10. ábra.



10. ábra. Paraméterezett nyalábletapogatás szögfelbontása

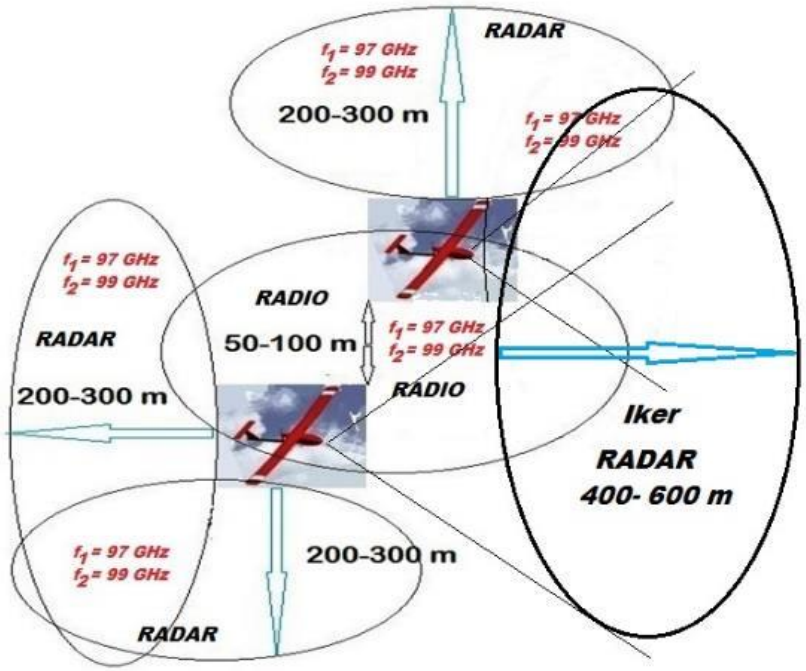
[3] A Capon–módszer sajátosságainak elemzése megtalálható [4]–ben.

Fontos kiemelni, hogy az iker drónok fedélzeti antennáinak összekapcsolásával az antennák egymáshoz viszonyított megnövekedett távolsága, a nagyobb bázisvonal távolság miatt, lehetőséget ad az iránymérés és a szögfelbontás további növelésére. [9]

Az iker drón antennastruktúra legnagyobb kihívása az egymás közelében települő rendszerelemek egymásra hatásának szabályozásában van. Az „in situ" mérések eredményeként megvalósulhat a különböző reflexiók, az antenna elemek mozgása, rezgéséből eredő hullámterjedés változás folyamatos értékelése, a drónok egymáshoz viszonyított mozgásából származtatott állapot hibák csökkentése. Ezzel növelhető a korrelációjavító eljárások/eszközök pontossága, a különböző antennarácsok egymáshoz viszonyított fázisviszonyainak, illetve az üzemszerű működés során beálló változások pontos mérése és adaptív korrigálása.

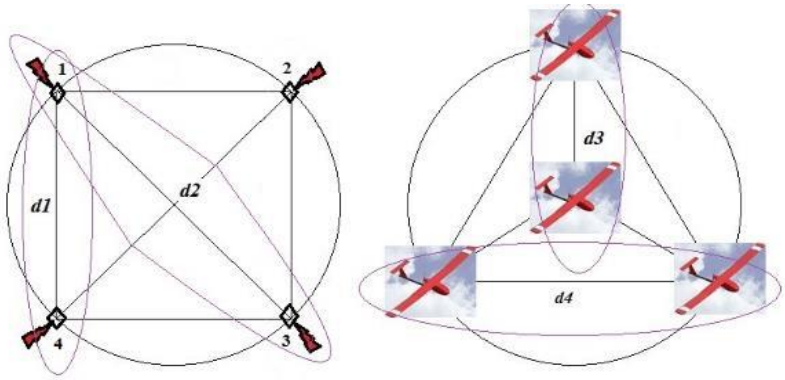
Kézenfekvő elvárás, hogy a drón felületére helyezett antennastruktúra és a kötelék repülés formációja támogassa a rendszertechnikai megoldásokat. Ilyen feladat a két drón közötti olyan adatforgalom repülés közbeni biztosítása, mellyel maximalizálható a rendszer koherens jelfeldolgozási tényezője. A 11. ábrán bemutatott megoldás a kötelék repülés kivitelezéséhez nélkülözhetetlen telemetriai adatcserét is lehetővé teszi. A gyakorlatban is megvalósítható repülési formáció szerint egy központi drónhoz maximum 2x3 drón csatlakoztatható kiterjesztett iker drón (kötelékrepülés) üzemmódban, hiszen a két drón egymáshoz képest 6 lehetséges térrész valamelyikében maximálisa 50–100 m távolságon belül foglal pozíciót. A közöttük kiépülő megbízható telemetriai és a vételi csatornák, a keresztkorrelációs tényező maximalizálása érdekében 100 GHz környékén pl. 97 és 99 GHz frekvencián párhuzamosan üzemelnek. Ezek a vivőfrekvenciák több mint 10–szeresei a drónok által használt kommunikációs és radar antennák működési értékeinek így megoldható a drón kötelék zavarvédelméhez szükséges jelek amplitúdó és fázishelyes átvitele.

A drónok szárnyvégein, az orrgondolában és a hátsó térrész irányába néző antennák felhasználhatók a 100 GHz–es frekvencián üzemelő térrész figyelő radarok antennáiként, így a drónok környezete a tér minden irányában megfigyelhető. A 12. ábra az antennák lehetséges elhelyezését szemlélteti a rádiók és a radarok számára. A drón fedélzeti iker radarok következtében a drónok előterében a rádiólokációs mező kiterjesztése megduplázódik. [10]



11. ábra. Kötelékrepülésre felkészített drón többfrekvenciás adatkapcsolata

A 12. ábra az általam preferált, négyzet és háromszög, ikerrepülési formációkat szemléltet.



12. ábra. Iker drón antennastruktúra és/vagy kötelékrepülési formáció

IKER DRÓN ZAVARVÉDELEM MEGVALÓSÍTÁSÁNAK TECHNOLÓGIAI ELVÁRÁSAI

Korunk technológiai színvonalán a régi katonai rendszerekben alkalmazott analóg megoldásokhoz képest újszerű RF szűrőkhöz integrált digitális jelfeldolgozással, már a polgári alkalmazású drónok is magas jel–keresztkorreláció értékekkel számolnak. Ennek okai:

- a műveleti pontosság független az alkatrészek értékének változásától;
- a nagyon nagy sebességű grafikai processzorok, az FPGA (Field Programmable Gate Array – programozható logikai kapukat tartalmazó hálózat) és DSP (Digital Signal Processor – digitális jelfeldolgozó egység) áramkörök flexibilis, könnyen átprogramozható jelfeldolgozók;
- aránylag könnyű (ha rendelkezésre áll a megfelelő tudás) a feladatok változásához alkalmazkodó, adaptív programok készítése, és a drón fedélzeti adaptív szűrőkbe történő adaptálása a számítási algoritmusok párhuzamosításával;
- a WIFI és LAN (Local Area Network –helyi–számítógépes, hálózat) hálózat beépített nagysebességű rutinjai is kiaknázhatók – pl. az adattömörítés, az adattovábbítás területén;
- az „I” and „Q” csatornák üzemmód függő illeszttetésével, a fázisfutási problémák megoldhatók, mivel a csatornák közötti együttfutás és a csatornák linearitása az elvárásokhoz igazítható;
- a dinamika, sávszélesség és a mintavételezés szükség szerinti, a 18 hónaponként megduplázódó számítástechnikai kapacitásokhoz igazodva, szükség szerint művelhető;
- 2^{16} bittartományon belül extrém nagy követelmények is teljesíthetők a szűrőkarakterisztikák linearitása, a fázis és amplitúdó elvárásaira vonatkozóan;
- az eredmények tetszőleges pontossággal reprodukálhatók;
- a legújabb kutatási eredményeknek megfelelő, folyamatosan javított korszerű algoritmusok aránylag egyszerűen és gyorsan adaptálhatók a meglévő rendszerekbe.

Az iker drónok egymáshoz viszonyított mozgásából, az antennák rezgéséből származó veszteségek csökkentése az elvárt jeltisztaság biztosítása elvárja különleges adójel struktúrák használatát úgy az adatkommunikációs jelutak, mint a radarok adójel struktúrájában. Ezek az adójel struktúrák, azon kívül, hogy maximalizálják az impulzus kompressziós szűrőkkel elérhető jel–zaj viszonyt és a bizonytalansági függvényük feladat specifikusan optimalizálható,

biztosítják a fáziscsúszások, a többszörös hullámterjedés, a hullámterjedési rendellenességek és reflexiók pontos mérését.

További megoldásra váró műszaki feladatok:

- az antennaelemek hatásfokának növelése 1.5–2 dB– lel, a parazita kölcsönhatások csökkentése, pl. speciálisan erre a feladatra kidolgozott vékony műanyag fémbevonatokkal;
- az antenna talpponti ellenállás az antenna irányától függően, antenna /– környezet/– felszín /– időjárási környezet/– antenna visszacsatolás következtében változik, mérések szerint 36–64 Ohm között. Ennek kompenzálása növelheti a hullámterjedési viszonyok kiaknázhatóságát;
- különlegesen hatékony adaptív fő– és oldalnyaláb elnyomó algoritmusok/rendszerek kidolgozása, mely a kombinált nagy kitöltési tényezővel rendelkező zajzavarhoz kevert nagyteljesítményű impulzus zavarok ellen is hatékony;
- az iker drónkoncepció flexibilisen változó teljesítményű adórendszereinek feladatra optimalizált kialakítása.

Jövőbeli kutatási terület a gráfelmélet eredményeinek rendszeradaptációja, hiszen természetes elvárás, hogy az antennák helyzetét az iker drónok repülési formációi feladat specifikusan támogassák.

Mivel az iker rendszerek zavarelnyomása a helyzethez flexibilisen alkalmazott algoritmus–struktúra és a jelfeldolgozást általában jellemző folyamatok nem gaussi normál eloszlásfüggvény szerintiek, ezért ígéretes a „Particle” szűrők nem gaussi normál eloszlásfüggvényre optimalizált algoritmus változatainak rendszerbe integrálása.

Az iker rádiólokáció lehetőségeit is kiterjeszti az iker drónok zavarvédelmi képességeinek növekedése, hiszen kiterjeszti a levegőből történő aktív/passzív rádiólokáció nyújtotta lehetőségeket.

ÖSSZEFOGLALÁS

A polgári felhasználású drónok feladatköre folyamatosan bővül. Az új feladatok ellátásához szükség van a fedélzeten elhelyezhető hasznos műszerpark növelésére. A tanulmány bemutatja, hogy iker drónok alkalmazásával megduplázhatók az adott feladat teljesítésére rendelhető fedélzeti műszerek száma, ugyanakkor közvetlen adatkapcsolattal rendelkező új műszaki elgondolások megvalósítása kiterjesztheti az egy időben elvégezhető feladatok körét, illetve javíthatja a meg lévő feladatok végrehajthatóságának minőségét.

Bizonyításra kerül, hogy a polgári drónok rendkívül érzékenyek a zavarásra, így alkalmazhatóságukat behatárolja a környezetünkben egyre jelentősebb mértékben jelenlévő interferencia, mely ronthatja a mérések eredményét, és a telemetriai adatforgalom megbízhatóságának csökkenésével baleseti tényezővé, repülésbiztonsági kérdéssé teszi a drón fedélzeti zavarvédelmi eljárásokat. [11]

A tanulmányban a drónok zavarvédelmével kapcsolatos tények és a leghatékonyabb drón fedélzeti adaptív szűrési eljárások rövid elméleti áttekintése kiegészül az iker drón fedélzeti zavarszűrés hatékonyságának szimulációs eredményekkel való szemléltetésével.

A drónok zavarvédelmi performanciáját az antenna rendszer, mint térbeli szűrő alapvetően befolyásolja. Az antennák geometriai elhelyezése, a „kiterjesztett apertúra” alkalmazásfüggő, az antennanyereség valamint az adás–vételi irány karakterisztika elvárásaihoz igazodik.

Megállapításra kerül, hogy a rendszer performanciák növelhetők az iker drónok fedélzetén található antennák topológiájának megválasztásával. A zavarszűrés leghatékonyabb megoldásai szoftver központúak, ahol a csúcstechnológiát képviselő RF sávszűrés, a nagy dinamika és jelkorreláció nyújtotta lehetőségeket is ki kell használni, még a legegyszerűbb egy drón fedélzeten alkalmazandó adaptív zavarszűrés esetén is.

Felhasznált irodalom

[1] SZABÓ S. A.: UAV (Pilóta Nélküli Légi jármű) műveletek humán tényezőinek elemzése repülésbiztonsági szempontból, Repüléstudományi Közlemények, Repüléstudományi Konferencia 2013, XXV. évf. 2013 2. szám. (http://www.szrfk.hu/rtk/kulonszamok/2013_cikkek/2013–2–36–Szabo_Sandor_Andras.pdf (Letöltés ideje: 2014. január 19.)

[2] SOLYMOSI J. – BHE Ltd– UAV(robotrepülő) előadás, Vác, 2012 Október. http://www.youtube.com/watch?v=B2DMJaeArj8 (Letöltés ideje: 2014. január 19.)

[3] PADOS L.: A digitális hozadék sáv felhasználásának szabályozása, 2013. augusztus 22, http://bme.videotorium.hu/hu/recordings/details/6793,A_digitalis_hozadek_sav_felhasznalasanak_szabalyozasa_a_valtozasok_kovetkezmenyeidmenyhirdetese (Letöltés ideje: 2014. január 19.)

[4] SELLER R.: Módszerek céltárgyparaméterek rádiólokációs mérési pontosságának növelésére, Egyetemi doktori értekezés, BME, Budapest 1996.

[5] BALAJTI I., VASS S .: Az elektronikai védelem alapjai, ZMNE, 2000, Budapest, 72. p.

[6] MANOLAKIS, D.G., INGLE, V. K., KOGON, S. M. (2005): Statistical and adaptive signal processing. London, Artech House. 796 p. ISBN 1–58053–610–7

[7] SKOLNIK, Merrill I. (2008): Radar handbook. 3rd ed. New York, McGraw–Hill, Chapter 6.

[8] BONDARENKO, B. F. (pod red.) (1987): Osznovü posztroenija RLSZ. Kiev, KVIRTU PVO

[9] CHERNYAK, Victor S. (1998): Fundamentals of multisite radar systems. Amsterdam, Gordon & Breach Science Publ. 475 p. ISBN 90–5699–165–5

[10] BALAJTI I. Short Study on Performances of Air Surveillance Augmented by Twin Radars, In AARMS, 2014, (kiadás alatt)

[11] VÁNYA L.: Hogyan védekezzünk a drónok ellen? Repüléstudományi Közlemények XXV. évf. 2013/2. szám. 255–261. pp

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Cser Orsolya

PÉNZÜGYI BIZTONSÁG ÉS KIBERBIZTONSÁG A BANKI RENDSZEREK TERÜLETÉN

Absztrakt

A biztonság az egyik legalapvetőbb emberi szükséglet, amely sohasem önmagában, hanem mindig a veszélyhelyzetre történő reagálásként jelenik meg. Egy állam belső biztonságát jelenti a politikai, társadalmi, gazdasági rend megóvása, a veszélyek elhárítása, mint például a gazdasági terrorizmus eszköze, a kibertámadás. A modern hadviselés egyik legfontosabb színtere a kibertér. Ennek támadása a banki rendszerek esetében fontossá tette azt, hogy az informatikai rendszerek a lehető leginkább biztonságos módon kerüljenek kialakításra a szervezeten kívül és belül. A pénzügyi szolgáltatási tevékenység csak a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg, illetve folytatható. Ennek érdekében a jövőre vonatkozóan érdemes kidolgozni egy olyan gyakorlati szabályozást – a többféle területen használt Legjobb Gyakorlatok (Best Practises) módszerével -, amely által a pénzügyi szervek (bankszektor) összehangoltan és azonnali reagálással képesek fellépni az őket ért támadások ellen.

Security is one of the most basic human needs, which is never alone, but always in the emergency response as shown. Internal security of a state is the political, social and economic order to preserve or eliminate hazards, such as instrument of economic terrorism, cyber attack. Cyberspace is a major arena of modern warfare. This attack has made it important for the banking system, the IT systems in the most secure manner are developed inside and outside the organization. Financial service activities must be initiated in the event of an intention to information and control systems to reduce operational risks and to manage emergency situations or continued. To this end, you may want to develop a practical scheme for the future - in a number of ways for Best Practices (Best Practises) method - which is coordinated by the financial authorities (banking) and are capable of immediate response to counteract the attacks against them.

Kulcsszavak: *kibertámadás, informatikai rendszer, elektronikus szolgáltatás, bankbiztonság ~ cyber attack, IT system, electronic service, bank security*

A BIZTONSÁG ÉS A KRITIKUS INFRASTRUKTÚRÁK

A biztonság [1] az egyik legalapvetőbb emberi szükséglet, amely sohasem önmagában, hanem mindig a veszélyhelyzetre történő reagálásként jelenik meg. Egy állam belső biztonsága [2] a politikai, társadalmi és a gazdasági rend megóvását, a veszélyek elhárítását jelenti. Kérdéskörébe tartozik a gazdasági terrorizmus egyik eszköze, a kibertámadás elleni védelem is. Ez utóbbi veszélyhelyzet fontos kérdés, mivel annak célja a pénzügyi válságok kezelése, az ezzel kapcsolatos banki feladatok.

A biztonság alapfeltétele a gazdaság zavartalan működése és a fejlődés feltételeinek biztosítottsága, melynek gazdasági szempontjai:

- gazdasági stabilitás biztosítottsága: hatékony gazdasági szerkezet, biztonságos külgazdasági kapcsolatok, szabad verseny;
- stabil pénzügyi feltételek megteremtése: mérsékelt infláció, rendezhető adósság és hitelállomány, ösztönző kamatrendszer.

A pénzügyi válságok témakörének és azok kezelésének szorosan kapcsolódó területe a pénzintézeteknél történő értékmegőrzés. A védelem- és hadigazdaságtan fogalmi rendszere, szemléletmódja alkalmazható egy látszólag távoli területen, mint a bankszféra, amely értékeink védelmében tevékenykedik.

A banki biztonság kiemelt jelentőségű, hiszen egy bankrendszert adott esetben kibertámadás érhet. Így szükségszerű, hogy a bankok tekintetében a megfelelően biztonságos környezet biztosítva legyen, ezért a biztonságot be kell építeni az információs rendszerekbe. A rendkívüli események bekövetkezésének okai lehetnek szándékos vagy óvatlan magatartás, mint pl. egy információs rendszereket érő kibertámadás, illetve váratlan események összessége, mint például egy természeti csapás. Az adott magatartás, esemény következtében az élet és vagyonbiztonság súlyos veszélybe kerül, amely akadályozza, vagy megbénítja a bank normális működését. A rendkívüli események megelőzése, megakadályozása, a keletkezett hátrány mértékének csökkentése érdekében a helyi katonai és rendőri szervekkel szoros együttműködést kell kialakítani.

A modern társadalmak nagymértékben függenek a különböző infrastruktúráktól (energiaellátás, ivóvíz ellátás, informatikai és banki hálózatok stb.), amelyek komplex rendszerét is egymástól való függőségek jellemzik. E rendszerek működési zavarai, illetve egyes elemeinek ideiglenes kiesése, vagy megsemmisülése jelentős kihatással vannak mindennapi életünkre, a gazdaság és a kormányzat hatékony működésére. Az állam, a gazdaság szereplői, valamint a lakosság részéről elvárás, hogy ezen alapvető létfontosságú, vagy kritikus infrastruktúrák lehető legnagyobb biztonsággal [3] működjenek.

A kritikus infrastruktúra elemek terrorcselekményekkel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid, kivételes és kezelhető legyen.

A kritikus, vagy létfontosságú infrastruktúrák [4] az általános definíció szerint "létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt következményekkel járna."

Ezen infrastruktúrák részben az állam, részben a magánszféra tulajdonában vannak, illetve azokat az állam vagy a magánszféra működteti.

A létfontosságú infrastruktúrákat kár érheti, működésükben zavar keletkezhet vagy azok meg is semmisülhetnek terrorcselekmény, természeti katasztrófa, hanyagság, baleset, számítógépes hackertevékenység, bűncselekmény vagy rosszhiszemű magatartás

következtében. Az infrastruktúrák biztonságának növelése ezért elsőrendű kérdéssé vált a fejlett országok biztonságpolitikájában.

Az infrastruktúrák biztonságnövelésének fő területei, az egyének, közösségek védelmének és a kritikus infrastruktúrák biztonságának magasabb szintre emelése. Mindhárom területen a veszélyek és fenyegetettségek fizikai, informatikai eredetűek vagy a rendszerek komplexitásból adódnak.

A megoldást az új fenyegetettségek és kockázatok fizikai, informatikai és pszichológiai szintű okainak felderítése, összefüggéseik megértése és kezelése jelenti.

Összességében a Kritikus Infrastruktúrák (KI) [5]:

- azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei;
- amelyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése;
- közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat;
- az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.

A létfontosságú infrastruktúrák *több gazdasági ágazatra kiterjednek*, többek között a bankügyletekre és pénzügyekre, a szállításra és forgalmazásra, az energiaiparra, a közművekre, az egészségügyre, az élelmiszerellátásra és tájékoztatásra, valamint a kulcsfontosságú állami szolgáltatásokra. Ezen ágazatok néhány létfontosságú eleme nem tartozik a szigorúan vett „infrastruktúra" fogalmába, de valójában olyan hálózatok vagy ellátási láncok, amelyek valamely alapvető termék vagy szolgáltatás biztosítását támogatják.

A létfontosságú infrastruktúrákat fenyegető katasztrofális *terrortámadások lehetősége egyre nő*. A létfontosságú infrastruktúrák ipari ellenőrző rendszerei elleni támadás következményei rendkívül eltérőek lehetnek.

Az infrastruktúrák katasztrofális meghibásodásának egyik típusa, amikor az infrastruktúra egy részének meghibásodása a többi meghibásodásához vezet, ami *dominóhatást* válthat ki. Ilyen meghibásodás az infrastrukturális ágazatok egymásra gyakorolt szinergikus hatása következtében alakulhat ki. Ennek egy egyszerű példája lehet a villamosenergia-szolgáltató közüzemek elleni támadás, ahol megszakad a villamosenergia-szolgáltatás, és ezáltal más elektromos készülékek – így a banki rendszerek is - leállhatnak. Az egymást követő események láncolata szintén nagy károkat okozhat, és a közüzemeken keresztül is a bank-, pénzügyi rendszerek leállását idézheti elő.

A KIBERTÉR

A modern hadviselés egyik legfontosabb színtere a kibertér [6], amely egy olyan tartomány, ahol hálózatos rendszerekben működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására, kiterjesztve azon hálózatokra is, melyek elemei nem rádiócsatornán, hanem vezetéken (rézvezeték, optikai kábel stb.) vannak egymáshoz kapcsolva.

A kibervédelem ennek alapján arra irányul, hogy fenntartsa a saját hálózatos információs rendszereinkben a hozzáférhetőséget az információkhoz, információalapú folyamatokhoz, és biztosítsa ezen rendszerek hatékony használatát békeidőben, válság vagy konfliktus idején egyaránt.

A kiberhadviselés [7] az információs dimenzióban megvalósuló hálózati hadviselést jelenti. Leegyszerűsítve a kritikus információs infrastruktúrák bizalmasságának, sértetlenségének és rendelkezésre állásának befolyásolására irányuló tevékenység informatikai, fizikai és emberi eszközökkel.

A kibertámadás észlelésének igénye szoros együttműködést és összehangolt cselekvést kíván az információs rendszerek tervezői, gyártói, forgalmazói, adminisztrátorai, felhasználói, valamint a szolgáltatásokat biztosító, jogalkotó és hírszerző szervezetek között. Az információs rendszereket támadók műveleti sebessége meghaladhatja a humánmegoldásokat tartalmazó észlelési és válaszadási képességeket. A hatékony kibervédelem érdekében elsődleges fontosságú automatizált módszerekkel felbecsülni az esemény súlyosságát (a rendszer sérülése, kompromittálódás, rosszindulatú program bejutása a rendszerbe) és csökkenteni azok negatív hatásait.

A helyreállítás megkezdéséhez és a szükséges válaszlépések megtételéhez a támadások időbeni felderítése alapvető feltétel.

Általánosan elfogadott, hogy egy sikeres kibertámadás legrosszabb esetben is csupán kevés sérüléssel járna, de a létfontosságú infrastrukturális szolgáltatások szempontjából veszteséget eredményezhet. Például a banki hálózat elleni sikeres kibertámadás miatt az ügyfelek nélkülöznék a banki szolgáltatásokat mindaddig, míg a szakemberek elvégzik a hálózat helyreállítását és javítását.

A kibertér támadása – informatikai vagy más módon – a bankok esetében fontossá tette azt, hogy az informatikai rendszerek a lehető leginkább biztonságos módon kerüljenek kifejlesztésre a szervezeten kívül és belül. A pénzügyi rendszerek kiemelt szerepet töltenek be, hiszen ezek megfelelő működése nélkül a pénzügyi folyamatok egy része vagy egésze működésképtelenné, de legalábbis jelentősen akadályozottá válik.

INFORMÁCIÓS HADVISELÉS [8]

Napjaink új típusú társadalmában a különféle információs tevékenységek az un. információs környezetben, vagy más néven az információs színtéren zajlanak. Ennek következtében a katonai műveletek működési területei és tartományai tovább bővültek, kiegészültek az információs hadszíntérrel.

Az információs hadviselés során alkalmazható fenyegetések négy kategóriára [9] bonthatók: "kompromittálás, megtévesztés, szolgáltatás akadályozása/megszakítása, fizikai megsemmisítés. Mind a négy kategória kockázatot jelent azokra az önálló, vagy hálózatba szervezett fegyverekre és támogató rendszerekre (banki rendszerek), amelyek nagymértékben támaszkodnak információs rendszerekre. A fenyegetés származhat szervezett erőktől (államok) vagy strukturálatlan ellenfelektől (hacker)."

A kompromittálásnak többféle formája [10] lehet, így például a technológia illetéktelen megszerzése vagy szoftverhiba, a rendszerbe történő illetéktelen behatolás, rosszindulatú szoftver használata, felderítő szervezet adatgyűjtése vagy egy pszichológiai művelet.

Ahhoz, hogy az automatizált információs rendszereket megvédjük, első lépésben meg kell érteni az ellenük irányuló fenyegetéseket, mint pl. az adatok és információk kompromittálása, a szolgáltatások részleges vagy teljes akadályozása, rongálása. Ennek legjobb eszköze a képzés és a szoros együttműködés az operátorok és a felhasználók között.

Az előzetes vizsgálatként össze kell gyűjteni a minimális információkat, jelezni kell a várható fegyelmi lépéseket, javaslatot tenni a további vizsgálatra. A kompromittálás utáni veszteségek felbecsülését egy központilag irányított rendszernek kell végeznie, mely egy központi adatbázisból és célirányosan kialakított programokból és projektekből áll.

Az információs rendszerek biztonsági monitorozása a saját hivatalos távközlés lehallgatása, olvasása, másolása vagy rögzítése, amelynek célja anyagot biztosítani az analízishez, amely lehetővé teszi az automatizált banki információs rendszerek biztonsági fokának pontos megállapítását. Ebben az információs környezetben az információs műveletek [11] a fizikai-, az információs- és a tudati dimenzióban érvényesülő, koordinált tevékenységet jelentik, amelyek a szembenálló fél információira, információalapú folyamataira és infokommunikációs

rendszereire gyakorolt hatásokkal képesek befolyásolni az ellenfelet. Az információs műveletek célja az információs fölény, uralom és végül a vezetési fölény kivívása.

Az információs műveletek elsődleges fenyegetései: kompromittálás, adatsérülés vagy információs művelet megszakadása. A biztonsági problémák esetében a megelőzés, a gyors reagálás és a károk csökkentése tekinthető kiemelt feladatnak. E feladatok mindegyikénél egyre nagyobb súllyal jelentkezik a számítástechnikai megoldások elterjedt használata.

A különböző szempontok szerinti megfogalmazások sokszínűsége bizonyítja az információs műveletek védelme érdekében a széles körű együttműködés szükségességét, a kockázathoz kötött védelmi feladatokat és a minden részletre kiterjedő képzést.

A PÉNZÜGYI ÉS BANKRENDSZEREK

A pénzügyi rendszerek [12] működésében – mint az élet más területein is - egyre hangsúlyosabb szerep jut az elektronikus szolgáltatásoknak, melyek a gyorsabb és költségtakarékosabb kiszolgálást jelentik a bankok részéről. Törvényileg, központosítva, jogszabályok által kívánják a banki szolgáltatások biztonságát garantálni, azonban meglátásom szerint az információbiztonság tekintetében jelenleg nincs olyan egységes szabályozás, amely a szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit meghatározzák. Ugyan tökéletes védelmet nyújtani talán lehetetlen, de mégis törekedni kell rá, hogy a szükséges biztonságos környezet kifejlesztésre kerüljön.

Ezáltal a biztonsági gondolkodásnak [13] az új alkalmazások, rendszerek kialakításánál, tervezésénél meg kell jelennie ahhoz, hogy a pénzügyi rendszerek kiberterébe a lehető legkevesebb veszélyforrás juthasson be. Elsődleges szempont a biztonságos fizikai környezet kialakítása és a további biztonsági követelmények megállapítása.

Célszerű a bankrendszerek területén olyan szabályozások általi megoldások létrehozása, amelyek felhasználásával a banki szolgáltatások biztonsági szintje jelentősen növelhető, valamint a felmerülő pénzügyi, gazdasági, nemzetbiztonsági kockázatok nagymértékben csökkenthetők. A pénzügyi rendszer biztonságát folyamatosan fenyegetések érik, mint például a katasztrófa és háborús helyzetek, valamint a csalók és rablók tevékenységei. Ezen problémák ellen kell felkészíteni a felsőszintű igazgatást, és azután együttesen fellépni a fenyegetettség megszűntetése és a biztonságos körülmények visszaállítása céljából.

A kibertér ma Magyarországon a legtöbb fejlett infrastruktúrával rendelkező országhoz hasonlóan védtelennek tekinthető. Bár az informatikai rendszerek támadásával emberéletekben nem vagy csekély kár eshet (közvetett hatásként), de a gazdasági, és ennek következményeként a politikai károk felbecsülhetetlenek.

Észtország kritikus információs infrastruktúráit [14] 2007. április 27-én külső, elosztott túlterheléses (Distributed Denial of Service – DDoS) támadás érte, amelyet tömeges levélküldés (spammelés) és weboldalak megváltoztatása (deface) egészített ki. A főbb célpontok az észt parlament számítógépei, valamint a *bankok*, minisztériumok, napilapok és elektronikus hírközlő szervezetek voltak. A támadás mind Észtországot, mind pedig a NATO-t felkészületlenül érte, pedig kivitelezéséhez csekély erőforrásokra volt szükség.

Magyarországon [15] egyelőre nem került napvilágra olyan incidens, mely külső támadás eredménye lett volna, de 2009-ben több olyan informatikai hiba is bekövetkezett, amely az adott kritikus információs infrastruktúra működését megakasztotta. Ez emberek tíz- és százezreinek okozott nehézséget, a sajtó kiemelten foglalkozott velük és jelentős presztízsveszteséget jelentett az üzemeltető intézménynek.

Magyarországnak is van tehát keserű tapasztalata az IT rendszerek leállásának következményeivel kapcsolatban, de a direkt, összehangolt támadások hatása egyelőre elképzelhetetlen. A bankügyi tranzakciók működésében hazánkban is egyre hangsúlyosabb szerep jut az elektronikus szolgáltatásoknak. Ezen szolgáltatások biztonságos működése

nemzetbiztonsági szempontból kritikus kérdés, hiszen ezek nélkül az ország gazdasági és pénzügyi működése jelentős akadályokba ütközne.

A szolgáltatások biztonságát a jogalkotók jogszabályokkal próbálják garantálni, azonban bizonyos területeken jelenleg nincsenek olyan egységes műszaki ajánlások, melyek a szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit meghatároznák. A nemzetközi trendek és a hazai tapasztalatok is azt mutatják, hogy az elektronikus banki szolgáltatások állandó célpontjai a szervezett bűnözésnek, a hackereknek és más államok hivatalos szerveinek.

Tökéletes védelmet nyújtani aránytalanul magas költséget jelentene, azonban az elvárható gondosság elve alapján szükséges a nyilvánosan elérhető szolgáltatásokat biztonságosan kifejleszteni. Ez azt jelenti, hogy a biztonsági gondolkodásnak már az új alkalmazások tervezésénél meg kell jelennie. A banki szolgáltatásokba biztonsági megoldásokat fejleszteni több szinten lehet.

A bankok biztonsági szintje jelentősen növelhető, és így a felmerült nemzetbiztonsági kockázatok nagymértékben csökkenthetők. A legjobb gyakorlatok (best practice, azaz széles körű tapasztalaton alapuló, több szervezetnél is sikeresen bevált gyakorlat) felhasználásával és továbbfejlesztésével, valamint az elektronikus banki ügyletek védelmi igényeihez történő hozzáigazításával lehet elérni.

A PÉNZÜGYI REÁLFOLYAMATOK BIZTONSÁGA

A tapasztalatok a közös katonai-civil [16] együttműködésről az alábbiak:

- A makrogazdasági körforgásnak folyamatosan kell működnie ahhoz, hogy a pénzellátás, és a reálfolyamatok (termelés) folytonossága biztosítva legyen.
- A pénzügyi rendszer biztonságát folyamatosan fenyegetések érik, mint például a katasztrófa és háborús helyzetek, valamint a csalók és rablók tevékenységei.
- Ezen problémák ellen kell felkészíteni a felsőszintű igazgatást (CMX gyakorlatok), és azután együttesen fellépni a fenyegetettség megszűntetése és a biztonságos körülmények visszaállítása céljából.
- A modern aszimmetrikus hadviselésbe főszerepben a terrorizmus és kiberbiztonság van, mint napjaink kiemelt biztonsági feladatai.
- Elterjedőben vannak a potenciális támadások kritikus infrastruktúrák ellen, (ebben az esetben a bankszektor).
- A bankok tekintetében biztosítani kell a megfelelően biztonságos környezetet, a biztonságot be kell építeni az információs rendszerekbe.

A bankbiztonsági tevékenység mindazon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondolkodás, amely a pénzintézet saját tulajdonú tárgyainak, értékeinek, valamint az alkalmazottak és az ügyfelek biztonságának védelmét szolgálja.

A Nemzeti Biztonsági Stratégia [17] (NBS) célja, hogy iránymutatást nyújtson a kormányzati szektor számára biztonságpolitikai – azon belül pénzügyi - kérdésekben. Filozófiájában ezért átfogó és összkormányzati megközelítést követ. Az ország biztonsága azonban mindenekelőtt közügy, ezért a stratégia egyik feladata, hogy a szakmai körökön túl a mindennapi életben is hasznosítható támpontot nyújtson a hazai biztonságpolitikai gondolkodásban.

Az NBS-ben szerepelnek azon biztonsági elemek is, melyek egy pénzügyi krízis esetében – mint például kibertámadás az ország bankrendszere ellen – fontos szempontok annak érdekében, hogy a veszélyhelyzetet megszűntessék.

Megfogalmazásra kerültek mindazon tényezők, melyek a pénzügyi biztonságot meghatározzák az egyes nemzetállamok gazdaságának működése tekintetében:

- pénzellátás – bankválság esetén a készpénzellátás korlátozása;
- azonnali betét kivétel pánik – pl. Postabank-botrány (1997. február);
- pénzügyi tartalék – a krízishelyzetek esetére;
- pénzügyi moratórium – pénzintézetekből történő pénzkivétel korlátozása.

A NBS 30. pontja a pénzügyi biztonságról szól, iránymutatást nyújt a kormányzati szektor számára egy pénzügyi krízis (pl. a kibertámadás) problémáinak kezeléséről és megszűntetéséről.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény 2. számú mellékletében a nemzeti létfontosságú rendszerelemek kijelölése alapján a pénzügy is egy kritikus infrastruktúra ágazatnak tekintendő [18]:

	A	B
	Ágazat	Alágazat
17	pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
18		bank- és hitelintézeti biztonság
19		készpénzellátás

A NATO CMX GYAKORLATA – 2012. NOVEMBER [19]

Kritikus infrastruktúráink sérülékenyek és támadhatók. A szakemberek nem látnak olyan határozott lépéseket, amelyek ezen hálózatok – mint például a banki és pénzügyi számítógépes hálózatok – megfelelő, komplex védelmét erősítenék. Mindez azt jelenti, hogy a kritikus infrastruktúrák rendkívül sebezhetőek.

A fejlett hadi- és informatikai kultúrával rendelkező országok a 21. század elejének egyik legkomolyabb kihívásaként kezelik a kritikus információs infrastruktúrák védelmét. Magyarországon mindeddig nem készült olyan tanulmány, amely számításba venné, hogy milyen láncreakciót válthat ki egy kritikus információs rendszereket érintő átfogó, informatikai támadásokat is magába foglaló cselekménysorozat, mint például a bankrendszerünk ellen történő kibertámadás - ahogyan azt 2012 novemberében a CMX 2012 gyakorlatban szimulálták.

Egy, az információs infrastruktúrákat célzó támadás akár napokig tartó működési zavarokat okozhat az országban. A NATO 2012. évi CMX válságkezelő és egyben kibervédelmi (támadás érte a bankrendszert) gyakorlatának fő célja a jelen kor kihívásai elleni egységes fellépéshez szükséges döntések konszenzusos meghozatala volt:

- NATO-szerződés 5. cikkelyének érvényesítése – a tagországok közösen léptek fel a támadás elhárításáért és a rendszerek helyreállításáért;
- A hazai válságkezelési rendszer döntés-előkészítő és döntéshozatali folyamatainak, valamint a NATO-központtal és a tagországokkal való együttműködés gyakorlása;
- A Gyakorlathoz a 2007-es, Észtország elleni kibertámadást vették mintául (ma már nincsen „valódi” háború kibertámadások nélkül).

A szakemberek felhívták a figyelmet, hogy az ilyen típusú támadásoknál elsősorban a megelőzésre kell törekedni, mivel a más szervezetek által előre tervezett és célzott támadásra szinte lehetetlen felkészülni.

BANKBIZTONSÁGI TEVÉKENYSÉG

Egy bankrendszer [20] tekintetében a legfontosabb kritériumok:

1. A pénzügyi szolgáltatási tevékenység csak a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg.
2. A pénzügyi intézménynek ki kell alakítania a pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről.
3. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.
4. A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére.
5. A pénzügyi intézménynek [21] tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:
    a) a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb - a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal;
    b) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről;
    c) a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.

A rendkívüli helyzetek kezelésének módjára az alábbiak fogalmazhatóak meg:

1. A pénzintézetnek a mérete, az általa végzett pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenysége jellege, nagyságrendje, összetettsége arányában megbízható irányítási rendszerrel kell rendelkeznie, és ennek keretén belül köteles a felmerülő kockázatok azonosítására, mérésére, kezelésére, nyomon követésére és jelentésére szolgáló hatékony eljárásokat alkalmazni.
2. Emellett írásban rögzített eljárásrendekkel, szabályzatokkal kell rendelkeznie a működési kockázatok mérésére, kezelésére, valamint vészhelyzeti és üzletmenet-folytonossági tervvel a folyamatos működés fenntartása, továbbá a súlyos üzletviteli fennakadásokból következő esetleges veszteségek mérséklése érdekében.

A Magyar Nemzeti Bank (MNB) alapfeladata a fizetési és elszámolási rendszerek felvigyázása, e rendszerek biztonságos és hatékony működése, továbbá a pénzforgalom zavartalan lebonyolítása érdekében. A 2012. július 14. napjától az MNB [22] alapvető és egyéb feladatai az alábbiakban foglalható össze:

- Az MNB más felelős hatóságokkal együttműködve feltárja a pénzügyi közvetítőrendszer egészét fenyegető üzleti és gazdasági kockázatokat, elősegíti a rendszerszintű kockázatok kialakulásának megelőzését, valamint a már kialakult rendszerszintű kockázatok csökkentését vagy megszüntetését.
- Feltárja a pénzügyi közvetítőrendszer egészét fenyegető üzleti és gazdasági kockázatokat, elősegíti a rendszerszintű kockázatok kialakulásának megelőzését, valamint a már kialakult rendszerszintű kockázatok csökkentését vagy megszüntetését.
- Az MNB elnöke a rendszerszintű kockázatok felépülésének megakadályozása vagy a kockázatok csökkentése érdekében rendeletet adhat ki.
- Amennyiben olyan körülmény áll fenn, amely miatt a hitelintézet működése a pénzügyi rendszer stabilitását veszélyezteti, az MNB a hitelintézetnek rendkívüli hitelt nyújthat.
- Az MNB sürgős, rendkívüli, a pénzügyi rendszer egészének stabilitását és a pénzforgalom zavartalanságát veszélyeztető esetben hitelt nyújthat, amelynek lejárata legfeljebb három hónap lehet.

A Magyar Nemzeti Bank elnöke rendeletben szabályozza, hogy a rendszerkockázatok felépülésének megakadályozása vagy a kockázatok csökkentése érdekében szükséges intézkedéseket: a túlzott hitelkiáramlást megakadályozó előírásokat, a rendszerszintű likviditási kockázatok felépülését megakadályozó likviditási követelményeket, felépítésének és működésének feltételeit, a rendszerszinten jelentős intézmények csődvalószínűségét csökkentő többletkövetelményeket.

Mindezen – egyebekben üzleti titkot képező – eljárások, szabályzatok, intézkedési tervek megfelelőségét a Pénzügyi Szervezetek Állami Felügyelete (PSZÁF) köteles ellenőrizni. A jogalkotó 2013. szeptember 16.-ai döntésével 2013. október 1.-jei hatállyal összevonta a PSZÁF-ot az MNB-vel [23]. Ennek alapján az MNB új szervezetében már megjelennek a pénzügyi biztonság eléréséhez javasolt feladatok.

Megállapítható, hogy az NGM csak a szabályozás elméleti oldaláról érintett, a gyakorlati tennivalók tekintetében MNB (magába foglalva a PSZÁF-ot), esetleg a Magyar Államkincstár (MÁK) bizonyul illetékes szervnek.

KÖVETKEZTETÉSEK

A pénzügyi szolgáltatási tevékenység végzéséhez szükséges egy a működési kockázatok csökkenését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó intézkedési terv.

A biztonsági kockázatelemzés eredményei alapján gondoskodni kell az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint a rendszeres biztonsági mentésről és a kritikus folyamatok eseményeit naplózó biztonsági környezetről.

A rendkívüli helyzetek kezelésének eljárásait, szabályzatait, intézkedési terveik megfelelősségét a PSZÁF köteles ellenőrizni, ezért célszerű a bevonása.

Az MNB alapfeladata a fizetési és elszámolási rendszerek felvigyázása, azok biztonságos és hatékony működése, a pénzforgalom zavartalan lebonyolítása érdekében.
Összességében az NGM csak a szabályozás elméleti oldaláról érintett, a gyakorlati tennivalók érdekében a PSZÁF, az MNB és a MÁK az illetékes szervek.

Mindezek érdekében a jövőre vonatkozóan érdemes kidolgozni egy olyan gyakorlati szabályozást – a többféle területen használt Legjobb Gyakorlatok (Best Practises) módszerével –, amely által az állami és pénzügyi (bankszektor) szervek összehangoltan, azonnali reagálással képesek fellépni az őket ért támadások ellen.

Kulcsfontosságú szereppel bír az NGM-en kívül a 2 állami, pénzügyi felügyeleti szervünk, úgymint az MNB (PSZÁF!) és a MÁK. Minden pozitívan előremutató eredmény, megoldás eléréséhez az általuk közösen megfontolt és kimunkált tevékenységre van szükség a jövőben a bankokat fenyegető kibertámadások ellen.

Felhasznált irodalom

[1] Gazdag Ferenc, Tálas Péter: A biztonság fogalmának határairól, Nemzet és Biztonság, 2008/1. szám (3-9. o.)

[2] Gazdag Ferenc: Biztonsági tanulmányok – Biztonságpolitika, ZMNE, Budapest, 2011. 37-46. o. ISBN 978-615-5057-23-6

[3] A Kormány 1139/2013. (III.21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[4] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[5] Sík Zoltán Nándor: A kritikus információs infrastruktúra védelem kormányzati feladatai az információs hadviselés korában http://old.ivsz.hu/resource.aspx?ResourceID=GetDocStoreFile&EntryID=3353 (2013.december 17.)

[6] Haig Zsolt, Várhegyi István: A cybertér és cyberhadviselés értelmezése Hadtudomány 2008. elektronikus szám 1-12. o. ISSN 1215-4121 http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (2014. január 16.)

[7] Haig-Kovács-Ványa: Az elektronikai hadviselés, SIGINT és a Cyberhadviselés kapcsolata Felderítő Szemle X. évf. 1-2. sz. 2011. 183-209. o. http://www.kfh.hu/hu/letoltes/fsz/2011-1-2.pdf (2014. január 16.)

[8] Haig Zs.: Az információs hadviselés kialakulása, értelmezése. Hadtudomány XXI. évf. 1-2. szám 2011. (12-28. o.) http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf (2014. január 16.)

[9] Kassai Károly: A minősített információk és adatok védelme http://www.zmne.hu/kulso/mhtt/hadtudomany/2002/1/z-05/chapter1.htm, (2013. december 12.)

[10] Kassai Károly: A minősített információk és adatok védelme http://www.zmne.hu/kulso/mhtt/hadtudomany/2002/1/z-05/chapter1.htm, (2013. december 12.)

[11] Haig-Kovács-Munk-Ványa: Az infokommunikációs technológia hatása a hadtudományokra, NKE, Budapest (2013. 173 o.) ISBN: 978-615-5305-02-3

[12] Vígvári András: Pénzügy(rendszer)tan Akadémiai Kiadó, Budapest 2009. (192-194. o.) ISBN 978-963-05-8595-8

[13] Vígvári András: Pénzügy(rendszer)tan Akadémiai Kiadó, Budapest 2009. (414-417. o.) ISBN 978-963-05-8595-8

[14] Dr. Haig Zsolt – Dr. Kovács László: Fenyegetések a cybertérből http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=57 (2013. december 17.)

[15] Dr. Kovács László – Dr. Krasznay Csaba: Digitális Mohács - kibertámadási forgatókönyv Magyarország ellen http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf 2013. december 10.

[16] Cser Orsolya: Biztonságunk egyik záloga a hatékony civil-katonai együttműködés http://mhtt.eu/hadtudomany/Hadtudomany_2013_3-4_10.pdf (2013. november 29.)

[17] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról

[18] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény 2. számú melléklete

[19] A NATO kibervédelmi gyakorlatán is jól vizsgáztunk (CMX 12 NATO Válságkezelési gyakorlat nemzeti feladatai) http://bitport.hu/biztonsag/a-nato-kibervedelmi-gyakorlatan-is-jol-vizsgaztunk (2013. december 2.)

[20] A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996.évi CXII. törvény

[21] Jakab Péter: Egy működő vállalati komplex biztonsági rendszer felépítése, működése http://regi.hte.hu/data/upload/File/HTE_Forum_JakabP_080902.ppt (2013. december 19.)

[22] A Magyar Nemzeti Bankról szóló 2011. évi CCVIII. törvény

[23] Cser Orsolya: A pénzügyi rendszer, mint kritikus infrastruktúra ágazat – avagy a pénzellátás folyamatosságának védelme „Szervezeti, szabályozási és innovatív változások a létfontosságú rendszerek védelmében” tudományos-szakmai konferencia 2013.11.14. – elektronikus megjelenés 2014. március végén a konferencia külön kiadványában

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Gyebrovszki Tamás
gyebrovszki.tamas@nbsz.gov.hu

STUXNET - MINT AZ ELSŐ ALKALMAZOTT KIBERFEGYVER - A TALLINNI KÉZIKÖNYV SZABÁLYRENDSZERE SZEMPONTJÁBÓL

Absztrakt

A cikk meghatározza, hogy a Tallinni Kézikönyvben lefektetett szabályok alapján hogyan válaszolhat egy állam egy olyan kibertámadásra, amilyet a Stuxnet féreg valósított meg Iránban. Választ keres továbbá arra a kérdésre, hogyan kell alkalmazni a kiberhadviselés szabályait a hagyományos hadviselés függvényében. Végül sürgeti a kiberműveleteket szabályozó jogi keretrendszer kidolgozását.

This article defines a response should be done to a cyber attack such as worm called Stuxnet performed in Iran based on rules defined in Tallinn Manual. It searches an answer how to apply rules of cyberwarfare in comparison with traditional warfare. It points up a need for establishing legal framework regarding to cyber operations.

Kulcsszavak: *Stuxnet, kiberfegyver, kiberkonfliktus, kritikus infrastruktúra. Stuxnet, cyber weapon, cyber conflict, critical infrastructure.*

BEVEZETÉS

A tömeges számítások elvégzése a tudomány számos területén okozott fejfájást, így a számítógép feltalálása nagy ugrást jelentett. Konrad Zuse német feltaláló a világon elsőként létesített programvezérelt számítógépet 1938-ban [1]. A számítógépet később már információ feldolgozásra, tervezési feladatokra is felhasználták, példa erre a Budapesten található Erzsébet-híd újjáépítése, amikor a híd statikai számításait az MTA Kibernetikai Kutatócsoport végezte a Magyarországon első, az M3 megnevezésű 1959-ben átadott számítógép segítségével [2]. Viszonylag rövid idő alatt megjelentek számítógépek a távközlés, az irányítástechnika, gyártásirányítás, kereskedelem és még számos területen. Napjainkra kevés olyan feladat létezik, ahol nem alkalmazható számítógép.

Korunk számítógépe magában hordozza a globális összekapcsolhatóságban rejlő páratlan lehetőséget és persze az ezzel járó veszélyeket is. Az egyre kisebb méretű és egyre nagyobb képességű eszközök általi fejlődési lehetőséget csak elcsépelt jelzőkkel illethetjük, mint forradalmi, vagy ugrásszerű. Csak a távközlés területén egyetlen példa, hogy akár kerékpározás közben is megkapjuk elektronikus leveleinket a világ bármely részéről, ami az információhoz jutásunkat, gazdasági lehetőségeinket segítheti elő. A kibertér azonban nemcsak előnyös tulajdonságokkal segíti életünket, hanem sajnos potenciális veszélyforrás is egyben.

Ahogy az alkalmazások egyszerűsítik azokat a feladatokat, amelyekkel korábban sok időt töltöttünk, egyre több olyan van, melyekben nem kellene megbíznunk, sőt óvakodnunk kellene használatba vételüktől. Jó példa ezekre az olyan mobilalkalmazások, amelyek egyre népszerűbbek, azonban gyanús tevékenységeket, vagy egyenesen rosszindulatú funkciókat is végeznek. Az elmúlt egy évben sokszorosára emelkedett a mobiltelefonokra fejlesztett malware-k száma [3]. Az okostelefonok elterjedtek és a használói között kormányfők, állami intézmények vezetői, védett személyek is szép számmal vannak. E személyek célpontok, elsősorban kémkedési célzattal gyűjtenek adatokat róluk, a hagyományosnak mondható eszközökkel [4] illetve a mobil malware-k útján, vagy akár piaci termékek is találhatók [6] személyek követésére, ellenőrzésére. A kritikus infrastruktúrák kitettsége is okot ad a fejfájásra, ugyanis ezek az ipari vezérlőrendszerek (ICS) sok esetben elavultak és sérülékenyek [12].

A kritikus infrastruktúrát üzemeltető intézményeket fenyegető kibertámadások már emberáldozattal is járhatnak, ami indokolta, hogy az elmúlt években komoly hangsúlyt kapott a védelmi képességek erősítése, a rendszerek védelme.

Az informatika fejlődése a társadalom fejlődését erősíti, olyan módon, hogy egy államnak és annak szereplőinek minőségileg magasabb színvonalú életet kínál, magasabb hatékonysággal gazdálkodik, termel, szolgáltat. Az információs társadalom elsősorban nem azt jelenti, hogy az állampolgárok többsége rendelkezik Internet hozzáférési lehetőséggel, hanem azt, hogy az állam, a kormányhivatalok, az önkormányzatok és a közigazgatás egyéb szereplői, gazdaság szereplői olyan saját belső (többnyire összekapcsolt) informatikai rendszereket alkalmaznak, amelyeknek központi szerepe van a termelésben, a gazdaságban és általában a társadalomban.

Kulcskérdés értékelnünk, hogy mekkora a kár, ha a fent említett kritikus infrastruktúrákat, információs társadalmat éri kibertámadás, hogyan védekezzünk a támadások ellen, amikor az információ szabad áramlása és hozzáférhetősége társadalmi érték? Hogyan kell védekezni, csökkenteni a kárt, milyen eszközöket vethetünk be, melyek a jogi keretek [7]? Az Irán urándúsító kapacitását támadó Stuxnet malware a Tallinn Kézikönyv szerint hogyan sorolható be és mi lehetne a jogos válaszintézkedés?

Cikkemben többek között ezekre a kérdésekre adok választ a Tallinni Kézikönyv felhasználásával.

„TALLINN KÉZIKÖNYV A KIBERHADVISELÉS NEMZETKÖZI JOGI SZABÁLYAIRÓL” [5]

Tallinn a 2007-ben elszenvedett kibertámadás, Észtország fővárosa. A NATO Cooperative Cyber Defence Centre of Excellence-t (NATO Kibervédelmi Kiválósági Központot, továbbiakban CCDCOE) 2008. május 14-én létesítették Tallinnban, célja a védelmi képességek erősítése. A CCDCOE megalapításától kezdve a NATO vezetőinek ad technikai és jogi tanácsokat a kiberhadviseléssel kapcsolatos ügyekben. A szponzorok között van Hazánk, Észtország, Lettország, Litvánia, Németország, Olaszország, Lengyelország, Szlovákia, Spanyolország, Hollandia és az Egyesült Államok.

A 2013-ban a Cambridge University Press által kiadott könyv a „Tallinn Manual on the International Law Applicable to Cyber Warfare” címet viseli (továbbiakban Kézikönyv). A Kézikönyv szerzőit és közreműködőit a CCDCOE hívta meg neves egyetemekről, intézményekből független nemzetközi jogászszakértők, technikai szakértők, a szerkesztőbizottság, és a megfigyelők voltak, összesen 46 fő. A három évig tartó munka célja az új típusú hadviselés, a kiberhadviselés terén alkalmazható jogi és katonai lépések vizsgálata volt mind a jus ad bellum mind a jus in bello vonatkozásában. A fő hangsúlyt azonban a békeidőben végzett ellenséges kibertevékenységek elleni jogi lehetőségek vizsgálatára fordították. A munka eredménye lett a 302 oldalas Kézikönyv. A projekt során szorosan együttműködtek a tallinni CCDCOE kutatóintézettel. A projekt igazgatója Michael N. Schmitt professzor volt aki a US Haditengerészeti Főiskola Nemzetközi jogi tanszékének vezetője, koordinátora Dr. Eneken Tikk vezető szakértő volt. Dr. Tikk, a 2007-es kibertámadás elemzésével és dokumentálásával foglalkozott, ezt követően számos országgal, nemzetközi szervezettel működött együtt a kiberbiztonság stratégia területén. Bár a Kézikönyv nem hivatalos dokumentum, nem tükrözi sem a CCDCOE, sem a szponzor államok, sem pedig a NATO nézőpontját, a maga nemében egyedülálló értékkel bír, nincs ilyen átfogó jellegű, a kiberbiztonság területén alkalmazható jogi lépésekről, elvekről szóló könyv. Véleményem az, hogy az egyes országok felhasználhatják a nemzeti jogszabályalkotásukban.

A Kézikönyv 2 részből áll, a részeken belül fejezetek vannak, ezeket pedig szekciók tagolják tovább. Az egyes szekciókon belül találhatóak meg a szabályok. Minden szabályt pontokba foglalt kommentár, magyarázatok és példák támasztják alá. Az első rész a „Nemzetközi kiberbiztonsági jog”, a második a „Kiberhadijog” címet viseli.

Maga a Kézikönyv 95 szabályt tartalmaz. A szövegek nem kötelező érvényű ajánlást, hivatalos álláspontot tükröznek, hanem többféle szempont bemutatásával a jogalkotás további lépéseiben ad zsinórmértéket. A szerzők véleménye szerint az állam vagy felelősségre vonja az agresszort, vagy „arányos ellenintézkedésekkel” válaszolhat.

Az első fejezet az állam és a kibertér viszonyát határozza meg. A kibertámadásokat „fegyveres támadásnak” lehet minősíteni, így jogos az önvédelem a megtámadott állam részéről, beleértve a hagyományos fegyverek alkalmazását is. Ugyanakkor nem tekinthető fegyveres támadásnak a kiberkémkedés, a számítógépes lopás, a honlapok elleni támadások, amennyiben a károk nem állami méretűek. Az agresszor állam viseli a felelősséget, akkor is, ha más országokból való közvetítők útján végzi a támadást. A kézikönyv összeállítói szerint a kibertámadásokat a vegyi, a biológiai és a radiológiai fegyverek alkalmazásához kell hasonlítani.

A szuverenitás keretében az állam hatalma kiterjed a fennhatósága alatt álló területen, a kibertér és a kibertevékenység ellenőrzésére is. Jogosult szabályokat alkotni azon személyek vonatkozásában, akik a fennhatósága alatt álló területen kibertevékenységet folytatnak, valamint magáról az ellenőrzése alatt álló kibertér infrastruktúrájáról is. A nemzetközi légtérben és vizeken, valamint a világűrben – a légügyi és a tengeri hajózási joghoz hasonlóan – az adott

járműben vagy objektumban folytatott kibertevékenységre a tulajdonos állam szabályai vonatkoznak, és az azok elleni kibertámadás az adott állam elleni támadásnak minősül. Az államok felelősséggel tartoznak, ha területükről az ellenőrzésük alatt álló szervezetek más országok ellen kibertámadást hajtanak végre. Az azonban, hogy a kibertámadást egy adott országból indították, még nem bizonyítja az érintett ország felelősségét. Fennáll ugyanis annak a lehetősége is, hogy más államok használták az adott ország kiberterét a támadás elkövetésére. A kibertérben megtámadott államnak joga van arányos ellenlépéseket tenni.

A kiberművelet akkor minősül erő alkalmazásának, amikor hatása összemérhető egy hagyományos fegyveres támadással. Az erő alkalmazásának tisztázása érdekében a szerzők meghatározták az erővel való fenyegetés fogalmát. Megállapították, hogy olyan kibertámadás esetén, amelynek hatása felér egy fegyveres támadásával, az államnak joga van az önvédelemhez, de ennek során figyelembe kell vennie a szükségesség és az arányosság elvét. Egy adott állam jogosult a kibertámadás ellen fellépni, ha az már bekövetkezett vagy fenyegető közelségben van a bekövetkezése. Az államoknak joguk van az önvédelmet több országgal közösen kollektív védelem keretében biztosítani. Az önvédelemnek összhangban kell lennie az ENSZ Alapokmányának 51. cikkelyével, amely szerint a támadás tényéről azonnal tájékoztatni kell az ENSZ Biztonsági Tanácsát. A nemzetközi szervezetek kiberhadviselésben történő szerepvállalását az ENSZ Biztonsági Tanácsa esetében, illetve a regionális szervezetek vonatkozásában áttekintették és megállapították, hogy a kibertámadások során a nemzetközi szervezeteknek is joguk van a fellépésre.

A Kézikönyv második fejezete a kiberkonfliktusokkal foglalkozik, az állam joga az önvédelemre, arányos ellenlépés megtételére és a nemzetközi szervezetek beavatkozásának lehetőségét.

A harmadik fejezet pedig áttekinti a fegyveres konfliktusok jogszabályi hátterét és azok alkalmazhatóságát a kiberhadviselésre. Fontos megállapítás, hogy a kibertámadásokra is az általános hadviselésre érvényes szabályok vonatkoznak. Ezt követően a kiberhadviselés földrajzi kiterjedésének kérdésével foglalkoztak, majd megszabták a nemzetközi és az államon belüli fegyveres kiberkonfliktusok kereteit.

Az alapvető probléma itt jelentkezik, hiszen a támadó kilétének meghatározása nem triviális, a hadviselő felek azonosítása a hagyományos hadviselésben biztosított, a kibertérben ez nincs így, a *Támadó meghatározása komoly nehézségekbe ütközik*.

A negyedik fejezet magát a kiberkonfliktust tekinti át, ennek keretében foglalkozik a támadások szereplőivel, a támadásokkal, a hadviselés módszereivel, az óv- és ellenintézkedésekkel, az árulással, a kémkedéssel. Megállapították, hogy nincs arra vonatkozó szabály, ki vehet részt a kiberkonfliktusokban. Amennyiben a fegyveres erők tagjai a nemzetközi jog alapján elveszítik katonastátusukat, akkor elfogásuk esetén nem tekinthetők hadifogolynak. A konfliktusban érintett lakosság azon tagja, aki részt vesz a műveletekben, elveszíti a civilekre vonatkozó védettségét. A kiberműveletekben részt vevő felbérelt zsoldosok nem tekinthetők harcoló félnek, így hadifogolystátuszt sem kaphatnak.

Védekező és támadó kiberhadműveletről a következőket mondják: Akkor minősül egy művelet a kibertérben elkövetett támadásnak, ha hatására személyek sérülnek vagy halnak meg, illetve vagyontárgyak rongálódnak vagy semmisülnek meg. A támadások célszemélyei lehetnek a fegyveres testületek és szervezetek tagjai. A nemzetközi jog a kibertérben is tiltja a terrorizmust és annak eszközeit. A hadviselés eszközei és módszerei kapcsán ügyelni kell arra, hogy nem szabad felesleges sérülést és szükségtelen szenvedést okozni ellenfélnek. A kiberműveletekre is vonatkozik az arányosság elve, amelynek alapján a megtámadott fél nem okozhat sokkal nagyobb veszteséget a támadónak, mint amennyit elszenvedett. A kiberműveletekben a szemben álló feleknek figyelembe kell venni a polgári személyek

védelmét, valamint ügyelni kell a támadási módszerek megválasztására, a célok kiválasztására, a támadás előtti figyelmeztetésre, illetve a megtámadott fél védelmi kötelezettségére.

A kiberhadviselésben az árulás, a megtévesztés és a kémkedés kérdéskörét vizsgálva megállapították, hogy hasonló jogok vonatkoznak ezekre a tevékenységekre, mint a hagyományos hadviselés során.

A Tallinni Kézikönyv szerzői az ötödik fejezetben a védett személyek és objektumok meghatározásával és védelmével foglalkoznak. Védettséget élveznek az egészségügyi, a vallási, az ENSZ-hez tartozó személyek, eszközök és objektumok, valamint a gyermekek, az őrizetben lévő személyek, az újságírók, a polgári lakosság, a veszélyes létesítmények, a diplomáciai testületek és a kulturális javak.

A hatodik fejezet a megszállással kapcsolatos nemzetközi jogi kérdéseket dolgozza fel. A kiberművelet során elfoglalt területen a védendő személyek jogaira figyelemmel kell lenni, valamint olyan mértékben biztosítani kell a kibertérhez való hozzáférést, amely a védett személyek biztonságához szükségesek. A megszálló hatalom jogosult intézkedéseket és általános szabályokat foganatosítani a megszállt területen, valamint integrálhatja a megszállt területeken lévő számítógépes hálózatokat saját rendszereibe. Ennek keretén belül joga van a hálózatok lefoglalására.

Az utolsó, hetedik fejezet a semleges államokkal foglalkozik. A hadviselő feleknek tilos a semleges államok informatikai rendszereit megtámadni, illetve a kibertámadásokhoz a semleges államok területét vagy számítógépes hálózatait felhasználni.

A STUXNET [7, 8, 10, 11, 13, 14, 15]

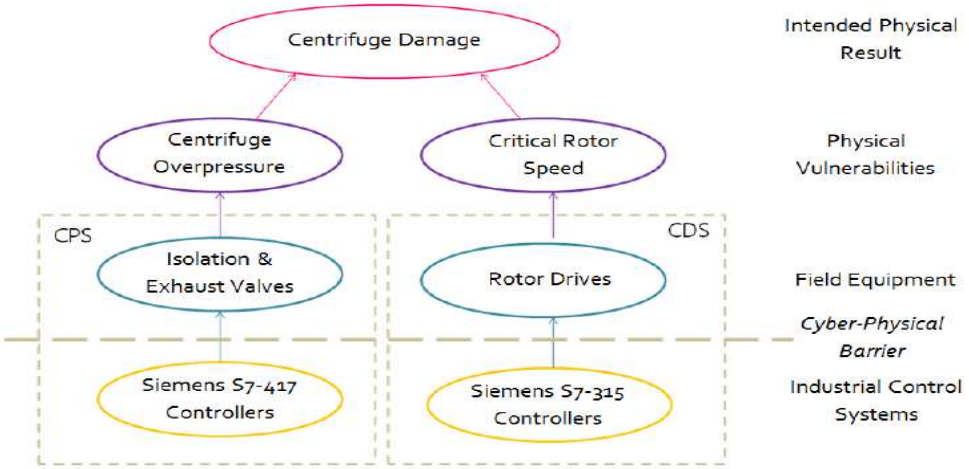
A Stuxnet egy olyan káros szoftver, amelyet célzottan ipari vezérlőrendszerek megfertőzésére, manipulálására és rombolására fejlesztettek ki. Ezt tekinthetjük az első ismertté vált kiberfegyvernek. Bevetésére az „Operation Olympic Games" fedőnevű, titkos művelet keretében történt, amelynek célja Irán atomprogramjának lassítása volt, meghibásodások előidézése útján. A kifinomultabb, első változatot elsőként 2007. november 15-én töltötte fel egy ismeretlen személy a Virustotal-ra, majd egy virulensebb változata elszabadult és elkezdte a terjedést.

Irán atomprogramja az ötvenes években kezdődött. A 79-es forradalmat követően azonban az megrekedt. Első atomerőművét 2011 szeptemberében adták át Bushehr-ben. Egyik urándúsító üzemét Natanz-tól mintegy 32 km-re észak-északnyugati irányban találhatjuk meg a 7. főközlekedési út és a 665-ös út kereszteződésénél (Ész 33º43'24,43" Kh 51º43'37,55"). A kivitelezés során a telep nagy része a föld alá került, nyilván az esetleges légitámadások elleni védekezés jegyében. Az üzem létezését csak 2003-ban ismerték el az irániak. 2009-re 5000 IR-1 centrifuga működött az üzemben. Bár Irán folyamatosan állítja, hogy atomprogramja békés célú, az ENSZ-BT 2006-tól kezdődően 8 határozatot hozott Irán ellen, a dúsítási tevékenység felfüggesztése tárgyában. A P5+1 országok és Irán külügyminisztereinek 2013 novemberében Genfben folytatott tárgyalása eredményeként Irán 6 hónapra visszafogja atomprogramját és átfogó vizsgálatot tesz lehetővé nukleáris létesítményeiben a Nemzetközi Atomenergia Ügynökségnek.

A Stuxnet az elemzések szerint a Siemens Simatic S7 PLC családjába tartozó S7-300 (315) és S7-400 (417) eszközök működésébe avatkozott be olyan feltételek mellett, amiből kiderül, hogy azt valóban az Iránban működtetett urándúsító üzem gyártási folyamatának lassítására fejlesztették ki.

1. ábra. A Siemens Simatic S7 termékcsalád
(http://www.plcdev.com/book/export/html/373)

Erre mutatnak az adatok, ugyanis Irán egy elavult technológiát alkalmazott, olyan speciális peremfeltételekkel, amit sehol nem alkalmaztak. A pakisztáni *Abdul Qadeer Khan* által megszerzett urándúsító centrifugák technológiai leírásai váltak a pakisztáni atomfegyver előállításának alapjává. Ezek alapján kidolgozott P-1 jelű centrifugák eljutottak Iránba is. A megbízhatatlannak jellemzett iráni változat az IR-1 nevet kapta és mintegy 8000 állt rendelkezésre Natanzban 2009-ben. A gyártási technológia részletes ismertetése helyett azt emelném ki, hogy a technológiai ismeretbéli hiányokat saját megoldásokkal egészítették ki az iráni mérnökök, ezzel azt egyedülálló technikai jellemzőkkel ruházva fel. Ez utóbbi a bizonyíték a támadás céljára. Megjegyzendő, hogy bár a Stuxnet szinte minden Windows platformot képes volt megfertőzni, azonban csak az iráni Natanzban fejtette ki a hatását. A Stuxnet féreg fizikai kárt képes okozni az iráni urándúsító berendezésekben. A károkozás az UF_6 molekulákat feldolgozó centrifugarendszer szelepeinek vezérlését zavarta meg a kalibrációs adatok megváltoztatásával, majd későbbi verziója a centrifugák sebességének vezérlését vette át, az urándúsítási folyamat akadályozása céljából. Mindkettő megoldás egyaránt rongálta a centrifugákat. Az alábbi ábrán látható, hogy a kétféle változat hogyan fejtette ki a hatását.



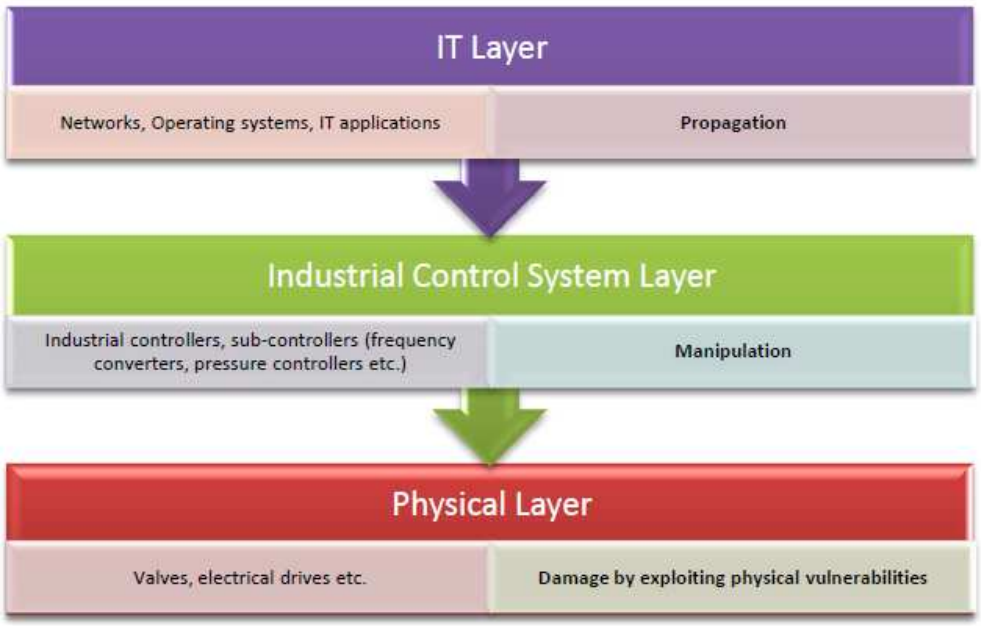
2. ábra. A két fő Stuxnet változat hatásmechanizmusa[1]

1CPS: Cascade Protection System, iráni fejlesztés, a túlnyomás elkerülésére. CDS: Centrifuge Drive System, a centrifuga motorvezérlő rendszere.

Az első kifinomultabb változat (Stuxnet 0.500) többek között lopott digitális tanúsítványokat alkalmazott, adatot gyűjtött a fertőzött rendszer üzemi paramétereiről, rögzítette a normál üzem adatait majd azokat játszotta vissza a kezelők megnyugtatása érdekében, miközben az urándúsító centrifugák nyomása a kritikus tartományba emelkedhetett. A malware hét szakaszból álló ciklusában négy szolgál rombolásra, három előkészítésre és a normál üzemre visszaállásra.

A második, némiképp agresszívabb változat (Stuxnet 1.x) szintén alkalmazott ellopott digitális tanúsítványokat, a rotorok sebességét változtatta meg az üzemi tartományon kívülre, így a centrifugák korai meghibásodását idézte elő. A káros tevékenységében öt szakaszt váltogat különböző időtartammal pl. 1410 Hz-re gyorsítja a centrifugákat, majd „rátapos a fékre" és 2 Hz-re csökkenti a sebességet. Ez a mechanikus megterhelés rövidtávon károsítja a centrifugákat, de a lassú szakasz az addig szétválasztott molekulák összekeveredését is eredményezi, így a gyártás hatásfoka ezáltal is degradálódik. Az egyes romboló szakaszok után a vezérlés visszaáll névleges frekvenciára. A cél a centrifuga fokozatos, észrevétlen tönkretétele és a dúsítási folyamat megzavarása. Ez utóbbi kockázatosabb formája a támadásnak, könnyebben lelepleződhet a Stuxnet, ugyanis a sebesség változtatása nem része a gyártási folyamatnak, a centrifugák zajának változását vélhetően füllel is lehet észlelni.

A fertőzés és a hatás kiváltása az alábbi ábrán látható módon 3 rétegen keresztül valósulhatott csak meg. Az 1. réteg az IT réteg, amelyen keresztül a folyamatba a káros kód bejuttatása megtörtént (windows, wincc). A 2. réteg a folyamatirányító rendszer és alrendszerei, amelyek a beavatkozásért felelősek. A Stuxnet ebben a rétegben módosította a működést. A 3. réteg maga gyártási folyamat fizikai környezete, azok a folyamatirányító rendszer által vezérelhető elemek, amelyek befolyásolása a szabályozási láncba való beavatkozást jelenti.



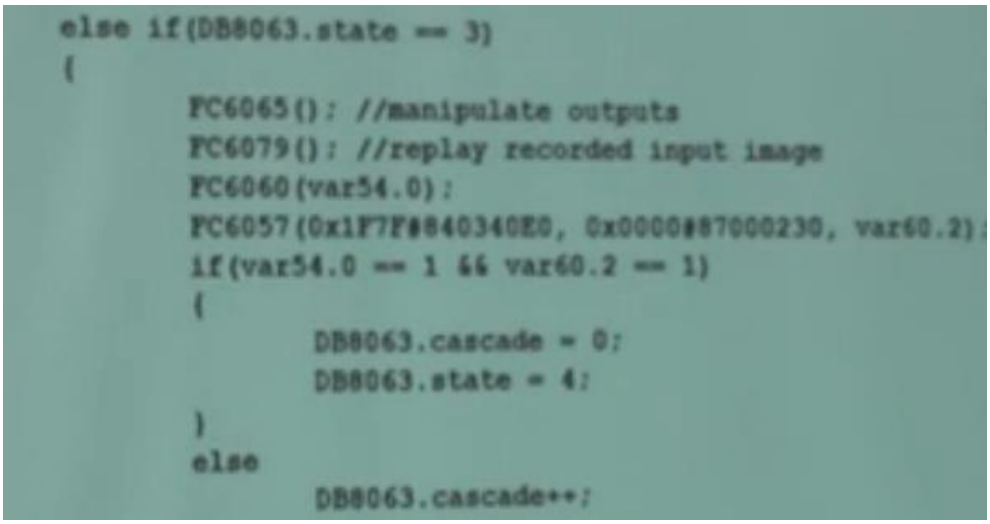
3. ábra. A Stuxnet hatásmechanizmusa

Érdemes a támadást vizsgálni az időtartományban is. A legelső változat (symantec: Stuxnet 0.500) 2005. november 3. – 2009. július 4. között, míg az azt követő (symantec: Stuxnet 1.001, Stuxnet 1.100, Stuxnet 1.101) 2009. június 22. – 2012. június 24. között működött. Ez azt jelenti, hogy a Stuxnet többlépcsős fejlődésen ment keresztül.

A vezérlőszerverekről annyit lehetett megtudni, hogy az első változat 4 vezérlőszerverrel működött négy ország területén (Egyesült Államok, Franciaország, Kanada, Thaiföld). Ezek a szerverek a fertőzés kezdeti szakaszában, még az IT rétegben voltak képesek kommunikálni a

fertőzött géppel. Magát a fertőzést egy izolált rendszerbe kellett bejuttatni, amit egy közbenső adathordozó fertőzésével valósítottak meg. Egy vélhetően szerződéses mérnöknek aki a fertőzött Step 7 projekt fájlokhoz (.s7p vagy .zip) hozzáfért és jogosult volt az izolált rendszerhez hozzáférni lehetett az összekötőkapocs a pendrive-jával.

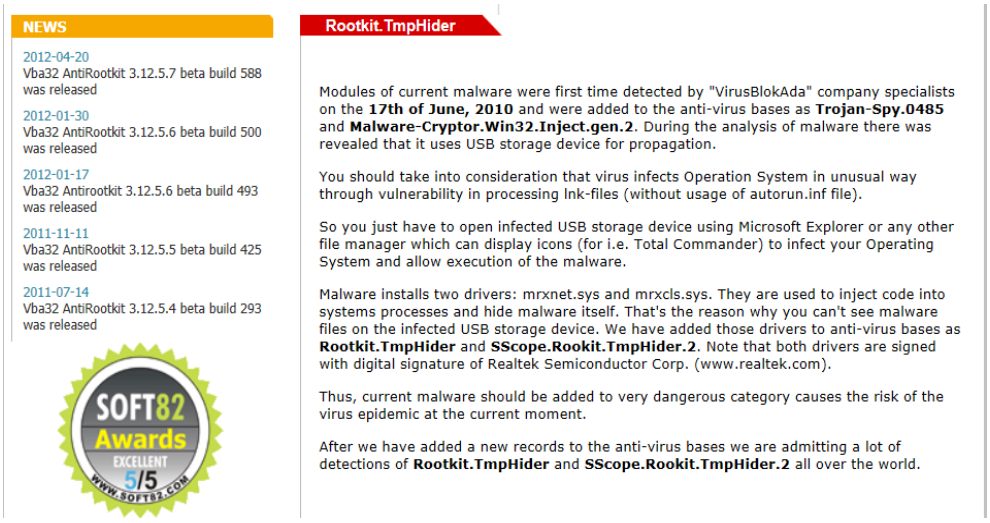
A Stuxnet kivizsgálásáról a legrészletesebb beszámolót a Symantec tette közzé. Konkrét fertőzéssel kapcsolatos adat, kód, (mélyelemzést Langner tett közzé, de nem ismert milyen forrásból jutott hozzá) nem állt a rendelkezésemre a cikk írása során, de annyi bizonyos, hogy a Stuxnet 2010-ig, tehát évekig gyakorlatilag zavartalanul működhetett. Az alábbi ábra Langner elemzéséből származik, a pszeudokód-részlet a többek között a korábban rögzített adatok visszajátszását mutatja.



4. ábra. Stuxnet visszafejtett és kommentezett kódrészlete
(Langner prezentáció)

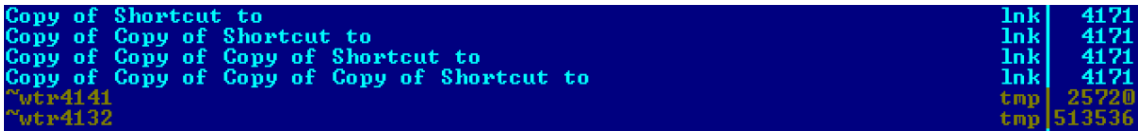
Az összesen 4 -féle változat többféle fertőzési vektorral rendelkezik, de az összes változatban közös, hogy Siemens Step 7 projekt fájlokat fertőz, USB- keresztül érkezik a fertőzés (bár itt háromféle változat létezett).

2010. június 17-én a fehérorosz VirusBlokAda antivírus szakértője Sergey Ulasen azonosította a Stuxnet 1.1000 változatát, akkor még más néven. Az első publikáció az alábbi ábrán látható.



5. ábra. Az első azonosítás
http://anti-virus.by/en/tempo.shtml

Az alábbi ábrán látható a CVE-2010-2568 sérülékenység kihasználásával fertőző pendrive tartalmának listája Far Manager-el. A két fertőzést tartalmazó fájl a VirusBlokAda munkatársaitól két elnevezést kapott, a Trojan-Spy.0485 és a Malware-Cryptor.Win32.Inject.gen.2. A tmp kiterjesztésű fájlok futtatható kódot tartalmaznak. A pendrive tartalmának explorerrel történő listázása elegendő volt a fertőzésre.



6. ábra. A Stuxnet 1.100 fertőzött pendrive tartalma

A kritikus infrastruktúra elemek kitettsége nem változott jelentősen az elmúlt években sem. A Stuxnet csak az első az azóta ismertté vált többi között, így ennek tükrében nagyobb hangsúlyt kell fektetni a kibervédelemre.

A STUXNET A TALLINI KÉZIKÖNYV TÜKRÉBEN

A támadó az Egyesült Államok és valószínűleg Izrael [8]. A *Támadó pontos kilétét meg kell állapítani* annak érdekében, hogy az arányos ellenlépés megtehető lehessen. Ez sok esetben komoly nehézségekbe ütközik. A jelenlegi meghatározáshoz az segített hozzá, hogy Cartwright nyugalmazott tábornok kiszivárogtatta [8]. A Stuxnet vezérlő és kommunikációs szervereinek vizsgálata (4 ország területén) nem tette volna lehetővé a támadó kilétének megállapítását.

A Kézikönyv alapszabálya szerint tehát *arányos ellenintézkedés* szóba jöhet.

A Stuxnet féreg véleményem szerint kritikus infrastruktúra támadását hajtotta végre. A célpont a Natanz (Irán) közelében található üzem, melyben mintegy több ezer centrifugát alkalmaztak urándúsításra. Figyelembe véve, hogy a UF_6 (urán-hexafluorid) erősen mérgező, agresszív anyag, emellett radioaktív is, ezért egy üzemi baleset előidézése személyi sérüléssel, esetleg emberi áldozatokkal járhat, ezért a *fegyveres támadás besorolás megfontolandó*.

Nem tudjuk jelenleg eldönteni, hogy összemérhető-e egy fegyveres támadással a Stuxnet, mert nem tudjuk, hogy valójában okozott-e üzemi balesetet, vagy „csak” meghibásodás történt, ami javítható volt. Amennyiben történt rombolás, áldozatok voltak, akkor azt erő alkalmazásának kell tekinteni, ugyanis a hatása felért a fegyveres támadás hatásával.

ÖSSZEGZÉS, KÖVETKEZTETÉS

A Tallinni Kézikönyv tisztázza a kiberhírszerzés, kiberhadviselés, nemzetközi jogi alapjait. Az elkészült munka alapja lehet Magyarország védelmi-, nemzeti biztonsági-, kiberbiztonsági stratégiáinak megújításának, a magyar jogalkotás kihasználhatja a Kézikönyv által összefoglaltakat annak érdekében, hogy a kiberműveletek jogi hátterét megteremtse, kiberhadviselés terén a nemzetközi hadijogi hátteret a későbbiekben átemelhesse.

A Tallinni Kézikönyv nem ad segítséget a kibertérben a területi hatály (földrajzi terület) fogalmára. A nemzetközi jog alapján minden ország felelős a területéről egy másik ország érdekeltsége ellen állami, vagy nem állami szereplő által indított támadásért. Kérdéses azonban, hogy felelőssé tehető-e egy ország azért, ha egy, a területén működő kliens gépről juttatnak be károkozó számítógépes vírust egy másik ország létfontosságú elektronikus információs rendszerébe. Ezen túlmenően a kiberhadviselésben nem tisztázott az állami és a nem állami szereplők helyzete sem, mert a kézikönyv is leegyszerűsíti a kérdést az állam területe feletti felelősségére.

A Stuxnet féreg támadás álláspontom szerint sérti a megtámadott szuverenitását (rules 1.4.), ezért arra a Kézikönyv szerint arányos ellenintézkedést (rules 13. 14.) tehet, de javasolt az

ENSZ BT összehívása. Mindazonáltal az ENSZ szankciókkal sújtott Irán ezt nyilván nem alkalmazhatta.

Fontos lenne a magyar jogalkotásnak a kiberműveletek jogi hátterét megteremteni, melynek első lépéseként a téma széleskörű konzultációja szükséges. Elsősorban meg kell határozni a Magyar Honvédség a kiberműveleti tevékenységének alapelveit [9], de ugyanilyen sürgető a többi, kiberműveletek terén illetékes területet meghatározni, valamint az alapelveket lefektetni. További kutatást igényel a kibertámadó azonosítási módszereinek kutatása és fejlesztése. Nem utolsósorban szükséges a kibertámadó-képességek kialakítása az új jogi keretek mentén.

Kiemelést érdemel, hogy a kibervédelmi képességek megerősítése még ennél is sürgetőbb, különös tekintettel az új törvényi keretek közötti lehetőségekre. Az elkövetkező évek számos kiberbiztonsági feladata között a kibervédelmi együttműködésekben rejlő szinergiák kiaknázása lehet a megoldás a hatékonyabb és kevésbé kitett kibervédelmi menedzsment kialakítására.

Felhasznált irodalom

[1] Konrad Zuse Internet Archive (letöltve: 2013.07.07.) http://zuse.zib.de/

[2] Lőcs Gyula: fejezetek az informatika történetéből *http://web.itf.njszt.hu/wp-content/uploads/2012/11/Locs_inftort11-15.pdf* (letöltve: 2013.07.07.)

[3] Dara Kerr: Mobile malware grows by 614 percent in last year http://news.cnet.com/8301-1009_3-57591042-83/mobile-malware-grows-by-614-percent-in-last-year/ (letöltve: 2013.07.07.)

[4] Ewen MacAskill, Nick Davies, Nick Hopkins, Julian Borger, James Ball: GCHQ intercepted foreign politicians' communications at G20 summits http://www.guardian.co.uk/uk/2013/jun/16/gchq-intercepted-communications-g20-summits (letöltve: 2013.07.15.)

[5] The Tallinn Manual *http://www.ccdcoe.org/249.html* (letöltve: 2013. 06. 12.)

[6] mSpy honlap http://www.mspy.com/features.html?gclid=CMfIzPbcnLgCFcyR3god4ycAHA (letöltve: 2013.07.07.)

[7] W32.Stuxnet Dossier http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (letöltve:2013.07.15.)

[8] David E. Sanger: Obama Order Sped Up Wave of Cyberattacks Against Iran The New York Times 2012.06.01. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1& (letöltve:2013.07.15.)

[9] Kassai Károly: Kiberveszély és a Magyar Honvédség. http://hadmernok.hu/2012_4_kassai.pdf (letöltve:2013.07.15.)

[10] Ralph Langner: Egy XXI. század kibernetikai fegyvere - a Stuxnet megfejtése http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (letöltve:2013.07.15.)

[11] Ralph Langner: To-kill-a-centrifuge.pdf
http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
(Letöltve:2013.12.21.)

[12] ENISA: Can we learn from SCADA security incidents?
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents/at_download/fullReport (Letöltve:2013.12.30.)

[13] Ralph Langner: Stuxnet deep dive (prezentáció)
http://www.digitalbond.com/blog/2012/01/31/langners-stuxnet-deep-dive-s4-video/
(Letöltve:2013.12.30.)

[14] Cserháti András: A STUXNET VÍRUS ÉS AZ IRÁNI ATOMPROGRAM
Fizikai Szemle 2011/5. 150.o.
http://wwwold.kfki.hu/fszemle/fsz1105/cserhati1105.html (Letöltve:2013.12.30.)

[15] Oleg Kupreev, Sergey Ulasen: Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.gen.2 Review
http://www.f-secure.com/weblog/archives/new_rootkit_en.pdf (Letöltve:2013.12.30.)

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Horváth József
horvath0101@gmail.com

ELEKTRONIKAI HADVISELÉS A MAGYAR HONVÉDSÉGBEN

Absztrakt

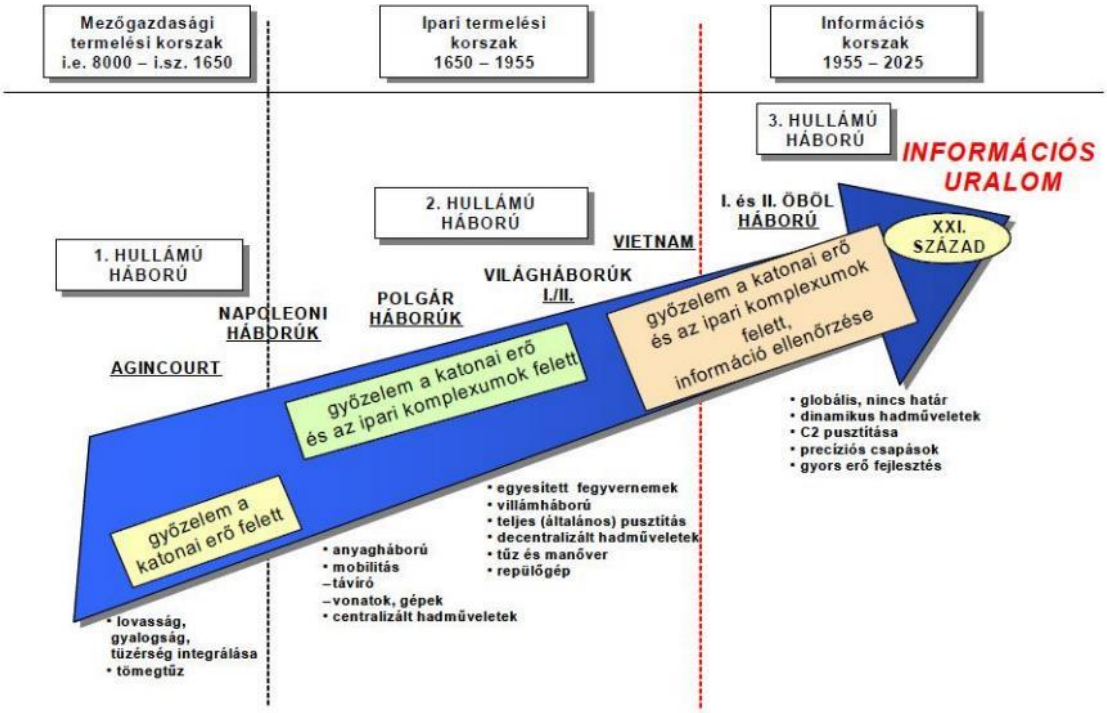
A jelenlegi, aszimmetrikus hadviselési körülmények között katonáinknak a legmodernebb, high-tech technológiára van szükségük feladataik teljesítéséhez. A mérnököknek ehhez biztosítaniuk kell az új megoldásokat, eszközöket és rendszereket, melyek képesek a legmegfelelőbb választ adni a legújabb veszélyekre és kihívásokra. Napjaink hadviselésének egyik fontos szegmense az elektronikai hadviselés, amely képes hatékonyan támogatni csapatainkat. Az eredményes támogatás elsődleges feltétele a legfejlettebb eszközök megléte. Jelen cikkben a szerző bemutatja az elektronikai hadviselés fejlődését, szerepét napjaink hadviselésében. Elemzi az elektronikai hadviselés aktuális helyzetét a Magyar Honvédségben, illetve a bemutatja a fejlesztések egyik lehetséges irányát.

During the recent, asymmetric warfare circumstances our soldiers need the most up to date, high-tech technology to fulfill their tasks. The engineers have to provide new solutions, assets and systems, which can give the most appropriate reaction for the newest risks and challenges. In the recent warfare the electronic warfare is an important segment, which is able to support the activity of our troops effectively. The primary condition of the efficient support is the state-of-the-art equipment. In this paper, the author describes the evolution of the electronic warfare and its role in the current warfare. He analyses the current situation of the electronic warfare in the Hungarian Defence Forces and shows one of the possible ways of development.

Kulcsszavak: *elektronikai hadviselés, NEWFIP, rádió-távirányítású robbanóeszköz, szoftverrádió ~ electronic warfare, NEWFIP, R-CIED, software-defined radio*

BEVEZETÉS

A technikai fejlődés újabb és újabb vívmányai nagy hatással vannak életünkre, még akkor is, ha annak az ember a maga saját – a technikai fejlődés teljes időtartamához viszonyítva – rövid élete során nem tulajdonít nagy jelentőséget. Az is lényeges, hogy az egyik nap még újdonság másnapra már az életünk szerves részét képezi, gondoljunk csak a mikrohullámú sütőre vagy a mobiltelefonra. Sok esetben pedig úgy lépünk túl az egyes eszközökön, mintha sosem léteztek volna, gondoljunk csak az úgynevezett „walkman”-re, melyekkel a maga korában mindenki úgy közlekedett, mint napjainkban a fiatal generáció a médialejátszókkal és a táblagépekkel. A technikai fejlesztések nemcsak a polgári, hanem a katonai életben is jelen vannak, sok esetben a katonai fejlesztés eredményének szándékosan csökkentett képességű változata kerül átadásra a polgári felhasználóknak. Ennek egyik példája a GPS[1], aminek katonai verziója sokáig nagyságrendekkel nagyobb pontosságot biztosított az arra jogosult felhasználók részére, mint a kereskedelmi forgalomban kapható verzió. A katonai és polgári életben alkalmazott technika fejlődése szoros kapcsolatban áll, hatásuk a hadviselésben is megjelenik, melyet az alábbi ábra illusztrál.



1. ábra. Az ipar és a hadviselés fejlődése közötti párhuzam [1]

A hadviselés módját jelentősen megváltoztató technikai újítások között mindenképpen meg kell említeni a lőfegyvert, a repülőgépet, a rádiót és az informatikai eszközöket. Fontos az is, hogy egy-egy technikai fejlesztés megjelenése mindig egyet jelentett az új eszköz illetve rendszer hatékony alkalmazását korlátozó, vagy teljes mértékben akadályozó eljárások és eszközök rövid időn belül történő kifejlesztésével.

Napjaink információs technológiáján alapuló hadviselésének egyik fontos eleme az elektronikai hadviselés, melynek kialakulását és az aszimmetrikus hadviselésre jellemző alkalmazási területeit mutatom be a következő fejezetben.

[1] Globális helymeghatározó rendszer, Global Positioning System

AZ ELEKTRONIKAI HADVISELÉS KIALAKULÁSA

A rádió 1901-ben történő bemutatása magában hordozta a katonai alkalmazásba vételt és természetesen útjára indította a rádiófelderítés kialakulását, hiszen valamennyi katonai vezető számára fontos információt hordoznak az elfogott rádióadások, legyen az maga az üzenet, vagy akár a forgalmazási sajátosságok alapján felfedett alegység tevékenysége, mozgása. Sok esetben azonban nem volt fontos a rádióadás tartalma, vagy nagyobb biztonságot jelentett a frekvenciatartomány zavarása, így megjelent az igény az elektronikai zavarás eszközeinek kifejlesztésére. A radarok 1930-as évek körüli alkalmazásba vétele pedig egyet jelentett a rádiótechnikai felderítés és zavarás megjelenésével. A különböző technikai rendszerek kifejlődésével vált az elektronikai hadviselés egy olyan széles spektrumot átfogó területté, melyet napjainkban ismerünk.

„Az elektronikai hadviselés azon katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza a frekvenciaspektrum ellenség részéről történő használatát és biztosítja annak a saját csapatok általi hatékony alkalmazását. Területei az elektronikai támogató tevékenység[2], az elektronikai ellentevékenység[3] és az elektronikai védelem. Az elektronikai támogató tevékenység az elektronikai hadviselés azon része, amely magába foglalja – a fenyegetés azonnali jelzése érdekében – az elektromágneses kisugárzások felkutatására, elfogására, és azonosítására, valamint a források helyének meghatározására irányuló tevékenységeket. Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát. Az elektronikai ellentevékenység egyik területe az elektronikai zavarás, amely az elektromágneses energia szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti azzal a céllal, hogy megakadályozzuk az ellenség elektronikai eszközeinek vagy rendszereinek hatékony működését. Az elektronikai védelem az elektronikai hadviselés azon része, amely biztosítja az elektromágneses- és egyéb spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére.” [2]

Az elektronikai hadviselés tevékenységének megértéséhez fontos az is, hogy tisztázzunk egy olyan félreértést, amely számos helyen felfedezhető a SIGINT[4]-ről és az elektronikai hadviselés támogató tevékenységéről szóló cikkekben.

Az angol terminológiából átvett SIGINT kettő területből tevődik össze, ezek a COMINT[5] és az ELINT[6]. Sok esetben a SIGINT elnevezést használják olyan esetekben, amikor egyszerűen csak annak részterületéről, a rádiófelderítésről, azaz a COMINT-ról beszélnek. [3]

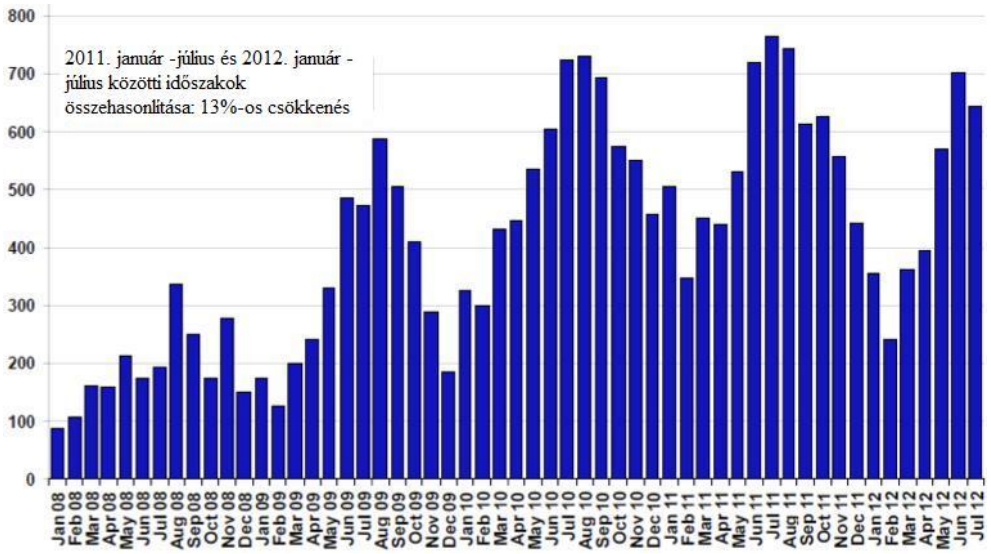
A félreértést az okozza, hogy ez a két terület sok esetben ugyanolyan képességgel bíró eszközöket alkalmaz, azonban a kapott információ felhasználásának módja eltér egymástól. „Az elektronikai támogatás harci információkat szolgáltat, amelyeket fel lehet használni elektronikai ellentevékenységhez, tüzérségi tűz-, vagy repülőcsapások kiváltásához, a csapatok manőveréhez, vagy a veszély elhárításához. Mindezt a vett információ gyors analizálása és feldolgozása, valamint viszonylagosan rövid érvényességi ideje jellemzi. A SIGINT ugyanakkor felderítési információkat továbbít az összfegyvernemi törzs felé a parancsnoki döntéstámogatás céljából.” [4]

[2] Szintén alkalmazott megnevezés: elektronikai megfigyelés, electronic surveillance, ES. A szerző megjegyzése.
[3] Szintén alkalmazott megnevezés: elektronikai támadás, electronic attack, EA. A szerző megjegyzése.
[4] Jelfelderítés, Signal Intelligence, SIGINT
[5] Rádiófelderítés, Communication Intelligence, COMINT
[6] Rádiótechnikai felderítés, Electronic Intelligence, ELINT

AZ ELEKTRONIKAI HADVISELÉS ALKALMAZÁSA AZ ASZIMMETRIKUS HADVISELÉSBEN

A napjainkra jellemző aszimmetrikus hadviselésben az elektronikai hadviselés fontos szerepet játszik, ezzel bizonyítva, hogy nemcsak a hagyományos hadviselésben képes ezen terület jól kiképzett szakállománya hatékonyan részt venni az erők védelmében vagy az információszerzésben. Számos nemzet vesz részt békeműveletekben és kijelenthető, hogy minden esetben ellátják csapataikat a személyi állomány és a technikai eszközök védelme érdekében a rádió-távirányítású improvizált robbanóeszközök (R-CIED[7]) semlegesítésére alkalmazható elektronikai zavaróeszközökkel illetve több nemzet is alkalmaz COMINT eszközöket a szemben álló fél kommunikációjának „elfogására". [5]

A 2. ábrán az ISAF[8] jelentése alapján látható az improvizált robbanóeszközökkel elkövetett, úgynevezett IED[9] támadások alakulása. 2011-ben emelkedés volt tapasztalható 2010-hez képest, majd a 2012-es évben csökkenés következett be, az incidensek száma a 2010-es év eredménye alá süllyedt. Az ISAF jelentések azt mutatják, hogy a civil áldozatok 60%-a a lázadók IED támadásainak eredménye, akik ezen támadási módszert, mint háborújuk legalapvetőbb eszközét kezelik. [6]



2. ábra. IED támadások számának alakulása Afganisztánban [7]

Az IED-k egyik típusa a már korábban említett R-CIED, amelynek hatékony ellenfele az alábbi képen is látható, gépjárművekbe épített vagy hordozható kivitelű elektronikai zavaróeszköz, a köznyelvben már elterjedt angol nevén jammer. Ezen eszközök miatt az elektronikai zavarás az a terület, amely a hétköznapi ember számára az elektronikai hadviselés tevékenységei közül a leginkább előtérben van, hiszen a sajtóban napi szinten lehet látni ilyen eszközökkel felszerelt gépjárműveket.

[7] Rádió-távirányítású improvizált robbanóeszközök, Radio Controlled Improvised Explosive Devices, R-CIED

[8] NATO vezetésű biztonsági erők elnevezése Afganisztánban, Nemzetközi Biztonsági Közreműködő Erő, International Security Assistance Force, ISAF.

[9] Improvizált robbanóeszközök, Improvised Explosive Devices, IED

3. ábra. Magyar jelzésű HMMWV zavaróeszközének antennái az MH PRT táborában [8]

Afganisztáni tapasztalatom, hogy a Mazar-e Sharif-be telepített német Tornado repülőgépeket az erők védelme érdekében a csapatok felvonulási útján számos alkalommal alkalmazták az R-CIED eszközök ellen úgynevezett „burning”[10] eljárásra, amellyel a rádiótávirányítási rendszert próbálták hatástalanítani. Erre azért volt szükség, mert egy jól megkonstruált IED az alábbi képen is látható pusztításra volt képes még egy ilyen erősen páncélozott harcjárműben is.

4. ábra. IED támadásban megsemmisült amerikai jármű, Afganisztán [9]

ELEKTRONIKAI HADVISELÉS A MAGYAR HONVÉDSÉGBEN

A korábbi évtizedekben a Magyar Honvédség számos olyan alegységgel rendelkezett, melyeket ebben az időszakban rádióelektronikai harcnak illetve elektronikai harcnak nevezett feladatra hoztak létre. 1974. december 16-án alakult meg a Magyar Néphadsereg Vezérkar Rádióelektronikai Főnökség illetve a Rádióelektronikai Ellenőrző Központ Budapesten. Ezen kívül számos szervezet került létrehozásra illetve megszüntetésre az évek folyamán. Néhány ilyen egység és alegység neve a teljesség igénye nélkül: 69. Önálló Rádiózavaró Zászlóalj, a 57. Önálló Légvédelmi Zavaró Zászlóalj és a 81. Önálló Honi Légvédelmi Zavaró Zászlóalj Békéscsabán, a Győrben történt megalakítása után 7 évvel később MH 78. Gróf Pálffy Miklós Elektronikai-harc Századra átszervezett MN 78. Rádiózavaró Század, a pécsi 29. Elektronikai-harc Század, az egri 92. Elektronikai-harc Század. A fegyvernem életében fontos fordulópont 1992, amikor az MH akkori elektronikai harc erőit a kiskunfélegyházi 5. Kiskun Elektronikai Harc Ezredbe vonták össze, illetve 2001, amikor az 5. Kiskun Elektronikai Harc Ezred Egerbe diszlokált át és századdá alakult. [10] [11]

Az MH elektronikai hadviselési képessége, szakállománya és technikai eszközparkja az elmúlt évtizedben hatalmas változásokon ment keresztül. A korábbi alakulatok száma

[10] Burning: égetés

lecsökkent, jelenleg 1-2 helyőrségben koncentrálódnak a szaktechnikával rendelkező alegységek. Ezen cikkemben elsődlegesen a jelenleg is funkcionáló szervezetekkel foglalkozom, ezek feladatrendszerét elemzem, azonban bemutatom az elektronikai hadviselésben érintett többi szervezet tevékenységét is.

Szaktechnikával rendelkező alakulatok közé tartozik az MH 5. Bocskai István Lövészdandár kötelékében lévő MH 5/24 Bornemissza Gergely Felderítő Zászlóalj Elektronikai Hadviselés százada (továbbiakban: EHV század), valamint az MH 59. Szentgyörgyi Dezső Repülőbázis (továbbiakban MH 59. SZDRB) Gripen repülőgépeinek elektronikai hadviselési (továbbiakban EHV) képességét kezelő Elektronikai Hadviselési Támogató Központja.

Az MH 5/24 Bornemissza Gergely Felderítő Zászlóalj EHV százada jogutódja a 2001-ben megalakult egri századnak. [12]

„A zászlóalj szervezeti elemei:

- - zászlóalj parancsnokság;
- - felderítő-adatértékelő csoport;
- - csapatfelderítő század;
- - felderítő század;
- - harcászati hírszerző század;
- - elektronikai hadviselés század;
- - támogató szakasz.” [13]

Az EHV század eszközei között egyaránt megtalálhatóak a korábbi évtizedekben alkalmazott rendszerek, valamint újabb beszerzésű típusok is. A 70-es évekből fennmaradt állomások alapvetően a rádiófelderítő technikák, amelyek a hagyományos, analóg adatforrások felderítésére képesek. Megtalálhatóak közöttük az R-1378 rövidhullámú rádiófelderítő állomás (FLÓRA), az URH/F és az URH/L rádiófelderítő állomások. A viszonylag új beszerzésű, jelenleg rendszeresített zavaróeszközök kizárólag az R-CIED-k indítóeszközeinek (rádióberendezések, GSM, CDMA telefonok) zavarására alkalmasak, korlátozott frekvenciasávban és teljesítménnyel használhatóak. A nagy hatékonyságú, a szemben álló fél elektronikai eszközeinek lefogására alkalmas zavarás biztosításához nem elegendőek. [14]

Az MH 59. SZDRB Elektronikai Hadviselési Támogató Központja a Gripen beszerzést követően került megalakításra. A központ feladata a fenyegetettség és ellentevékenységi könyvtárak kialakítása, fejlesztése, ellenőrzése, valamint ezek fedélzeti számítógépbe való betöltése. A repülések után az eredmények kiértékelése, a kapott eredmények alapján a könyvtárak pontosítása majd a módosított könyvtárak tesztelése történik. [15]

Az eredmények kiértékelése a különböző elektronikai kisugárzó eszköz jellemzőit tartalmazó adatbázisok alapján történhet, amelynek jó alapja lehet például a NATO kisugárzó eszközök (NEDB[11]) adatbázisa, vagy egy speciálisan erre a célra kialakított saját, honi adatbázis.

A Gripen EHV feladatrendszerében alkalmazott eszközök viszonylag új fejlesztésűek, azonban mint arra már egy korábbi cikkemben is rámutattam, már most elérhető hozzá újabb, a könyvtárrendszerek szerkesztésében nagy segítséget nyújtó támogató rendszer, amely nagyobb pontosságú adatbázis kialakítását tesz lehetővé rövidebb idő alatt. [16]

Mivel már a Gripen viszonylag új fejlesztésű EHV rendszeréhez is érhetőek el újabb fejlesztések, gondoljuk végig, milyen technikai változások következhettek be az EHV század technikai eszközei vonatkozásában, azok beszerzése óta eltelt 30-40 év alatt.

Az előző bekezdésekben olyan alakulatokkal foglalkoztam, amelyek szervezetszerű elektronikai hadviselés alegységgel rendelkeznek, de fontos megemlíteni azon alakulatokat is, melyeknek bár nincs EHV alegysége, azonban mindennapi életük szerves részét képezi az elektronikai hadviselés egyes feladatainak gyakorlása. Ezek a Győrben települő MH 12.

[11] NATO Emitter Database

Arrabona Légvédelmi Rakétaezred, a Veszprémben települő MH 54. Veszprém Radarezred illetve a szintén Veszprémben települő MH Légi Vezetési és Irányítási Központ. Ezen alakulatok, kiegészítve az MH 59. SZDRB erőivel, részt vesznek az évente megrendezésre kerülő NEWFIP (NATO Electronic Warfare Integration Period) elnevezésű, többnemzeti elektronikai hadviselés gyakorlaton, melynek jelen cikk írója is aktív szervezője 2012 óta. A gyakorlat célja a NATO Integrált Lég- és Rakétavédelmi Rendszer, a NATINAMDS[12] részét képező nemzeti egységek, alegységek felkészítése az elektronikai hadviselési vonatkozású, általában védelmi jellegű tevékenységek végrehajtására.

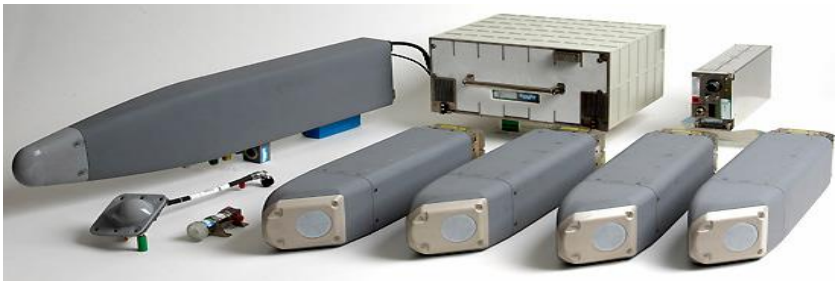
A fentieken kívül még más alakulatoknál is folyik felkészítés az elektronikai hadviseléssel kapcsolatban. Jelen cikk írója volt a főszervezője az alakulatoknál rendszeresített rádiólokációs álcázó eszközök, az úgynevezett szögvisszaverők telepítésének legutóbbi gyakorlásának, melyre 2013. szeptember 17-én került sor.

A feladat során az MH 37. II. Rákóczi Ferenc Műszaki Ezred szakállománya a szentesi, tiszai vízi gyakorlótéren két szögvisszaverő típussal (Szféra és Piramida) épített imitált hidat a telepített PMP szalaghíd mellett, illetve távolabb, a hékédi gyakorlótér bekötőútján az OMU szögvisszaverő ernyőkkel a szárazföldi erők mozgását álcázták. A két helyszínen végrehajtott telepítés egy komplex feladat részét képezte, mivel a telepítés befejezésekor az MH 59. Szentgyörgyi Dezső Repülőbázis Gripenjeinek radarjai tesztelték a telepítés hatékonyságát, azaz azt, hogy melyik szögvisszaverő típussal imitált híd látható a pontonhíd mellett a radarfelvételeken, illetve azt, hogy az OMU szögvisszaverővel milyen hatékonyan lehet rejteni a csapatok mozgását a fejlett technológiát képviselő Gripen PS-05/A radarjával szemben. [17]

Mielőtt továbblépnénk a következő fejezetre, szót kell ejtenünk még egy funkcióról, melyet egy már korábban említett, jelenleg nem létező elektronikai hadviselési szervezet gyakorolt. Ez pedig az anno gödöllői központtal üzemeltetett, a Vezérkar közvetlen alárendeltségében működő Rádióelektronikai Ellenőrző Központ (RELEK) volt, amely a kor színvonala feletti technikai felszereltséggel rendelkezett. A RELEK feladata kettő részből állt. Egyrészt ellenőrzési funkciót gyakorolt a híradó rendszerek felett, másrészt a fejlesztő tevékenységet támogatta. A híradó-biztonsági, álcázási, elektronikai kisugárzási rendszabályok betartásának ellenőrzését az Északi-középhegység, a Dunántúli-középhegység és az Alpokalja magaslatai felhasználásával kiépített „Egérfogó” rendszerrel végezte a RELEK állománya. [18] [19]

MERRE TOVÁBB?

Magyarország számos külföldi misszióban vett már részt, melyekben az elektronikai zavaró eszközök alkalmazásra kerültek és hamarosan egy újabb, eddig ismeretlen területen is bevetésre kerülnek a Magyar Honvédség erői. A Gripenek a Baltikum területén légtérrendészeti feladatokat fognak ellátni 2015 – 2018 között, ahol a gépek önvédelemi rendszerét képező elektronikai hadviselési rendszernek is (EWS[13]-39) fontos szerep jut majd. [20]



5. ábra. JAS-39 Gripen EWS-39 ellentevékenységi rendszerének elemei [21]

[12] NATO Integrated Air and Missile Defence
[13] Elektronikai hadviselési rendszer, Electronic Warfare System, EWS

Az elektronikai hadviselés és az elektrooptikai ellentevékenység az egyike azon katonai tevékenységeknek, melyekre az amerikai elnök, Barack Obama 2012-ben a korábbi évekhez képest is növekvő költségvetési keretet kért a 2013. évre vonatkoztatva, összegszerűen 4,95 milliárd dollárt. A keret egy része 12 db U.S. Navy Boeing EA-18G Growler elektronikai hadviselési feladatokra képes repülőgép vásárlására volt betervezve. A repülőgéptípus képességei között szerepel a szemben álló fél légvédelmének elnyomása, radarok zavarása, valamint aktív elektronikai kisugárzással működő légvédelmi radarok rombolása Raytheon AGM-88 (High-speed Anti-Radiation Missile, HARM[14]) típusú rakétával. [22]

6. ábra. Boeing EA-18G Growler elektronikai hadviselési célú repülőgép [23]

Egy másik jelentős pénzügyi tétel a Joint IED Defeat Organization (JIEDDO) szervezet „Attack the network"[15] projektjének támogatása. A program fő célja az improvizált robbanóeszközöket előállító hálózatok (pénzügyi támogatók, készítők és kiképzők, valamint az ezen tevékenységet támogató infrastruktúra) rombolása felderítési, célmeghatározási-céltervezési[16], biometrián alapuló azonosítási illetve helyszínelő képességek biztosításával. Az elektronikai hadviselési célú kiadások növelésével Barack Obama azt reméli, hogy képesek lesznek megfékezni a terroristákat, még mielőtt azok lecsapnának valahol. Az Amerikai Védelmi Minisztérium által a 2014. évre benyújtott pénzügyi tervben is kiemelt prioritásként kezelik az elektronikai hadviselést, számos pontban megemlítik, mint az egyik fontos részterület. Példaként kiemelném, hogy a tudomány és technológia alprogramon belül 500 millió dollárt terveztek be az elektronikai hadviselés fejlesztésére. [24] [25]

A fenti példák is alátámasztják, hogy érdemes és szükséges ezen képesség fejlesztésére forrásokat biztosítani, mint ahogy azt teszi az egyik legnagyobb katonai hatalom is. Fontos azonban az is, hogy egy, az USA földrajzi méreteihez és gazdasági helyzetéhez viszonyítva jelentősen kisebb ország is hatékony fejlesztésekre és beruházásokra lehet képes, megfelelő tervezés esetén.

A modern elektronikai hadviselési eszközök szükségessége nem lehet kérdés a Magyar Honvédség keretén belül sem, hiszen valamennyi ország jelentős költségeket fordít ezen feladatok végrehajtásához szükséges eszközök fejlesztésére és beszerzésére. Fontos szempont az is, hogy az MH érdekeit nem feltétlenül szolgálja más országok által már kiselejtezett eszközök átvétele, azok állapota illetve technológiai értelemben vett elavultsága miatt. Ebben az esetben azt is figyelembe kell venni, hogy ezen eszközök technikai paraméterei ismertek több alkalmazó előtt is. Ugyanez a helyzet áll fenn a különböző gyártók által előállított technikai eszközök esetében is, hiszen valamennyi potenciális vásárló részletes információt kap az adott eszköz képességeiről.

[14] High-speed Anti-Radiation Missile: nagysebességű radarromboló rakéta
[15] „Támadd a hálózatot!", a szerző saját fordítása
[16] Targeting: AAP-6 alapján.

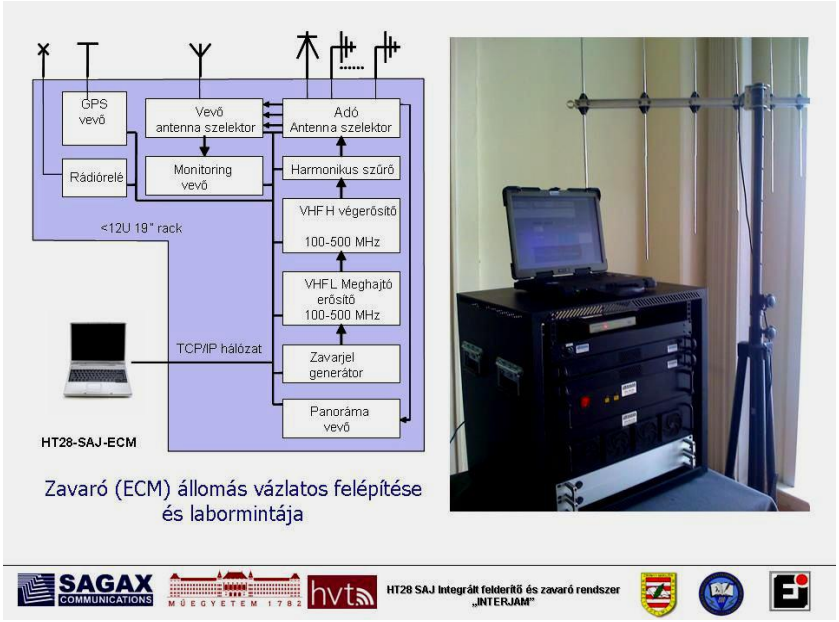
A NATO 2006-2016 közötti időszakra vonatkozó haderőtervezési javaslata (2006 Force Proposals for Hungary) Magyarország részére több elektronikai hadviselési vonatkozású javaslatot is tartalmaz. „Egy dandár elektronikai hadviselési képességére vonatkozó leírás:

- kettő iránymérő alap (minimum három rádió-iránymérő állomás egységes vezénylésével);
- lehallgató munkahelyek, amelyek egyidejűleg hat HF, VHF, UHF és SHF frekvenciasávban működő eszközök felderítésére képesek;
- rádiótechnikai felderítő képesség meghatározott frekvenciatartományban;
- érzékelő-elemző központ, ahol megvalósul a NATO szövetségi felderítő és elektronikai hadviselési informatikai rendszerhez történő kapcsolódás;
- kettő kommunikációs mobil zavaróállomás.” [26]

A fentiek alapján egyértelműen kijelenthető, hogy az MH elektronikai hadviselési rendszerében szükség van több feladat elvégzését is biztosító, komplex rendszer kidolgozására, rendszeresítésére, amelyre egy Magyarországon kifejlesztett, a szoftverrádió technológián alapuló eszköz megfelelő lehet. Szoftvertechnológia esetén olyan eszközökről beszélünk, melyek működését az alkalmazott szoftver határozza meg, a szoftver fejlesztésével, átírásával a működés jelentős mértékben módosítható, természetesen a rendszerhez kapcsolódó elemek által szabott határokon belül. A korábbi, egy-egy frekvenciatartományban üzemelő eszközök esetleges modernizációja nem lehet alternatíva, mivel annak végrehajtása gazdaságtalan lenne. A szoftverrádió elméleten alapuló készülékek a megfelelő egyéb rendszerekkel (pl. különböző frekvenciatartományban dolgozó antennarendszerek) kiegészítve jóval szélesebb spektrumban képesek dolgozni, megoldható lehet a felderítés és zavarás egy eszközzel történő végrehajtása. A különböző szintekhez tartozó feladatok meghatározása után megtörténhet az eszköz elvárt paramétereinek meghatározása, majd következő lépésként több állomás egy rendszerbe kapcsolása. Ezen metódus alapján viszonylag rövid idő alatt lehetséges egy hatékony, több feladatra is alkalmazható elektronikai hadviselési rendszer kialakítása. [27] [28] [29]

Ilyen jellegű kezdeményezés volt az Integrált elektronikai felderítő és zavaró rendszer fejlesztése, az Interjam-projekt.

A pályázatot egy négy tagból álló konzorcium nyújtotta be a Nemzeti Kutatási és Technológiai Hivatalhoz a Kutatás-fejlesztési Pályázati és Kutatáshasznosítási Iroda által 2007-ben hirdetett Jedlik Ányos Programra. [30]



7. ábra. Interjam projekt, zavaró állomás vázlatos felépítése és labormintája [30]

„A konzorcium tagjai voltak:

- SAGAX Informatikai Szervező és Tanácsadó Kft;
- a Budapesti Műszaki és Gazdaságtudományi Egyetem, Szélessávú Hírközlés és Villamosságtan Tanszéke;
- a Zrínyi Miklós Nemzetvédelmi Egyetem Információs Műveletek és Elektronikai Hadviselés Tanszéke, valamint
- a HM Elektronikai, Logisztikai és Vagyonkezelő ZRt.” [30]

A projekt fő célkitűzése egy olyan két fő egységből álló felderítő-zavaró berendezés kifejlesztése és prototípusának megépítése volt, amely a 20-3000 MHz frekvenciasávban képes elektronikai felderítést és mintegy 800 W kimenő teljesítménnyel elektronikai zavarást végrehajtani. [30]

A szoftverrádió technológián alapuló EHV eszközök beszerzésével és azok egy, a NATO elveknek is megfelelő vezetési rendszerbe történő beintegrálásával a jelenleg is meglévő elektronikai felderítő és zavaró képesség még magasabb szintre emelhető, valamint a második fejezetben is említett elektronikai ellenőrzési funkció is visszaállítható.

ÖSSZEGZÉS

A világ modern hadseregeiben mindig is fontos volt a fejlett technológia alkalmazása, legyen az a lőfegyver, a repülőgép vagy korunk mindennapi használati eszköze, a számítógép. Napjaink hadviselésére jellemző, hogy nagymértékben alkalmaz kisugárzó elektronikai eszközöket is. Ez alátámasztja azon elgondolásokat, melyek arra ösztönzik a fejlesztőmérnököket, hogy az elektronikai hadviselés minden területével érdemes foglalkozni. Az első fejezetben röviden ismertettem az elektronikai hadviselés fejlődését és részterületeit. Bemutattam, hogy az elektronikai hadviselés területei a valós életben is bizonyítanak, azaz nemcsak elméleti szakterület, hanem a kifejlesztett eszközök valóban hasznosak, akár életet is menthetnek. A második fejezetben az MH elektronikai hadviselés szervezeteinek, technikai eszközeinek és gyakorlatainak rövid ismertetésével alátámasztottam, hogy a fejlesztésekhez szükséges szervezeti alapokkal, valamint a fejlesztések alkalmazásához szükséges állománnyal a Magyar Honvédség rendelkezik. A harmadik fejezetben az USA példája felhasználásával rámutattam, hogy a beruházásoknak több iránya lehetséges, lehet az már egy kifejlesztett eszköz megvásárlása, egy szervezet feladatrendszerének pénzügyi támogatása vagy saját fejlesztések elindítása.

Véleményem szerint a cikkben foglaltak alapján kijelenthető, hogy minden hadseregben, így a Magyar Honvédségben is fontos a technikai eszközök folyamatos fejlesztése, az új technológiák bevezetése. Szerencsére nem kell mindig újat kitalálni, rendkívül hasznos és költséghatékony megoldás valamely már létező eljárás vagy rendszer adoptálása. Ilyen eszközrendszerre nagyon jó példa a szoftverrádió technológia, amely a benne rejlő lehetőségek kiaknázása esetén a Magyar Honvédség elektronikai hadviselési képessége szempontjából jelentős és időtálló fejlesztést jelentene a napjainkra jellemző nehéz gazdasági helyzetben szükséges költséghatékonyságot is szem előtt tartva.

Felhasznált irodalom

[1] Dr. Haig Zsolt alezredes – Dr. Várhegyi István nyá. ezredes: *A vezetési hadviselés alapjai.* Budapest: 2000., ZMNE, Egyetemi jegyzet.

[2] MH Összhaderőnemi Elektronikai Hadviselési Doktrína. MH DSZOFT Kód: 11222. HM HVK Felderítő Csoportfőnökség kiadványa, 2005. 6-8 pp.

[3] Balogh Péter: A Magyar Honvédség ISTAR (ISR) képességei, a fejlesztés lehetséges irányai, különös tekintettel az elektronikai hadviselésre. Hadmérnök, VII. Évfolyam 4. szám - 2012. december, 75-94. oldal, ISSN 1788-1919

[4] Dr. Haig Zsolt mk. alezredes: Az információs műveletek, a SIGINT és az elektronikai hadviselés kapcsolatrendszere. KFH felderítő szemle, VI. évfolyam, különszám, 2007. február, 27-47. oldal, ISSN 1588-242X

[5] Germany's Tornado: Berlin Mulls Deploying Spy Jets to Southern Afghanistan. Forrás: http://www.spiegel.de/international/spiegel/germany-s-tornado-berlin-mulls-deploying-spy-jets-to-southern-afghanistan-a-456013.html letöltve: 2013. október 13. A szerző saját fordítása.

[6] Thomas Joscelyn & Bill Roggio: Analysis, the Taliban's 'momentum' has not been broken. Forrás: http://www.longwarjournal.org/archives/2012/09/analysis_the_taliban.php letöltve: 2013. október 18

[7] Thomas Joscelyn & Bill Roggio: Analysis, the Taliban's 'momentum' has not been broken. Forrás: http://www.longwarjournal.org/images/Afghan-executedIED-attacks-ISAF-data-Aug2012-page.jpg letöltve: 2013. október 19.

[8] A szerző saját felvétele, Afganisztán, Pol-e Khomri, 2010. október.

[9] Mirwais Adeel: US troops may face more IED attacks in Afghanistan. Forrás: http://www.khaama.com/us-troops-may-face-more-ied-attacks-in-afghanistan-2056 letöltve: 2013. október 13.

[10] Szűcs László: Lehallgatásból önálló fegyvernem. Forrás: http://www.honvedelem.hu/cikk/13362 letöltve: 2013. október 18.

[11] Magyar Honvédség 78. Gróf Pálffy Miklós Elektronikai harc század évkönyve, 1985-1995., Győr

[12] A Magyar Honvédség 5. Bocskai István Lövészdandár története II. 2004–2008., Debrecen: 2009. Magyar Honvédség, ISBN 978-963-06-4151-7

[13] Balogh Péter: A Magyar Honvédség ISTAR (ISR) képességei, a fejlesztés lehetséges irányai, különös tekintettel az elektronikai hadviselésre. Hadmérnök, VII. Évfolyam 4. szám - 2012. december, 80-81 p. oldal, ISSN 1788-1919

[14] Balogh Péter: A Magyar Honvédség ISTAR (ISR) képességei, a fejlesztés lehetséges irányai, különös tekintettel az elektronikai hadviselésre. Hadmérnök, VII. Évfolyam 4. szám - 2012. december, 83. p. oldal, ISSN 1788-1919

[15] Dr. Kovács László: A légierő elektronikai hadviselése a terrorizmus elleni harcban. Repüléstudományi közlemények különszám, 2008. április 11., ISSN 1789-770X

[16] József Horváth: JAS 39 Gripen in air operations, Repüléstudományi közlemények, XXV. évfolyam, 2013. 2. szám, 394-404. oldal, ISSN 1789-770X A szerző saját fordítása.

[17] Antal Ferenc: Átkelés és álcázás. Forrás: http://www.honvedelem.hu/cikk/40053 letöltve: 2013. október 13.

[18] Ványa László: Az elektronikai hadviselési csapatok: hogyan tovább? Hadtudomány, 2001. február 05., ISSN 1215-4121 Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/2001/2/05/chapter1.htm letöltve: 2013. október 13.

[19] Bozsóki Attila: Az elektronikai harc gyakorlatok kiképzési tapasztalatai, együttműködés lehetőségei a légierő csapataival. Repüléstudományi konferencia 2012, XXIV. évfolyam, 2012. 2. szám, 7-32. oldal, ISSN 1789-770X

[20] Rendkívül hálásak a balti államok Magyarországnak. Forrás: http://www.kormany.hu/hu/honvedelmi-miniszterium/hirek/rendkivul-halasak-a-balti-allamok-magyarorszagnak letöltve: 2013. október 13.

[21] Dr. Kovács László: A JAS 39 Gripen elektronikai hadviselési képességei. Forrás: http://www.szrfk.hu/rtk/kulonszamok/2006_cikkek/kovacs_laszlo.pdf letöltve: 2013. október 13.

[22] Electronic Warfare Spending Rises in 2013 Budget Request (Chandler Harris). Forrás: http://news.clearancejobs.com/2012/03/15/electronic-warfare-spending-rises-in-2013-budget-request/ letöltve: 2013. október 13. A szerző saját fordítása.

[23] Picture of the Boeing EA-18G Growler Electronic Warfare Platform. Forrás: http://www.militaryfactory.com/imageviewer/ac/pic-detail.asp?aircraft_id=388&sCurrentPic=pic8 letöltve: 2013. október 13.

[24] Electronic Warfare Spending Rises in 2013 Budget Request (Chandler Harris). Forrás: http://news.clearancejobs.com/2012/03/15/electronic-warfare-spending-rises-in-2013-budget-request/ letöltve: 2013. október 13. A szerző saját fordítása.

[25] United States Department of Defense, Fiscal Year 2014 Budget Request. Forrás: http://comptroller.defense.gov/defbudget/fy2014/FY2014_Budget_Request_Overview_Book.pdf letöltve: 2013. október 18. A szerző saját fordítása.

[26] Miskolczi József okl. mk. alezredes: A Magyar Honvédség elektronikai hadviselési erői és eszközei, alkalmazásuk lehetőségei. KFH felderítő szemle, VI. évfolyam, különszám, 2007. február, 143-151. oldal, ISSN 1588-242X

[27] Kommunikáció - 2006: Dr. Ványa László: Út a szoftverrádiók és a szoftver rádiózavaró állomások felé. Budapest: 2006. ZMNE, 76-83. oldal, ISBN 978-963-7060-18-2.

[28] Fürjes János: Korszerű rádiófelderítés kihívásai az információs műveletekben. Hadmérnök, III. Évfolyam 2. szám - 2008. június, 88-95. oldal, ISSN 1788-1919

[29] What is Software Defined Radio? Forrás: http://www.wirelessinnovation.org/introduction_to_sdr letöltve: 2013. október 23. A szerző saját fordítása.

[30] Dr. Ványa László: Az INTERJAM projekt első éve. Forrás: http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/04_Vanya_Laszlo.pdf 61-70. pp. letöltve: 2013. november 21.

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Kassai Károly
karoly.kassai@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELMI RENDSZABÁLYOK KATONAI SPECIFIKÁCIÓJÁNAK KIALAKÍTÁSA, A CIVIL ÖNKÉNTES TÁMOGATÁS MEGVALÓSÍTÁSÁNAK FONTOSABB KÉRDÉSEI

Absztrakt

Az utóbbi öt évben a Parlament és a Kormány törvényeket és rendeleteket adott ki egy naprakész, NATO és EU interoperabilis menedzsment és adminisztratív követelmények, technikai rendszabályok jogi megalapozása érdekében a közigazgatási szervezetek megfelelő szintű információbiztonságáért. A követelmények közös alkalmazása nem mindennapi kihívást jelent az alkalmazó szervezetek számára beleértve a Magyar Honvédséget is. A cikk célja a híradó-informatikai rendszerek biztonsági osztályba sorolási problémájának-, a kár és káros hatás katonai specifikációjának-, valamint a honvédelmi szervezetek szervezeti biztonsági szintbe sorolásának megértése az új Információbiztonsági Törvény (Ibtv. 2013.) követelményeinek megfelelően. Végül a cikk a biztonságosabb katonai kibertér érdekében elkezdi azonosítani egy kezdeti civil önkéntes és katonai együttműködés alapelveit.

During the last five years the parliament and the government launched acts and edicts to establish the legal basis for updated NATO and EU interoperable managements and administrative requirements, technical controls of the appropriate level of information security at public service organisations. The common implementation of the requirements is an extraordinary challenge for the organisations including the Hungarian Defence Forces. The article aids in understanding the problem of security classification of communications and information systems (CIS), the military specification of damages and the organisation security level classification according to the new Information Security Act (2013). Finally, the article starts identifying some basic guides for an initiative civil volunteer and military cooperation for the more secure military cyber space.

Kulcsszavak: *információbiztonság, elektronikus információbiztonság, kiberbiztonság, szabályozás ~ information security, electronic information security (INFOSEC, Information Assurance, CIS Security), cyber security, regulation*

BEVEZETÉS

A közelmúltban hatályba lépő jogszabályok új szabályozási környezetet jelentenek a közigazgatás, a Magyar Honvédség és a honvédelmi szervezetek számára.

A kilencvenes években megjelenő – majd a jelen évszázad elején újra feldolgozott – ajánlások szolgálhatnak némi támogatással, de az akkori és a mostani jogszabályok által határolt lehetőségek jelentősen eltérnek, így a helyzetet szakmai mérlegelés után, a katonai sajátosságok figyelembevételével, új megközelítéssel lehet, és kell megoldani.

Ez az új szabályozási környezet tekinthető hazánkban az első olyan keretrendszernek, ami – korlátozott hatókörrel – követelményeket határoz meg a minősített és a nem minősített adatkezelés összetett világára.

A honvédelmi szervezetek számára legfontosabb aktuális teendők a híradó-informatikai rendszerek biztonsági osztályba sorolása, a szervezeti biztonsági szint meghatározása, a jogszabályoknak megfelelő elektronikus információbiztonsági szabályozás kialakítása (a meglévő szabályozók pontosítása), így a cikk korábban megfogalmazott gondolatok folytatásaként[1] ezeket a kérdéseket világítja meg, segíti az értelmezést, illetve megoldási javaslatokat mutat be.

A BIZTONSÁGI OSZTÁLYBASOROLÁSHOZ SZÜKSÉGES KÁROK, KÁROS HATÁSOK KÉRDÉSEI

A biztonsági osztályba sorolás feladata nem ismeretlen hazánkban, a korábbi ajánlások már foglalkoztak ezzel a kérdéssel. [1] [2] Lényege, hogy a rendszereket (vagy vizsgálati szemponttól függően: az adatokat) csoportosítani kell annak érdekében, hogy a védelmi rendszabályokat ne egyedileg, később nehezen visszakereshető módon határozza meg az arra feljogosított személy. A szervezetnél előforduló adatok, adatkezelési folyamatok figyelembevételével elkészített besorolási rend lehetővé teszi a védelmi rendszabályok áttekinthető keretbe szervezését és központi menedzselését.

A hatályos jogszabály szerint (Ibtv.) a Magyar Honvédségnél az elektronikus adatokat kezelő híradó-informatikai rendszereket a bizalmasság, sértetlenség és rendelkezésre állás szerinti kármérték figyelembe vételével kell biztonsági osztályba sorolni (korábban ilyen jogszabályban rögzített követelmény hazánkban nem létezett). Az értékelést 1-től 5-ig számozott fokozatba sorolással kell végezni, a számozás emelkedésével párhuzamosan növekvő kármérték szerint. [3]

A jelenlegi jogszabályi követelmény a korábbi szabályozatlan környezettől eltér, így nyilvánvaló, hogy felül kell vizsgálni a Magyar Honvédségnél 2009-ben kialakított, a minősített és nem minősített adatokra vonatkozó közös besorolási rendet. [4]

A minősített adatokra vonatkozó kármérték a Mavtv. 1. számú melléklete szerint meghatározott, így az alkalmazó szervezeteknek e területen mérlegelési lehetőségük nincs. Az elektronikus adatkezelő rendszerekkel – katonai megfogalmazás szerint a híradó-informatikai rendszerekkel – kapcsolatban az adatkezelést megvalósító rendszerekre vonatkozó követelményeket a minősített adatok biztonsága szempontjából kell megfogalmazni. Ez azt jelenti, hogy a híradó-informatikai rendszerrel kapcsolatosan az a fő mérlegelési szempont, hogy a minősített adat illetéktelen megismerése megtörtént-e vagy nem, illetve megvalósult-e az az eset, hogy a rendszer szolgáltatásainak korlátai miatt az arra feljogosított személy nem férhetett hozzá a munkavégzéshez szükséges minősített adatot. A lényeg, hogy a rendszer adott állapotát (a sértetlenség és rendelkezésre állás szintjét) és a minősített adat bizalmasságát, sértetlenségét és rendelkezésre állását nem szabad összekeverni.

[1] Kassai Károly: A 2013. évi L. törvény végrehajtása érdekében a Magyar Honvédségnél szükséges elektronikus információvédelmi szakfeladatok, Hadmérnök, VIII. Évfolyam 4. szám - 2013. december.

A minősített adatokra vonatkozóan a Mavtv. szerinti kármérték nemzeti szinten általános megfogalmazású, az információbiztonsági célokra nincs felbontva (az alkalmazó szervezetek ezt a felbontást nagyobb probléma nélkül elvégezhetik).

Az Ibtv. által meghatározott ötös felosztás lehetőséget teremt a minősített adatok kezelésére feljogosított rendszerek esetében egy olyan lehetőségre, amikor a rendszer kiegészítője, eleme is besorolható, hozzá védelmi rendszabály rendelhető. Az első fokozatba sorolható a minősített adat kezelésére feljogosított híradó-informatikai rendszer azon eleme, ami minősített adatkezelést nem végez, de az adatkezeléshez nélkülözhetetlen szolgáltatást nyújt.[2] A 2-5 fokozatba a minősített adat minősítési szintjeit lehet azonosítani. A jogszabályban megfogalmazott besorolási kötelezettség ezzel végrehajtható, ugyanakkor figyelembe kell venni azt a tényt, hogy a későbbiekben a biztonsági osztályok alapján kell a védelmi rendszabályokat meghatározni. E területen a későbbiekben említettek szerint a funkcionalitásnak szükség esetén felül kell írnia a bizalmasság szerinti besorolást, különben értelmetlen és feleslegesen költséges védelmi rendszabályok alkalmazásának veszélye fenyeget. [5]

A nem minősített adatok biztonsági osztályba sorolása az előbbi eljárástól eltérő. Fontos kérdés a végrehajtási rendeletben rejlő rugalmasság felismerése, ami lehetőséget teremt az alkalmazó szervezetek számára, hogy „testre szabva" kijelöljék azt a szempontrendszert, mely szerint értékelni fogják azokat a károkat, káros hatásokat, melyek akadályozzák, korlátozzák a szervezeti célok megvalósulását. [5; 1. sz. melléklet, 1. 4. p.]

E lehetőséget figyelembe véve a honvédelmi szervezetek biztonsági osztályba soroláshoz a következő károkat, káros hatásokat célszerű figyelembe venni (egy megoldás):

1. Társadalmi-politikai szempontú-, vagy kötelezettség elmulasztásából fakadó káros hatások, károk:
    a) Az Alaptörvényben vagy jogszabályban meghatározott honvédelmi feladatok akadályozása, szövetségi – nemzetközi kötelezettségvállalás teljesítésére irányuló negatív hatás, szolgáltatások vagy a nemzeti adatvagyon körébe tartozó honvédelmi adatok megsemmisülése, sérülése, hozzáférhetetlensége következik be. A honvédelmi létfontosságú információs rendszer szolgáltatásaiban működési zavarok keletkeznek.
    b) A Magyar Honvédségre vonatkozó, jogszabályban meghatározott együttműködési, támogatási feladat, kötelezettség teljesítésének akadályozása vagy korlátozása következik be. A közérdekű adatszolgáltatással kapcsolatos kötelezettségek korlátozott végrehajtása vagy teljesítés elmaradása várható.
    c) A Magyar Honvédség társadalmi méretekben kimutatható bizalomvesztése, vagy szövetségesi-nemzetközi kötelezettségvállalás teljesítésére vonatkozó bizalomvesztés következik be.
2. A Magyar Honvédségnél katonai szervezeteket, csoportosításokat vagy személyeket érintő károk, káros hatások: jogszabályban meghatározott védelmet igénylő adatok bizalmasságának sérüléséből adódóan károk, káros hatások keletkeznek.
3. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi károk: a Magyar Honvédség híradó-informatikai rendszereivel vagy a kezelt elektronikus adataival kapcsolatos megsemmisülésből, meghibásodásból vagy információs károkozásból adódó közvetlen költségek.
4. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos közvetett anyagi károk:
    a) A Magyar Honvédség híradó-informatikai rendszereivel vagy a kezelt elektronikus adataival kapcsolatos helyreállítási költségek.

[2] Pl. biztonsági mechanizmus vagy nem minősített rejtjelző besorolású anyag.

b) A híradó-informatikai rendszerek meghibásodásaiból adódó, vagy a környezetet veszélyeztető események elhárítását célzó műveletek költségei.
c) A Magyar Honvédség híradó-informatikai rendszer működési hiányosságából, vagy adat bizalmasságának sérüléséből adódó perköltségek, vagy egyéb anyagi kötelezettségek.

A négy szempont mérlegelésekor kulcskérdés annak megértése, hogy a Magyar Honvédség szervezeteinek működése során, az adott szolgáltatás kiesésének, megszűnésének veszélyét a rendelkezésre álló adatkezelési alternatív megoldásokkal együtt kell értékelni. Ez egyrészt *rendszer szintű gondolkodást és szervezést igényel*, másrészt az *adatkezeléshez rendelt alternatív lehetőségek és megoldások kialakítását követeli meg*. A lényeget megvilágító tipikus kérdések:

- Ha meghibásodik az „xy" szolgáltatás, hogy kerül az adott felsővezetői intézkedés a katonai szervezethez? Más alakulaton keresztül, futárral, rádión!
- Mi történik, ha meghibásodik az „xy" számú munkaállomás? A felhasználó átül egy mások munkaállomáshoz, vagy egy másik felhasználó átveszi a kiesett funkciót!

Nem az a követelmény, hogy minden egyes elektronikus adatkezelő szolgáltatás minden eleme minden időpontban rendelkezésre álljon minden felhasználónak, hanem az, hogy *a szervezeti működést biztosító alternatív megoldások közül összességében annyi álljon rendelkezésre, ami a minimális szervezeti működést biztosítani tudja* (ami nem biztos, hogy elektronikus adatkezelő szolgáltatás) és a vezetésért és irányításért felelős vezetők ezeket az alternatív lehetőségeket ismerjék.

A fentiek mutatják a kettős feladatot: a honvédelmi szervezetek *minősített adatkezelés esetén alkalmazzák a törvényben meghatározott kármérték szerinti besorolást*, *nem minősített adatkezelés esetén pedig lehetőséget kapnak önálló besorolási rend kialakítására és alkalmazására*.

A minősített és a nem minősített híradó-informatikai rendszerek besorolásával kapcsolatos további, közös szempontok:

- *Az értékelést az adatkezelés funkciója szerint súlyozottan kell végezni.* A honvédelmi szervezetek elektronikus adatkezelésével kapcsolatos felelősség nem vonható el az adott rendszerért felelős vezetőtől. Megfontolt döntés szükséges arra vonatkozóan, hogy egy rendszer esetében melyik funkciót kell elsődlegesnek tekinteni a honvédelmi szervezetek vezetési és irányítási képességének működőképessége érdekében. A kérdés szokatlan lehet a minősített adatok kezeléséhez szokott gondolkodás esetén, amikor a fő feladat általában az adat bizalmasságának megőrzése. A bizalmasság szempontja mellett a sértetlenség és rendelkezésre állás más megközelítést jelent. Egy radar adat továbbítására szolgáló KORLÁTOZOTT TERJESZTÉSŰ minősített adatok kezelésére feljogosított rendszer rendelkezésre állási követelménye magasabb lehet egy olyan TITKOS minősített adatok kezelésére feljogosított rendszerénél (vagy önálló telepítésű számítógépénél), amelynek adatfeldolgozási funkciója féléves vagy éves periódusú. Nem lehet kijelenteni tehát, hogy „ami magasabb minősítésű az fontosabb" mert vannak olyan esetek, amikor ez az állítás nem állja meg a helyét. Ezért *kritikus fontosságú a honvédelmi szervezetek működésének pontos ismerete, a hadműveleti követelmények pontos azonosítása*.
- *Kiegészítő biztonsági célok követelményeit a biztonsági osztályba soroláskor figyelembe kell venni.* Amennyiben kiegészítő biztonsági célok azonosítása is megtörtént egy híradó-informatikai rendszer esetében, nyilvánvaló, hogy az ezzel kapcsolatos vizsgálati szempontokat rendszer-specifikusan kell kialakítani.

- *A biztonsági osztályba sorolást a híradó-informatikai rendszerért felelős vezető által jóváhagyott kockázatelemzés alapján kell végrehajtani.* Szakmai kihívás a rendszer szolgáltatásaival kapcsolatos lehetséges állapotok, esetek feltérképezése az akár kritikussá is forduló esetek elkerülése érdekében. Az áramellátás önmagában „nem a rendszer része", a szoftver licensz szerződések folytonossága szintén más szakterületen történő döntések és feladatok eredménye, így nyilvánvaló kihívás azon tényezők és hatások azonosítása, melyek hatással lehetnek az információbiztonsági célok teljesülésére.
- *A biztonsági osztályba soroláskor a biztonsági célok sérülését a fenyegetések és a sebezhetőségek bekövetkezési valószínűség szerint módosított hatásai szerint kell figyelembe venni.*

A bekövetkezési valószínűséggel kapcsolatban a jogszabályok követelményeket nem határoznak meg, így a Magyar Honvédség esetében ezt is központilag célszerű szabályozni, melyre egy megoldás a következő lehet:

A bekövetkezési valószínűséget 1-től 5-ig számozott fokozatba sorolással kell értékelni, a számozás emelkedésével párhuzamosan növekvő bekövetkezési valószínűség szerint:

- elhanyagolható bekövetkezési valószínűség (1);
- alacsony bekövetkezési valószínűség (2);
- közepes bekövetkezési valószínűség (3);
- nagy bekövetkezési valószínűség (4);
- kiemelkedően nagy bekövetkezési valószínűség (5).

A híradó-informatikai rendszerek biztonsági osztályba sorolásakor a bekövetkezési valószínűséggel súlyozott fenyegetésekből eredő kár, káros hatás szerint a következő módon lehet biztonsági osztályokat kialakítani (egy változat):

1. biztonsági osztály, jelentéktelen kár:
   a) Magyar Honvédség szinten társadalompolitikai károk, hatások nem azonosíthatók.
   b) A katonai szervezeteket, csoportosításokat vagy személyeket káros hatások érték, de Magyar Honvédség szintjén értékelhető kár nem keletkezett, jogszabályban meghatározott adat védelme nem-, vagy csak olyan mértékben sérült, ami katonai szervezet szintű megoldást igényel.
   c) A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi és közvetett anyagi kár elhanyagolható. A katonai szervezet híradó-informatikai szolgáltatásainak vagy a központi szolgáltatások üzembenntartási keretei között a kár kezelhető.
2. biztonsági osztály, csekély kár:
   a) A keletkezett társadalompolitikai károk katonai szervezet vagy középszintű vezető szerv szintjén kezelhetők.
   b) Jogszabály által védett adat bizalmassága sérült vagy adat, szolgáltatás sértetlenség és rendelkezésre állás követelményei nem teljesültek, melynek során katonai szervezeteket, csoportosításokat vagy személyeket csekély károk, káros hatások érték.
   c) A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi és közvetett anyagi károk az üzembenntartás központi keretei között kezelhetők. A helyreállítás vagy ideiglenes szolgáltatás biztosítása többlet műveleteket igényel.

3. biztonsági osztály, közepes kár:
    a) A keletkezett társadalompolitikai károk hatásaként katonai szervezetek, vagy középszintű vezető szerv működésével, műveleti képességeivel kapcsolatos bizalomvesztés keletkezik.
    b) A Magyar Honvédségre vonatkozó, jogszabályban meghatározott kötelezettség késve, vagy nem teljes mértékben teljesül.
    c) Jogszabály által védett adat bizalmassága sérül vagy adat, szolgáltatás sértetlensége és rendelkezésre állás követelményei több esetben – más közigazgatási szervezetek munkáját nehezítve – nem teljesülnek, melynek során katonai szervezeteket, csoportosításokat vagy személyeket kimutatható károk, káros hatások érnek.
    d) Honvédelmi létfontosságú információs rendszer működésében Magyar Honvédség szinten érzékelhető kiesés, vagy szolgáltatás csökkenés következik be. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi és közvetett anyagi károk az üzembenntartásra biztosított központi keretek között már nem kezelhetők. A helyreállítás, vagy ideiglenes szolgáltatás biztosítása Magyar Honvédség szinten többlet erőforrásokat igényel, ami más híradó-informatikai szolgáltatás rovására, más költségvetési keretek terhére történik.
4. biztonsági osztály, nagy kár:
    a) A keletkezett társadalompolitikai károk hatásaként a Magyar Honvédségre vonatkozóan az Alaptörvényben, jogszabályokban meghatározott feladatok – benne a szövetségesi kötelezettségek – elláthatósága, teljesíthetősége kapcsán bizalomvesztés keletkezik. A Magyar Honvédségre vonatkozó jogszabályokban meghatározott kötelezettségek teljesítése nem kiszámítható, megbízhatatlanná válik, más közigazgatási szervezet működésére is káros hatások alakulnak ki.
    b) Jogszabályban védelemre kötelezett adatok bizalmassága Magyar Honvédség szinten nagymértékben, tömeges adatokat érintve sérül, jelentős bizalomvesztést, nagyszámú peres eljárást okozhat, nehezen kezelhető személyi károk keletkezhetnek.
    c) Honvédelmi létfontosságú információs rendszer működésében Magyar Honvédség szinten megbízhatatlan működés következik be, a meghibásodások egymás hatását erősítik, a helyreállítások hatékonysága bizonytalan. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi károk a híradó-informatikai szakterület üzemeltetésére és fejlesztésére tervezett központi keretekből nem biztosíthatók, a központi tartalék alkalmazására és tárca szintű belső átcsoportosításra van szükség. A közvetett anyagi károk a környezetvédelemre, jogi képviseletre és egyéb, kárenyhítésre tervezett tárca szintű központi keretekből nem biztosíthatók, belső átcsoportosítást igényelnek.
5. biztonsági osztály, kiemelkedően nagy kár:
    a) A keletkezett társadalompolitikai károk hatásaként a Magyar Honvédségre vonatkozóan az Alaptörvényben, jogszabályokban meghatározott feladatok – benne a szövetségesi kötelezettségek – elláthatósága, teljesíthetősége kapcsán súlyos, nemzeti és nemzetközi szinten érzékelhető bizalomvesztés keletkezik. Jogszabályban meghatározott feladatok végrehajtása elmaradhat, a Magyar Honvédség alaprendeltetéséhez köthető együttműködési kötelezettségek nem teljesülnek.

b) Magyar Honvédség szinten honvédelmi körbe tartozó nemzeti adatvagyon pótolhatatlanul megsemmisülhet, honvédelmi létfontosságú információs rendszer működése nem biztosított. Jogszabályban védelemre kötelezett adatok bizalmassága Magyar Honvédség központi adatbázisok szintjén sérülhet, melynek mértéke kiemelt, a kár hatásainak kezelése hosszú időszakot vesz igénybe.
c) A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi károk a híradó-informatikai szakterület, tárca szintű tartalék mellett kormányzati szintű keretek terhére biztosíthatók. A közvetett anyagi károk a környezetvédelemre, jogi képviseletre és egyéb kárenyhítésre tervezett tárca szintű központi keretekből és belső átcsoportosításból nem biztosíthatók, kormányzati keretekből történő megerősítés szükséges.

Az értelmezéshez célszerű irányelveket meghatározni a honvédelmi szervezetek közös értékelési rendjének kialakulása, az egységes gondolkodás érdekében, de meg kell jegyezni, hogy a bekövetkezési valószínűség, az információs kár meghatározása, a biztonsági célok közötti súlypont helyes azonosítása segédeszközök, programok alkalmazása esetén sem nélkülözheti a szubjektivitást.

Az egyéni nézőpontokból adódó hibák kiküszöbölésének eszköze a gyakorlás és képzés, a kontrollcsoportok alkalmazása, illetve a Magyar Honvédség sajátosságait tükröző minél pontosabb központi követelmények meghatározása.

A VÉDELMI RENDSZABÁLYOK KIALAKTÁSÁNAK TÁMOGATÁSA, A SZERVEZETI BIZTONSÁGI SZINT BESOROLÁS

A honvédelmi szervezetek híradó-informatikai rendszereinek biztonsági osztályba sorolása kockázatelemzés nélkül tartalmilag elképzelhetetlen, melynek általános feladatait egy korábbi cikk már megfogalmazta.[3] A kockázatelemzésre vonatkozó nemzeti követelmények annyit változtak, hogy az alkalmazó szervezetek számára jogszabály meghatározza a kockázatelemzési stratégia és eljárásrend kialakítását. [5; 3. sz. melléklet, 3. 1. 1. 10. p. és 3. 1. 2. részfejezet]

A részletek említése nélkül megfogalmazható, hogy a híradó-informatikai rendszerek kockázatelemzése több szempontból értelmezhető feladat. A honvédelmi szervezeteknél szükség van *az általános tervezési feladatok támogatására, részleteket is feltáró strukturált elemzésre, illetve egy-egy célterületre vagy adatkezelési funkcióra irányuló kockázatelemzési folyamatokra*.

A biztonsági osztályba sorolás elvégzése érdekében elégséges egy általános, rendszer szintű kockázatelemzés, ami a legjelentősebb fenyegetésekkel, sebezhetőségekkel számolva az egész rendszerre, adatkezelési folyamatra vonatkozóan feltárja az előnyöket és hátrányokat. Ebben az esetben elérendő cél, hogy a fentiekben példaként bemutatott biztonsági osztályba soroláshoz szükséges döntés megalapozott legyen. Ehhez jól láthatóan nem részletes paraméterek azonosítására van szükség, hanem az adott értékelt területnél az esetleges kárra, káros hatásra koncentrálva az előnyök és hátrányok számbavételére és az esetleges kiegészítő védelmi rendszabályok igényének vagy lehetőségének azonosítására.

A biztonsági osztályba sorolás szakterületi támogatása, a feladat egységes szemléletű végrehajtása érdekében *szükség van a hivatkozott követelmények szerinti specializált kockázatelemzési módszertan kialakítására*, az ehhez szükséges feladat elrendelésre és képzésre vonatkozó részfeladatokkal együtt.

[3] Kassai Károly: Az elektronikus adatkezelő rendszerek egyes biztonsági kérdései; Hadmérnök, V. Évfolyam 1. szám - 2010. március, p. 260-262.

A támogatási feladatok között említeni kell a képzést is, melynek biztosítania kell az Ibtv. végrehajtásához szükséges ismeretek elsajátítását. [6]

A képzési feladatokat meghatározó jogszabály követelményei szerint a Nemzeti Közszolgálati Egyetem 2014-ben elindítja, de a végrehajtás során gátló tényező lehet a két szemeszteres képzés személyenként félévre eső százezres nagyságrendű képzési költség, illetve a költségvetési tervezésre vonatkozó átfutási idő. Könnyítés, hogy gyakorlati tapasztalattal kiváltható a képzésre vonatkozó beiskolázási követelmény, illetve a Nemzeti Elektronikus Információbiztonsági Hatóság véleménye szerint a közigazgatásban elfogadható megoldás a szervezetek, önkormányzatok összefogása és az elektronikus információbiztonság közös menedzselése (az önkormányzati társaságok mintája e szakterületen is követhető), és a képzésre közösen delegált személyek biztosítása.

Az összetett szervezeti struktúrák számára elégséges a központi feladatokért felelős szervezeti elemek állományát beiskolázni, ami a Magyar Honvédség esetében a szakmai feladatok irányításáért felelős HM szerv, a középszintű vezető szerv, az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (KCEHH) központi üzemeltetési feladatait ellátó honvédelmi szervezet érintettségét jelzi (a képzési követelményekre vonatkozó döntést célszerű az első évfolyam utáni tapasztalatok feldolgozására alapozni).

A szervezet biztonsági szintjének meghatározásakor az alkalmazott híradó-informatikai rendszerek kockázatelemzésen alapuló biztonsági osztályát, az elektronikus adatkezelés kockázatainak a szervezeti feladatokra történő hatásait kell figyelembe venni.

A szervezet biztonsági szint meghatározása a szervezet vezetőjének hatáskörétől nem vonható el, de a Magyar Honvédség szinten egységes szintek kialakítása érdekében szükség van egy központi szakmai támogató tevékenységre, ami az Ibtv. végrehajtására kiadott jogszabályban meghatározott felügyeleti rend biztosít. [7] Az elöljáró szakmai szint szakértői tevékenysége biztosítja a szervezetnél kialakított döntési javaslat kontrollját, és főleg azokban az esetekben nyújt hasznos segítséget, amikor az általánostól való eltérőséget, a besorolás során alkalmazandó lehetséges eltéréseket, vagy következő szervezeti biztonsági szint eléréshez szükséges szakfeladatokat kell jóváhagyatni.

Irányelvként kell tekinteni, hogy a honvédelmi szervezet híradó-informatikai rendszer adatkezelését biztosító legmagasabb biztonsági osztályt akkor kell a szervezet biztonsági szint besorolás alapjául tekinteni, ha a szervezeti feladatokra történő hatás a legmagasabb biztonsági osztályba sorolt rendszer kockázata szerint a legnagyobb.

A legmagasabb biztonsági osztálytól eltérő szervezet biztonsági szint besorolásról szóló döntésnek tartalmaznia kell a honvédelmi szervezet híradó-informatikai rendszereivel kapcsolatos feladatokra történő kockázatok értékelését, az eltérés indoklását, melynek a felügyeleti rend szerinti elöljáró szervezet jóváhagyása egyben a besorolás objektivitását is biztosítja.

A szervezet biztonsági szintbe történő besorolásakor értékelni kell, hogy a híradó-informatikai rendszer:

- a honvédelmi szervezet üzemeltetésében van, vagy a biztonságért felelős vezetőnek csak a felhasználói szintű biztonsági feladatokra van hatása;
- a honvédelmi szervezet működését milyen mértékben, vagy időszakban biztosítja.

Híradó-informatikai rendszer szolgáltatásait más szervezet számára biztosító honvédelmi szervezet esetében a szervezeti biztonsági szint besoroláskor a kiszolgálói feladatokat és a felhasználói szintű feladatokat elkülönítve kell értékelni.

A híradó-informatikai rendszerek biztonsági osztályának változásakor, vagy a szervezeti elemek olyan átalakításakor, ami hatással van az adatkezelésre, a szervezeti biztonsági szint besorolást soron kívül el kell végezni.

A fentiek szerinti besorolási feladatok célja a védelmi rendszabályok meghatározásának támogatása, a biztonsági osztályonként egységes eljárásrend kialakítása.

Az Ibtv. végrehajtásával kapcsolatos rendelkezések tartalmaznak információvédelmi rendszabályokat, illetve a minősített adatok védelmére vonatkozó jogszabályok is határoznak meg követelményeket, így az alkalmazó szervezetek nyilvánvaló feladata az elkülönült jogszabályok közös, erőforrás takarékos végrehajtása.

A Magyar Honvédség esetében e mellett kiegészítő feladat, hogy a központilag meghatározott, a honvédelmi szervezeteknél készítendő Elektronikus Információbiztonsági Szabályzatra (EIBSZ) vonatkozó követelményt[4] ki kell egészíteni az új jogszabályban meghatározott védelmi rendszabályokkal.

CIVIL ÖNKÉNTES ÉS KATONA EGYÜTTMŰKÖDÉSE A BIZTONSÁGOS KATONAI KIBERTÉRÉRT

Napjainkban a Honvédség híradó-informatikai rendszerei, a vezetési és irányítási képességek nem különülnek el olyan jelentősen a polgári távközlési, informatikai megoldásoktól, mint hosszú évtizedekkel korábban.

A híradó-informatikai rendszerek kapcsolódási pontjai, a hasonló technikai megoldások – és az ezekkel kapcsolatban megjelenő fenyegetések és sebezhetőségek – nyilvánvalóvá teszik a polgári megoldásokból származó tudás alkalmazásának szükségességét.

A 2013-ban megindított Honvédelmi Kötelék Program kidolgozása a volt Magyar Honvédelmi Szövetséghez (MHSZ) hasonlítható kezdeményezés, amely az iskoláskorú fiatalság felé célozza a katonai értékek közvetítését, míg az Önkéntes Tartalékos Rendszer (ÖTR) a felnőtt korú állampolgárok számára ajánl olyan szerződéses viszonyt, ami lehetővé teszi a Honvédség képességeinek kiegészítését, a szervezettszerű társadalmi támogatást akár elektronikus információvédelem, – kibervédelem területén is. A két megoldás közötti célterület egy olyan lehetőség, ahol az arra elhivatott (vagy kíváncsi, tenni akaró) állampolgár önkéntes alapon, nem tartalékos állományban szabad akaratából, ellentételezés nélkül szakfeladatok megoldását ajánlja fel a Magyar Honvédség számára ezen az érzékeny szakterületen.

Azon személyek, akik szükséget éreznek arra, hogy tudásukat, tapasztalataikat vagy egyéb szellemi javaikat a nemzeti szempontból érzékeny terület – a Honvédelem – megerősítésére fordítsák, véleményükkel, szándékukkal nem hagyhatók figyelmen kívül.

A civil önkéntes oldal és katonai együttműködés megfogalmazásának első lépése a közös célok, együttműködési területek azonosítása.

Nyilvánvaló cél a magyar katonai kibertér biztonságának erősítése, az elektronikus információbiztonság szintjének a fenyegetésekkel és sebezhetőségekkel arányos kialakítása, erősítése a „civil erő” támogatásával.

Elektronikus információbiztonság területén az ilyen együttműködés előzmények nélküli, így a megoldás érdekében tett *minden lépés úttörő megoldásnak minősíthető*.

Az elektronikus információbiztonság – kiberbiztonság szakterülete az egész világon bizalmas területű kérdés, így *a valós információ megosztás és együttműködés alapos előkészítés, pontos együttműködési feltételek és alapelvek lefektetése után képzelhető el*.

Az alkalmazott megoldások, a fejlődés és a világban bekövetkező szakterületi események egyértelműsítik azt a feltételezést is, hogy egy folyamatosan átalakuló és alkalmazkodó együttműködési rendet érdemes elképzelni, melynek kötelező elemei *a naprakészség, a folyamatos konzultáció, a változások érzékelése és a rugalmasság*.

A részletek említése nélkül nyilvánvaló az a szakterületi sajátosság, hogy a közigazgatásban és a Magyar Honvédségnél az adatok védelméért felelős szervezeti elemek léteznek. Ennek *a*

[4] 3/2012. (I. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról.

felelősségnek az elvonása, csökkentése vagy megosztása csak az állami felelősségérzet csökkenését, hamis biztonsági kép kialakulását eredményezné, így le kell szögezni azt is, hogy *az önkéntes alapú hozzájárulás csak a kibervédelmi képességek erősítését, fejlesztését szolgálhatja, a honvédelmi szervezetek alaprendeltetésből adódó felelősségét nem vállalhatja át*.

A nemzetközi média, a szakirodalom egyre több hírt szentel a különböző nemzeti kormányzati, katonai és egyéb nem kormányzati megoldásoknak, a feltételezett, vagy sajtóban bejelentett kiberműveleti támadó képességek ismertetésének. E területen nyilvánvaló, hogy az önkéntes civil – katonai együttműködésnél alapvetőnek kell tekinteni *a nemzetközi szerződések, jogszabályok és egyéb normák tiszteletben tartását, és átlátható, elszámoltatható, egyértelműen kibervédelmi körbe tartozó* tevékenységet lehet csak célkitűzésként megfogalmazni.

A kibertérben zajló műveletek váratlansága, intenzitása, hatásmechanizmusa döbbenetes ütemben fejlődik, ami a váratlanul szükséges kibervédelmi műveletek során az önkéntes résztvevők – vagy az önkéntes tartalékosok – alkalmazásának lehetőségét nagymértékben korlátozza (gyakori az a magyarázat, hogy a támadó előre nem jelenti be, mire készül, így nehézkes erre az esetre bevonulást szervezni). Az együttműködési területek kijelölésénél ezt a sajátosságot figyelembe kell venni, és *az együttműködés során a képességfejlesztést, a tudás erősítését, a biztonságtudatosság növelését kell előtérbe helyezni*.

Szakértői tevékenység

Cél a civil önkéntesek tudásának, tapasztalatainak hasznosítása a Magyar Honvédség kiberbiztonsági fejlesztési és szabályozási tevékenységében.

- Kibervédelmi stratégiai dokumentumok, koncepciók és tervek szabályozók, előkészítésében való konzultáció, véleményezés és javaslattétel.
- Hatástanulmányok, modellezés és szakmai segítségnyújtás a szabályozás, képzés és egyéb specifikus területek támogatása érdekében.

Forráskutatás, elméleti támogatás

Cél az nemzetközi és nemzeti szakirodalom figyelemmel kísérése, feldolgozása során felhalmozódott ismeretek alapján javaslatok megfogalmazása, trendek és iránymutató jelenségek azonosítása a katonai kibervédelmi képességek fejlesztése érdekében.

- A kibervédelemmel kapcsolatos szakirodalom valamint nemzetközi és nemzeti források felkutatása, elemzése, javaslatok megfogalmazása. A nemzeti és nemzetközi stratégiai szintű dokumentumok változásainak követése, az aktuális trendek felismerése és következtetések megfogalmazása.
- A nemzetközi szakirodalomban a katonai kiberbiztonsággal kapcsolatos nyílt forrású dokumentumok felkutatása, értelmezése és javaslatok megfogalmazása.

Elemzés – értékelés

Cél a nemzeti kibertérrel kapcsolatos helyzet elemzésén és értékelésén alapuló tudatos tevékenység, a nemzeti katonai kibertér biztonságának támogatása elméleti támogatása.

- Az EU szabályozók változásainak figyelemmel kísérése, az EU szakirányú szervezeteinek állásfoglalásai és az aktuális szakirányú programok megismerése, értelmezése.
- A nemzeti szabályozórendszer folyamatos figyelése, a változásokkal kapcsolatos szakmai teendők megfogalmazása, a szakmailag illetékes hatóságok által megfogalmazott helyzetértékelések, állásfoglalások elemzése és értékelése.
- A magyar kibervédelem aktuális helyzetének elemzése, trendek azonosítása, javaslatok megfogalmazása katonai kibertér biztonságának növelése érdekében.

Oktatás, képzés és biztonságtudatossági programok

Cél a civil önkéntes tapasztalatok és tudás integrálása a Magyar Honvédség elektronikus információvédelmi – kibervédelmi át és továbbképzési rendszerbe, illetve specializált, egyedi programok, gyakorlatok kialakítása, rendezvények szervezése lehetőleg pontosan megfogalmazott témák feldolgozása érdekében.

- Kibervédelmi rendezvények szervezése, a katonai oktatási és képzési rendszer keretén belül oktatókkal, segédanyagokkal, ismeretekkel a humán erőforrás támogatása.
- Közös elméleti, gyakorlati foglakozásokkal kijelölt szakterületi kérdések vizsgálata értékelés és javaslattétel.

A szervezeti együttműködés megvalósítása

A kialakított civil önkéntes – katonai együttműködés során cél a lehetőségek, zajló folyamatok figyelemmel kísérése és a szükséges korrekciók megtétele, a felhalmozódott tudás rendszerezése, hasznosítási lehetőségeinek kutatása, az együttműködés szélesítése, a belső szabályozók kialakítása és fejlesztése.

- Az önkéntesség elvének megfelelő koncepcionális fejlesztés és tudatos építkezés, programok és együttműködési fórumok lehetőségének felkutatása és megvalósítása.
- A jogszabályokban megfogalmazott lehetőségek kiaknázása, illetve az önkéntes civil – katonai együttműködéshez szükséges jogszabályi változtatási javaslatok megfogalmazása.
- Szakmailag érdekes katonai rendezvényeken a civil önkéntes fél részvételének biztosítása (vagy arról információ biztosítása), a Magyar Honvédség szakterületi kérdéseinek bemutatása.

ÖSSZEGZÉS

A feladatokat nem részletesen tartalmazó cikk jól érzékelteti, hogy a korábban kevésbé szabályozott elektronikus információbiztonsági szakterületen megjelenő jogszabályok olyan új követelményeket határoznak meg, amelyek a közigazgatásban, *a Magyar Honvédségnél megkövetelik a helyzet pontos értékelését és a feladatok lehető legpontosabb specializálását*, „testre szabását”.

A kockázatelemzés – biztonsági osztályba sorolás – szervezet biztonsági szintbe sorolás – illetve a védelmi rendszabályokat meghatározó szabályozók kialakítása logikailag sorba illeszthető feladatok, de az ezzel kapcsolatos részletek több helyen *pontosítást követelnek, a végrehajtás területén pedig minden egyes szabályozási lépésnél szükség van a minősített és nem minősített adatok egységes elvek alapján történő összehangolására*.

A jogszabályok ismeretében hiányként tárható fel *a kockázatelemzésre vonatkozó egységes módszertan és kötelező érvényű eljárásrend hiánya*, ugyanakkor jelzésértékű, hogy kormányzati követelmény már tartalmazza a szervezetek ez irányú feladatait.

A híradó-informatikai rendszerek elektronikus információbiztonsági szabályozása a jelenlegi helyzetben sem tekinthető egyszerű esetnek. Jogszabályok jelenleg pontosan végrehajtható és ellenőrizhető formai és tartalmi követelményeket nem határoznak meg a minősített vagy a nem minősített elektronikus adatkezelés biztonságának szabályozására, így *az alkalmazó szervezeteknek ki kell alakítani azt a specializált szabályozási rendszert, ami egyaránt megfelel a jogszabályoknak és a szervezeti érdekeknek*.

Az utolsó témaként szereplő civil önkéntes – katonai együttműködés egyértelműen az új kihívásokhoz szükséges megoldások keresését célozza. A civil tudás legjobb hasznosítása nem nélkülözhető erőforrás, ugyanakkor a bizalmi kérdésként kezelendő szakterületen az együttműködés kialakítása számos kihívást, megoldandó feladatot rejteget.

Befejezésként köszönet a fontosabb kérdések megvilágításában segítő Magyar Honvédség elektronikus információbiztonsági szakterületű képviselőinek, illetve független szakértőknek, akik a cikk előkészítésekor véleményüket kifejezték, válaszokat adtak, illetve további kérdéseket tettek fel, vagy megoldásokra váró feladatokra hívták fel a figyelmet.

Felhasznált irodalom

[1] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, 1996.

[2] Közigazgatási Informatikai Bizottság 25. számú Ajánlása, Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 25/1-2. kötet Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió; 2008. június)

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 7. §.

[4] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról; 15. §.

[5] 77/2013. (XII. 19.) NFM rendelet Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről; 1. sz. melléklet, 1.1. p.

[6] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról, 4. §.

[7] 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Kovács Zoltán
zkovacs@nbsz.gov.hu

„ELECTRONIC WRITTEN TASKING ORDER SYSTEM" ACCOMPLISHED WITHIN THE PROJECT „SECURE ELECTRONIC COMMUNICATION" III.

Abstract

The main objective of the "Electronic Written Tasking Order System" is to convey the written tasking orders sent to SSNS via secure electronic communication lines decreasing the quantity of the paper based data carriers, which results rapid fulfilment of the requests of the tasking organizations, as well as it creates opportunities to carry out several related procedures in electronic form. This article series describe the designation of the Electronic Written Tasking Order System through the activities of SSNS proving that this system is a cloud system in terms of the tasking organizations. With reference to this it analyses the relevant security issues, the success of those issues and the classification for the critical information infrastructure.

A Szolgálati Jegy Rendszer fő célja a szolgálathoz beérkező megrendelések biztonságos elektronikus úton történő továbbítása, ezáltal a papír alapú adathordozók számának jelentős csökkentése és a megrendelői igények mihamarabbi kiszolgálása, valamint bizonyos kapcsolódó ügymenetek elektronikus alapokra helyezésének megteremtése. A cikksorozat a Nemzetbiztonsági Szakszolgálat feladatain keresztül bemutatja az elektronikus Szolgálati Jegy Rendszer rendeltetését, majd bizonyítja, hogy az a megrendelők szempontjából felhő alapú rendszernek tekinthető. Ennek kapcsán áttekinti a releváns biztonsági kérdéseket, azok érvényesülését, valamint a kritikus (létfontosságú) információs infrastruktúrává történő besorolás kérdéskörét.

Keywords: *elektronikus Szolgálati Jegy Rendszer, felhő alapú rendszerek, felhő alapú rendszerek biztonsága, kritikus információs infrastruktúra ~ electronic tasking order system, cloud computing, cloud security, critical information infrastructure*

INTRODUCTION

The following paragraph can be read in a study published in 2010, entitled: "Computer Network Operations: Threats and Possible Defence Solutions in Hungary"

"The "Comprehensive Programme for Integrated Governmental Functions" includes such important issues related to economy and national security that we cannot disregard. By means of the "Central Management System" the whole budget system of Hungary will become transparent, therefore misuse of data gained from this system might influence the whole economy of Hungary. Thus the protection of this system is a high priority. The "Taxpayer-centric data service model" sets up Data Warehouses, here the priority is to maintain tax secrecy. The "Secure Electronic Communication" affects the processes of the Special Service for National Security. Although this is one of the most interesting tasks, its technology is not known to the public. The budget of the whole programme is 13881 million Forints." [1]

If the author of this part of the study, Csaba Krasznay regarded the project named "Secure Electronic Communication" as one of the most interesting issues, it is worth examining what it means. Certainly, only those parts can be published which do not contain classified information, even though the principle of the above mentioned project can be known, with some other important pieces of information which can be necessary for the planning of other systems.

The first article of this series of articles reviews the designation of Electronic Written Tasking Order System (eWTOS) accomplished within the framework of the so-called "Secure Electronic Communication" project, and in accordance with the tasks of the Special Service for National Security (SSNS), the procedure of the orders, and then examines how the eWTOS can be applied in the IT strategy of the Ministry of Interior. The second article analyses a currently important issue proving that the eWTOS can be regarded as cloud computing in terms of the tasking organizations. Concerning this it groups the cloud computing along with their features and classifies the eWTOS in the appropriate category. The third article discusses the security issues of the cloud computing by analysing to what extent it concerns the eWTOS as well as how the security panels prevail during their accomplishment. Finally two conclusions are drawn. On the one hand, even though the eWTOS has not been qualified as a critical information infrastructure yet, as every condition is given it is only a question of time. On the other hand, thanks to the already evolved high level security panels, the system is protected properly, thus after the classification these do not have to be modified in merits.

The series of articles concentrate on – primarily security – solutions considered during the planning. These articles do not aim to analyse the technical or other problems which appeared during the implementation or to describe different mistakes and their handling. They will only be mentioned if it is necessary to explicate the previously mentioned issues.

Review:

The first part of these series describes the tasks of eWTOS. In order to clarify it the functions, the activities and the process of the tasking orders received from the tasking organisations are reviewed. After this, within the framework of a historical overview, it enumerates the events which have determined the current structure and operation. of eWTOS . After clarifying the bases, it describes the structure and principle of operation of eWTOS and presents the similarities and the differences between the paper-based and electronic processes. Finally it discusses how eWTOS, invented in 2005, suits to the IT strategy of the Ministry of Interior published in 2012. On the basis thereof it determines that the system utilizes such forward solutions and performs such functions today which were only drawn up as strategic purposes on the level of the Ministry of Interior in 2012.

The second article of the article series demonstrates that eWTOS is a cloud computing system in terms of the tasking organizations sending written tasking orders to the SSNS. In

order to demonstrate that, first, the article reviews the features and characteristics of cloud computing systems. After that, it declares that eWTOS is a Community cloud (in the Deployment model category), and a Software as a Service (in the Service models category). It establishes that eWTOS is very important because today there are rather few cloud computing systems used by national security services and law enforcement agencies, so it is subservient to analyse carefully the experiences of it.

SECURITY ISSUES OF EWTOS

Risks and Security Issues of Cloud Systems

The greatest challenge of cloud systems, as a recently appeared, rapidly and continuously developing, altering technology is to establish complete security. The traditional IT safety solutions cannot entirely be applied in the cloud, what is more, there are new security risks which require new solutions. [2] These are the problems that had to be faced with during the development of eWTOS, and it was compounded by the fact that increased security requirements have to be fulfilled, since in eWTOS classified information must be transferred and handled.

The studies, blogs on cloud computing published on the INTERNET search for answers or try to give definitions, advice in a plenty of ways, sometimes aspiring to completeness, sometimes riving off a very focussed topic related to the security of cloud computing. Like in the definition and categorization of cloud computing the study published by the Information Technology Laboratory of NIST (National Institute of Standards and Technology) under the title „The NIST Definition of Cloud Computing" [3] is regarded as widely accepted and quasi-standard, as far as security concerned the same could be written about the „SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING" [4] by Cloud Security Alliance. In the document, the security aspects are divided into 13 domains, further classified into 2 main parts: governance and operation. The governance part includes mostly strategic, while the operational part discusses tactical security issues.

The Cloud Security Alliance^{SM} (CSA) first published the study mentioned above in April 2009, whose V3.0 version was published in 2011. In the latter one, the concept of Security as a Service (SecaaS) appeared first. In 2011 Security as a Service Working Group of Cloud Security Alliance^{SM} published a study under the title „Defined Categories of Service 2011"[5], which discusses the above-mentioned topics in detail.

In the aforesaid documents the CSA discusses the security issues of cloud computing focussing on business organizations. In terms of eWTOS these issues should be analysed differently, according to the method which was recommended to law enforcement agencies. [6] In this case, using the above mentioned documents of CSA (yet classifying the security issues differently, sometimes complementing and modifying the content) the analysis should be carried out along the four dimensions below:

1. The role of the law enforcement agencies:
   - user,
   - executor of lawful monitoring.
2. Deployment Models:
   - Private cloud,
   - Community cloud,
   - Public cloud,
   - Hybrid cloud.

3. Service models:
   - Cloud Software as a Service (SaaS),
   - Cloud Platform as a Service (PaaS),
   - Cloud Infrastructure as a Service (IaaS).
4. Security issues to examine:
   - operational reliability, operational safety,
   - data security,
   - other (legal, physical, etc.) security,
   - lawful monitoring.

In terms of eWTOS, the dimensions 1 to 3 were discussed in the previous article, so the security issues should be examined within the following frame:

1. The role: user,
2. Deployment Model: community cloud,
3. Service Model: Software as a Service.

During the analysis of the security issues of the four dimensions (operational reliability, operational safety, data security, other (legal, physical, etc.) security) the correspondence or diversions of the interests of the provider and the user should also be examined. [6] In terms of eWTOS a special situation occurred. On the one hand, the provider is one of the users, on the other hand, in certain security issues (e.g. data security) legal requirements must be satisfied. In the light of the foregoing it is considered that the interests of the user and the provider correspond in all the three issues, moreover the SSNS, which is also a provider, demands higher level security requirements than the users (tasking organizations) would do (e.g. access privileges). So, the correspondence or the diversion of the interests of the provider and user should not be examined anymore.

Operational reliability, operational safety

The issues of operational reliability, operational safety (hereafter operational reliability) concerning cloud computing (and also eWTOS) are remarkably similar to that of the traditional IT systems. Accordingly, the accepted and used security standards of traditional IT systems are perfect basic to analyse these questions. This category concludes the features relating to the reliable functionality and operation in normal circumstances.

Regarding the operational reliability field, two issues are worth discussing: administrative and technical. While the latter is evident for everyone, the former is not, or not as much as that concerning the data security topic. However, this is of great importance to evolve complete operational reliability.

The administrative issues involve practically each factor that is not technical, but supports operational reliability. Regarding eWTOS, complete system plan-, developing-, implementation-, test-, and operational documentations, as well as regulations, rules of orders for operation, a disaster recovery plan are done. Users and repairmen are trained in different levels, and custom service is evolved. During the operation of eWTOS, updating the above mentioned documents, repetitive trainings, and non-stop running of custom service are very important tasks.

Concerning the tasks belonging to technical issues of operational reliability – including but are not limited to – the following things have been evolved by the developers of SSNS. Criteria of reliable basic components are satisfied with high quality hardware and software elements During the selection the following criteria were defined: long term manufacturer support, quality assured manufacturing and quality control processes, which increase the possibility of long term, fail-safe operation of the system Besides the fact that these are also the basic requirements in case of unique software, at eWTOS the control of the source code is another

possibility. The eWTOS includes redundant elements, which means geographical redundancy in most cases, in other cases at least the possibility of evolving the geographical redundancy. In order to ensure high availability, redundancy is evolved by two physically same-way build up configurations which logically seems only one, so in case of malfunction of any equipment, the other configuration can take over all the tasks without loss of data packets. The RAID storage and fully comprehensive backup and data recovery system ensures the high level of data access. For interoperability eWTOS has well defined interfaces and uses standard data formats. It has a fully regulated version of control subsystems, which is connected to a pilot system, where new versions of software and hardware equipment can be tested before they are used in a hot system. The eWTOS includes a log and event analysis subsystem which can analyse all kinds of activities and states even automatically, and this can help not only the information management and data security, but also the operational reliability as well.

Regarding the operational reliability issues, the separation of responsibilities seems to be obvious; basically it is the SSNS that takes all responsibilities.

Information Management and Data Security

All the factors emerging with reference to the safe access to the user data (management, application, of unauthorized access can be regarded as a question of information management and data security (hereafter data security), for instance the identity and access management, the use of encryption and the vulnerability of the software used. In the eWTOS the data security issues have been solved in two different ways. On the one hand, well known solutions can be used, which are already available in connection with the traditional IT systems, or can easily be implemented to that system (e.g. antivirus software).On the other hand in order to solve new problems, completely new solutions must be implemented (e.g. data segregation).

Some of the data security issues could easily be solved in a technical way. For example on the online subsystem only the most necessary software was enabled to install because of the security risk of software vulnerabilities. However, on the offline terminals which are used for other tasks by the owner, SSNS could give only recommendations. But in this case, increased security requirements have to be fulfilled too, because of handling classified information on them.

The data security issues can be solved completely in technical, legal and administrative ways, however, some of the elements cannot be solved only in a technical way, or can be solved with unrealistically large expenditure. Some of them are ensured by law, others can be ensured by internal regime rules.

Due to the limitations of space and the information which is allowed to be published, without being exhaustive, the identity and access management of eWTOS should be reviewed:

- the whole system, the facilities of eWTOS, and the encryption devices correspond to legal requirements and authorised by law;
- application of multi-level, high level encryption methods (e.g. IPSec, which is mentioned in the IT strategy of the Ministry of Interior;
- encryption of the whole data communication;
- users management:
  a) create,
  b) inhibit,
  c) delete;
- multilevel authentication with biometric user identification;
- access management and control;
- full logging user activity;
- verifying user activity
- concerning the whole organization,

- concerning only one case;
- application, handling and verification of digital signatures, timestamp, certificates;
- matrix of signature management (determining the person that can sign a particular document)
- the whole lifecycle of a document can be tracked (even in case of an offline workstation;
- the content of the written tasking order cannot be modified after the application of (digital) signature;
- the documents can be:
    a) opened to read or edit,
    b) printed

only by special applications developed by SSNS.

The responsibilities are distributed between the user and the provider (SSNS), who is a user at the same time. The questions of data security should be analysed through the life cycle of the data [6] illustrated by Figure 1.

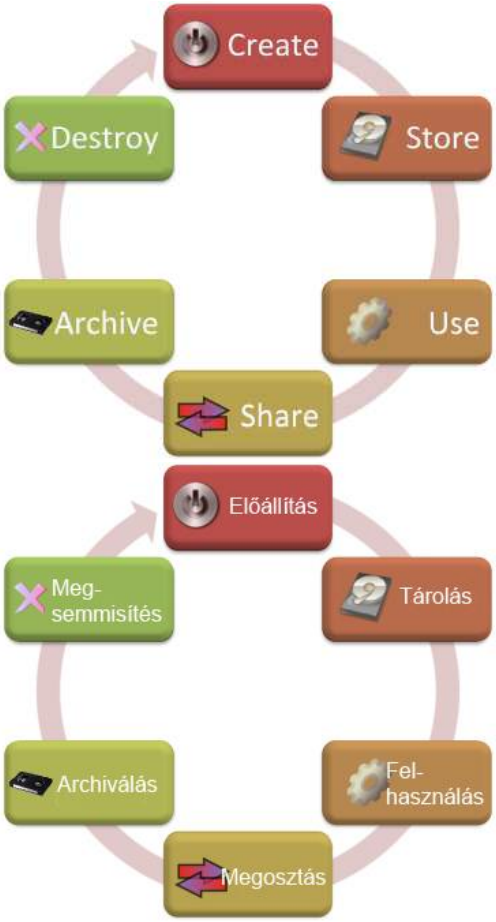


Figure 1. Data Lifecycle [1]

Regarding a traditional cloud system (i.e.: established and run by business organizations) in terms of security the six phases of the data lifecycle can be divided into two main groups concerning security: phases with and without data movement.

Phases with data movement:

- create
- use
- share
- destroy

Phases without data movement:

- store
- archive

This should be done because, in case of cloud computing, any kind of active operation accomplished by the user will be associated with data movement.

With respect to eWTOS, the lifecycle of data should be analysed in another way, since the security elements for data transferring are built into the system by SSNS. Every user (including the SSNS) has to analyse the following questions: in which stage of the processes are they concerned? in which stage are they concerned entirely or partly? , what are the security elements ensured by eWTOS, as well as, what are the ones that are their responsibilities to ensure? (e.g.: the storage of data of a document created in an offline workstation is the responsibility of the maker, but after transmission to the SSNS it is the responsibility of the SSNS. However, the protection of a transferred document is not the responsibility of the user even when it is addressed to the authorization organization and not to the SSNS, because the protection of the documents is guaranteed by eWTOS.)

Other (legal, physical, etc.) security

This category includes all the security issues which can not be managed in a technical way, or even a third party can be involved (e.g. audit). The legal guarantees (primarily contractual, or regulated by the law) which can solve the particular issues in an unambiguous way, including the questions emerging about reliability and data security issues, as well as the physical defence of data centres are classified here.

Regarding eWTOS this security issue is limited. The other (legal, physical, etc.) security issues which are significant when the provider is a business organization, in this case it is not necessary to analyse, because on the one hand the interests of user and the SSNS (who is provider and user at the same time) concur, and on the other hand this field is strongly regulated by law. In the traditional cloud computing case, this security issue includes things like content of contract, long-term viability (meaning accessing data in case the provider go bankrupt or get acquired and swallowed up by a larger company), access logs and other statistics ownership, provider espionage, transitive nature, or insecure or incomplete data deletion. In regards to eWTOS, some of these problems a priori are not interpreted, others are regulated by law in a sufficient way.

The physical security is guaranteed by two reasons. One of them is that the physical security of the datacentre, the online (and offline) terminals have to be established according to Act No. CLV of 2009 on the protection of classified information (PoCI). The other is that the premises, where the equipment of eWTOS is installed owned by national security services and law enforcement agencies, so for others reasons (e.g.: to observe regime about internal security), there are high level manpower and technics of security. This is especially true for the datacentre which is located at SSNS.

A third party can be involved when the contractor or maintainer of eWTOS carry out any kind of work on the system, but this is regulated in extremely precise and detailed contract, between SSNS and the contractor. This contract includes the same guarantee elements as any other contract signed by SSNS, including Nondisclosure agreement and security checks. On the other hand, audit is only made by National Security Authority, only according to classified

information protection, edge along regulations of law, and can access only data which belong to its circle of competence, so unauthorized data access cannot occur regarding to audit.

The responsibilities are definite in this issue, the legal guarantee is provided by law and the SSNS, physical security are provided by the owner of the premises where demarcations are unequivocal.

In conclusion it can be ascertained that eWTOS fulfils all security criteria (confidentiality, availability, integrity, authenticity and non-repudiation) [7], therefore all data created, stored, transferred, etc., in this system are protected properly.

EWTOS, as a critical information infrastructure, and the effects of classification on the security solutions

As a final step, it is appropriate to examine whether eWTOS can be classified as a critical information infrastructure, if yes, how it affects the security solutions.

According to the highly accurate definition of Dr. Ferenc Kovács: *„The critical infrastructures are the critical elements of the national, federal and EU infrastructure, whose significant damage, failure or loss would have a serious impact on the security, economy of the nation or nations, on the environment, the public health, and the efficient operation of governments or the state."* [8]

Act No. CLXVI of 2012 on the identification, designation and protection of critical systems and facilities [9] uses the phrases *essential* instead of *critical infrastructure*. It can be found on the part of the interpretative provisions of the Act:

„f) essential constituent: such constituent of a device, premises, or system of a sector defined in supplement 1–3, which is crucial to supply essential social services, particularly to ensure health, security of a person and property, economic and social public services, and due to the lack of continuous supply of these processes, the failure of them would have significant consequences,

g) national essential constituent: essential constituent designated by this law, which because of the lack of continuous supply of essential social processes, the failure of them would have significant consequences for Hungary,"

It is said by the designation of national essential constituent part of his Act:

„2. § (1) Designation or withdrawal of designation on national essential constituent can be initiated by:

a) the operator or

b) any organizations defined by Government Decree (hereinafter: proposing authority)

from belonging to sectors defined in supplement 1–3, to designated organization defined by Government Decree (hereinafter: sectoral designation authority) with presentation of identification report prepared after the identification process."

The infrastructures of law enforcement agencies are listed into Public Safety – Protection sector in supplement 3 line 41.

As it is said in „Green Paper on a European Programme for Critical Infrastructure Protection: *„ICT[1] systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)."* [10]

In view of the above, everything is given for eWTOS to be a critical (essential) information infrastructure. The initiation of designation, so the classification, has not been accomplished yet, and thus eWTOS is not a critical information infrastructure. The system was established to replace certain paper based processes, so there would not be any alternatives working parallel. After the initial period when electronic and paper based written orders with the same content

[1] ICT: Information and Communications Technologies

are handled parallel in the system; most of the written orders will be handled only in electronic form, so the failure or damage of eWTOS could set back the national security and law enforcement work, so *"influences serious consequences to the security ... of nation ... to efficient operation of ... or state."* [8] The improvement of eWTOS is planning with installation of more online workstations and subsystems which will be able to handle TOP SECRET! classified documents, so the dependency upon eWTOS will increase. Based on these, it can be declared that the classification of eWTOS as a critical information infrastructure is only a matter of time.

It is clear that eWTOS is suitable for excessively high level requirements in all the three security issues (operational reliability, data security, and other (legal, physical, etc.)). The security elements of eWTOS do not have to be changed even after the system is classified as a critical information infrastructure, because they have been evolved to meet these requirements. However, the security elements must be reviewed and upgraded time to time, because new vulnerabilities might be discovered, new attack methods might be evolved, and these could be a threat for eWTOS as well.

CONCLUSIONS

The second article verified that eWTOS can be regarded as cloud computing in terms of the tasking organizations. The security issues of any info-communication systems, including the cloud computing systems, used by the national security services and law enforcement agencies have high priority for them. This article has analysed the security issues of eWTOS by the syllabus connected with cloud computing system recommended by the author. [6]
In conclusion the planned and installed security elements covers the issues of cloud security published in the professional literature. Moreover, eWTOS, as a system handling classified data must meet significantly higher level requirements. From this perspective eWTOS can serve as a model for planning other systems.

On the other hand, we must add that we are only talking about the issues considered in the planning stage; the practical experience is rather limited yet. It is practical to review and analyse the security issues periodically whether they have lived up to the expectations in every aspect. (On the basis of test run and the four month operation it is stated, that problems occurred basically in the operational reliability field. These problems were not caused by lack of planning, but lack of realization of some hardware and software components.)

Today, it is very rare, that a cloud computing system is used by a national security service or a law enforcement agency. It is expected that the need of using cloud systems will grow by organizations mentioned above. At present there is no "security analysis template" available by a national security service or a law enforcement agency, which could help them to prepare the detailed requirements, including significantly detailed security requirements. In order to avoid that every organization must work out an overall, comprehensive requirement independently, it is subservient to create a template like this.

This work can be helped by analyses and developing of industry standards and best practices of developed countries and international organizations and moreover the analysis of eWTOS, as a „cloud model project". Moreover, it is more fitting to use the security requirements of a cloud computing system as a basic of template mentioned above, which was created especially for Hungarian national security services and law enforcement agencies, fit to the Hungarian law, and the security requirements of it are upgraded by growing experience, and then complete that with recommendations of international organizations which were evolved by primarily taking account only business organizations, not the other way around.

References

[1] Kovács László (szerk.): SZÁMÍTÓGÉP-HÁLÓZATI HADVISELÉS: VESZÉLYEK ÉS A VÉDELEM LEHETSÉGES MEGOLDÁSAI MAGYARORSZÁGON. Tanulmány. Budapest, 2010 ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM p. 56.

[2] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage: Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf – *(2011.11.05.)*

[3] Peter Mell and Tim Grance: The NIST Definition of Cloud Computing Version 15, 10-7-09 http://www.nist.gov/itl/cloud/index.cfm – (2011.10.21.)

[4] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0 http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf – (2012.01.05.)

[5] Defined Categories of Service 2011 https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf – (2012.01.05)

[6] Kovács Zoltán: Cloud security in terms of the law enforcement agencies – Hadmérnök VII. Évfolyam 1. szám - 2012. március

[7] Útmutató az IT biztonsági szintek meghatározásához. www.ekk.gov.hu/hu/emo/ekozigkeretrendszer/ek3-itbiztonsag/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.pdf – (2013.04.04.)

[8] Kovács Ferenc: Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok kidolgozása. Tanulmány. GKM, 2005. p. 7.

[9] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyar Közlöny 154. szám 2012. november 22. p. 26099 - 26107 http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk12154.pdf - (2013.04.04.)

[10] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final. http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf - (2013.04.04.)

Figures

[1]Figure 1. Data Lifecycle https://securosis.com/blog/data-security-lifecycle-2.0, (2012.01.05.)

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Krasznay Csaba – Török Szilárd
krasznay.csaba@uni-nke.hu – torok.szilard@gmail.com

HUNGARY'S CYBER DEFENSE READINESS FROM THE PERSPECTIVE OF INTERNATIONAL RECOMMENDATIONS

Abstract

A country's cyber defense structure is usually very complex and needs interagency cooperation. All countries have a different governance structure, but usually the ministries responsible for internal and external defense have an important role. This is confirmed by recommendations from various international organizations that show best practices for the creation of national cyber defense strategies. The goal of this study is to overview the structure of Hungarian cyber defense and its compliance with international recommendations.

Egy ország kibervédelmi szerkezete általában meglehetősen összetett, ezért elengedhetetlen az egyes elemek közötti együttműködés. Az országok eltérő kormányzati szerkezettel bírnak, azonban általános a minisztériumok felelősége a belső- és külső védelemi feladatok ellátásában. Számos nemzetközi szervezet, mint "legjobban bevált gyakorlat"-ként ajánlja a nemzeti kibervédelmi stratégia létrehozását. Ezen publikáció fő célja, hogy bemutasa a Magyarország kiber védelmi struktúráját, illetve összevesse azt a nemzetközi ajánlásokkal.

Keywords: *cyber defense, international recommendations, strategies ~ kibervédelem, nemzetközi ajánlások, stratégiák*

INTRODUCTION

As information technology growing quickly and broadly, the vulnerabilities of technology are exploited to a higher extent. With the in-depth knowledge and usage of IT it is more optimal and cost efficient to manage the inevitable data and information acquisition processes in various fields of intelligence, crimes and military warfare.

IT crimes (or cyber-crimes) need to be distinguished according to information technology users and their motivation: these can be amongst others mainly hackers (white or black hat – they mostly driven by financial interests), industrial spies, external and internal experts, and IT criminals.

To lay down a country's cyber defense tasks need the cooperation of various military, national defense and civil organizations. There are various different international recommendations that help in developing of a national cyber defense strategy and legislation system, and creating of roles and responsibilities. Although the defense structure is different country by country, some organizations have a special role in this hierarchy.

In Hungary, the Act L. of 2013 on the electronic information security of state and municipal organization and Hungary's National Cybersecurity Strategy deal with the cyber defense structure. The whole legislation system is constantly evolving, but its current state is suitable to take a snapshot and analyze its compatibility with international recommendations.

Based on the above it is necessary and relevant to design and develop a cyber defense center in Hungary, namely a Cyber Security Centre. The government built up a centralized IT operation and development company in the past few years called NISZ Zrt. (National Info Communication Service Provider and its subsidiaries) which has a central role. The operation of the National Telecommunication Core Network's (NTG) network security is being operated by the NISZ as of summer of 2013 – in close cooperation with the newly established Government Incident Response Team (Gov-CERT – Hungary).

This study uses the following guidance sets as a base point: ITU's National Cybersecurity Strategy Guide, ENISA's National Cyber Security Strategies and NATO's Cooperative Cyber Defence Centre of Excellence (CCD CoE) National Cyber Security Framework Manual and derives their requirements to the Hungarian situation.

INTERNATIONAL RECOMMENDATIONS

International Telecommunication Union (ITU)

ITU published its recommendations in 2011 under the title of National Cybersecurity Strategy Guide. This guidance was one of the first in this topic and its aim is to help settling down a national cyber security system. This publication recommends 10 steps as important strategic goals.

1. Top Government Cybersecurity Accountability: Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.
2. National Cybersecurity Coordinator: An office or individual oversees cybersecurity activities across the country.
3. National Cybersecurity Focal Point: A multi-agency body serves as a focal point for all activities dealing with the protection of a nation's cyberspace against all types of cyber threats.
4. Legal Measures: Typically, a country reviews and, if necessary, drafts new criminal law, procedures, and policy to deter, respond to and prosecute cybercrime.

5. National Cybersecurity Framework: Countries typically adopt a Framework that defines minimum or mandatory security requirements on issues such as risk management and compliance.
6. Computer Incident Response Team (CIRT): A strategy-led program contains incident management capabilities with national responsibility. The role analyses cyber threat trends, coordinates response and disseminates information to all relevant stakeholders.
7. Cybersecurity Awareness and Education: A national program should exist to raise awareness about cyber threats.
8. Public-Private Sector Cybersecurity partnership: Governments should form meaningful partnership with the private sector.
9. Cybersecurity Skills and Training Program: A program should help train cybersecurity professionals.
10. International Cooperation: Global cooperation is vital due to the transnational nature of cyber threats.

This recommendation designates those responsible governmental and civil players who have some role in the execution of strategic tasks. The key players are the followings:

- The Government, in Hungary the Prime Minister's Office
- The Parliament
- Owners and operators of critical infrastructures
- Courts
- Law enforcement authorities
- Intelligence organizations
- Manufacturers of IT security products
- Academies
- International partners
- Citizens

In Hungary strategic decisions are made by the Prime Minister's Office. The Ministry of Public Administration and Justice is responsible for the legislation and supervises the National Security Authority and is also one of the sustainers of National University of Public Service (NUPS). The Ministry of Interior supervises the critical infrastructures (through the National Directorate General for Disaster Management), the law enforcement authorities (Police, Counterterrorism Center), some intelligence organizations (Constitution Protection Office, Special Service for National Security with the Gov-CERT inside) and partially the National University of Public Service. The Ministry of National Development is responsible for the development of National Cybersecurity Framework. All of the aforementioned organizations are involved in international cooperation. ITU's enumeration does not deal with the military perspective.

European Network and Information Security Agency (ENISA)

ENISA is the European Union's cybersecurity agency which published its National Cyber Security Strategies – Practical Guide on Development and Execution book in December 2012. It proposes 20 steps for the development of a national cybersecurity strategy.

1. Set the vision, scope, objectives and priorities.
2. Follow a national risk assessment approach.
3. Take stock of existing policies, regulations and capabilities.
4. Develop a clear governance structure.
5. Identify and engage stakeholders.
6. Establish trusted information-sharing mechanisms.
7. Develop cyber-security contingency plans.
8. Organize cyber-security exercises.

9. Establish baseline security requirements.
10. Establish incident-reporting mechanisms.
11. Make citizens aware.
12. Foster R&D.
13. Strengthen training and educational programs.
14. Establish an incident response capability.
15. Address cybercrime.
16. Engage in international cooperation.
17. Establish a public–private partnership.
18. Balance security with privacy.
19. Evaluate.
20. Adjust the national cyber security strategy.

This guidance does not specify any organizations, but key players can be easily identified from the examples and use cases. It strengthen the roles of those organizations that can be derived from ITU's guidance.

Hungarian legal background

In 2013 the Hungarian government defined the National Cyber Security Strategy of Hungary (Government decree [2] of 1139/2013. III.21.) and based on this decree the act about „Electronic information security of state and local government institutions" [3] (hereinafter abbreviated as: IBTV) was ratified.

There are many previous regulations on the security of domestic systems, government institutions and networks related to public administration. The government's intention was to manage this field by creating detailed measures such as:

- Act C. of 2003 about Electronic Telecommunication.
- The related IHM decree of 27/2004. (X. 6.) (about the establishment, operation, competence of the duty system of the postal branch and the IT and electronic telecommunication branch, furthermore about the notification and liaising obligations of the designated service providers, the actions related to the network security of these service providers.
- Government decree of 100/2004. (IV. 27.) about the emergency management and classified period operation system in electronic telecommunication, about the tasks of public administration organizations, and the provisions of proper conditions for their operation.
- The NMHH decree of 4/2012. (I. 24.) about data protection and confidentiality obligations related to public electronic telecommunication service, special terms of data management and confidentiality, the security and integrity of networks and services, the management of traffic and invoice figures, furthermore the regulations related to ID display and call forwarding.

As part of the Digital Renewal Action Plan (2010-2014) it became necessary to create a legal background that is better suited to the development of domestic systems and the circumstances of electronic public administration.

Accordingly in spring 2012 the government decree of 83/2012. (IV. 21.) was adopted about the regulated electronic administration services and about the services to be mandatorily provided by the government, the government decree of 84/2012. (IV. 21.) about the designation of institutions related to electronic administration, furthermore the government decree of 85/2012. (IV. 21.) about the detailed rules and regulations of electronic administration. It is important to mention that these government decrees determine the minimum requirements towards service providers concerning the secure operation of the services.

The definition background of regulated electronic administration services is determined by the Act of 2004. CXL, Article 172 (hereinafter referred to as: 'Ket.' about the general rules of public administration procedures and services. The primary goal of the act is to establish those new legal institutions which provide procedure and data management guarantees to citizens and businesses, and makes it possible for them the usage of electronic communication, and eliminate over-regulations.

It has to be emphasized that data forwarding processed through the NTG network has to comply with the requirements of personal data protection which is elaborated in the act of 2003 C. Article 155, furthermore - with proper technological and logistics measures – it is necessary to hinder the interception, storage or surveillance of forwarded communication or data traffic related to the communication, moreover to hinder unauthorized or accidental access to data traffic related to communication.

The Cyber Security Centre in Hungary

Based on the above goals, expectations and regulations, a need for the establishment of a Cyber Security Centre (CSC) has arisen within the governmental IT operation structure. Due to the operational and organizational capabilities of a central IT operation, the NISZ is considered to be the most competent entity for the implementation.

The Cyber Security Centre needs to be scalable, adjustable to the defense requirements of organizations and their information systems, furthermore it needs to continuously provide information to the NISZ and its governmental clients. A centrally monitored and managed cyber security contributes to the reduction in cyber security risks and threats and it could even turn into a proactive defense system.

As an important part of the planning procedure it is necessary to list those types of solutions which can tackle the current cyber security challenges.

1. Monitoring center and incident management
2. (log analysis)
3. Network security analysis and malware laboratory
4. Defense capability against data leakage

The Cyber Security Centre receives input data from the National Telecommunication Core Network (NTG) namely the log files of devices that provide the IT security functions for NTG, moreover receives the network security information collected by GovCERT from external sources.

Based on the processing of input data the present relations and correlations, vulnerabilities and risks are defined, and based on this, real time or preventive warnings need to be forwarded to the operators and governmental users.

The Cyber Security Centre needs to meet some general requirements such as:

- Needs to provide an efficient solution for the analysis of the network's data traffic
- Needs to be available continuously in order to centrally process and evaluate the received log files in a reliable manner.
- Needs to detect and manage intruder suspect events and targeted attacks efficiently
- Needs to implement efficient and competent incident management supported by more comprehensive reports.

The detailed content of the listed items

1. Monitoring Centre, Incident Management: The expenditure on defense and other security measures will be efficient in case the CSC is able to interpret the signals of increased security incidents and events and to efficiently interfere, furthermore to maintain an intense technical and professional cooperation with competent authorities regarding specific cases.

Increasing reporting and detecting capability

a) The detection and more efficient reporting on increased security events (due to developments) are of key significance. Accordingly, NISZ being responsible for IT operation is expected to employ IT security professionals with relevant qualifications and experience, furthermore it is expected to produce sufficient early and trend reports for all professional and management levels.
b) In order to reach this, log processing needs to be developed according to the expectations of modern cyber defense.

2. IT security log analysis
    a) In order to collect and redundantly store log files, the extension of log collector systems is needed.
    b) Also the extension the analysis of log files is necessary (quantity, quality, etc.), including a more efficient processing and evaluation – e.g.: the log files of different services and applications need to be adjusted to the same level.
    c) It is necessary to track the samples from – even subsequently solved - incidents to processing systems. This requires the introduction of a framework system that makes it possible to be easily conducted by a monitoring employee without developer expertise.
    d) It is necessary to integrate the heterogenic log analysis in the IT operation systems and the log registration infrastructures into one frame system (with the introduction of proper methodology and professional solution).

3. Network traffic analysis
    a) The online analysis of the traffic is crucial to improve security therefore the most suitable product needs to be integrated into the system.
    b) The network analytical device should be able to monitor, interpret the total network traffic, and trace back immediately any communication between two endpoints. The visualization layer enables online processing, and a potential intruder attempt can be detected.
    c) The solution needs to be able to save the total monitored traffic, and complement the saved traffic with further information necessary for interpretation.
    d) The potential damages can be determined from the saved data and can be used later as evidence.
    e) The generated reports, warnings and trends need to be connected to the incident management, log analysis and report generating subsystems.
    f)
4. Data Loss Prevention solutions: Based on the current user, end point and mobile device structure and user habits within IKK two types of solutions need to be developed against data leakage Endpoint and network Data Loss Prevention (DLP and Net-DLP)
    a) These solutions ensure the tracking and control of inward and outward data traffic at endpoints, and ensure the collection of evidence.
    b) Mobile Device Management (MDM)
    c) Smart phones and tablets are quite popular in the government all these devices carry potential data leakage risks due to their storage capacity and mobile data medium functions (USB key, SD card, etc.).
    d) Their usage is manually untraceable, it is necessary to define client level and within that user profiles, and manage the related software packages and rules.

5. Ensuring data protection and legal compliance
    a) The NISZ as the central telecommunication and IT service provider of the government, is in a position facilitate adherence to electronic information security and data protection rules on an operational level at the institutions where its services are provided.
    b) Therefore the preparation of a central network and information security service level agreement (Security SLA) is necessary. This document lays down those fundamental technical measures that guarantee cyber security on an operational level.
    c) The technical measures listed in the Security SLA need to be applied to governmental clients individually and according to the specifications of governmental institutions served by NISZ. Based on this, the specific technical measures of the individual service agreement need to be correlated to the related electronic information protection and data protection rules.

ACHIEVABLE CYBER SECURITY RESULTS

This study examines the proper cyber security practice through international and domestic expectations and legal backgrounds overviewed in the study, and through the well-known public cyber security threats.

The goal of the aforementioned described Cyber Security Centre is to create a system to support governmental endpoint and network security protection, which enables to reveal threatening events and risks, control and management of necessary measures, furthermore ensures the continuity of confidentiality, integrity and availability. The target groups of the Centre are the National Telecommunication Core Network (NTG) and joining institutions.

The Cyber Security Centre needs to be scalable, adjustable to the defense requirements of organizations and their information systems, furthermore it needs to continuously provide information to the organizations, and meanwhile it needs to be a centrally controllable and manageable endpoint and network security system.

References

[1] Act L of 2013 about the electronic information security of state and municipal organizations

[2] Government decree about Hungary's National Cyber Security Strategy

[3] Wamala, F.: *The ITU National Cybersecurity Strategy Guide.* International Telecommunication Union, 2011.

[4] *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace*. European Network and Information Security Agency (ENISA), 2012.

[5] Klimburg, A. (ed): *National Cyber Security Framework Manual*. NATO CCD COE Publication, Tallinn 2012

[6] Act XLIII. of 2010 about central public administration organizations, and members of the government and secretaries

[7] 233/2013. (VI. 30.) government decree about the competence and authority of the incident management center of facilities and essential facilities, branch incident management centers, and governmental incident management centers of electronic information systems.

[8] 36/2013. (VII. 17.) Ministry of Justice decree about the branch rules regarding the monitoring and control of closed end electronic information system security.

[9] Act CLXVI of 2012 about the identification, appointment and protection of essential systems and facilities.

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Kurilla Boldizsár
boldigold@gmail.com

A LÉZEREK ALAPJAI, LÉZERFIZIKAI ESZKÖZÖK ÉS ALKALMAZÁSAIK ROBOTTECHNIKAI ESZKÖZÖKÖN

Absztrakt

Jelen cikk egy cikksorozat első része, amely a lézerfizikai eszközök különféle robotjárművek fedélzetén való alkalmazási lehetőségeinek kutatásáról szól. A ma használatos lézeres távolságmérők és más fedélzeti lézerberendezések többsége a pilóta nélküli légi-, személyzet nélküli földi- és vízi járműveken meglehetősen nagy tömegűek, így a legtöbb esetben nagyméretű hordozókra van szükség. A legújabb lézertechnológiák alkalmazásával egy sor műszaki feladat lényegesen nagyobb hatékonysággal és korszerűbben megoldható, mint ahogy ma használják, ugyanakkor új megoldások is születhetnek például a navigációs, kommunikációs és akár a felderítési feladatokra. A fent említettek mellett további fontos feladat a lézeres berendezések vizsgálata a fizikai méreteik és az energiafogyasztás csökkentése céljából. E cikk betekintést ad a lézerek fizikájának alapjaiba és bemutatja a szerző ezen irányú, korábban folytatott kísérleteit, kutatásait.

The present writing is the first part of a series of articles, what is about the research of the application opportunities of laserphysical tools on different robotic vehicles. Most of the currently used laser based distance measurement tools and other laser instruments on unmanned airborne-, terrestrial- and aquatic vehicles are too large and as a consequence larger carriers are required. With the application of the newest laser technologies a large amount of technical tasks can be solved much more efficiently and on a more modern way, as it has been used till present days. However new solutions could be born for navigation, communication and even exploration tasks.Next to the details what mentioned above, further testing is an important task for a robot equipped with other laser devices to reduce the physical size and power consumption. This article is intend to give an insight into the basics of laser physics and introduces the author's earlier research and experiments related to this direction.

Kulcsszavak: *lézer, emisszió, abszorpció, korreláció, nemcsomósodó fotonnyaláb ~ laser, emission, absorption, correlation, antibunching photon*

BEVEZETÉS

A lézer a „Light Amplification by Stimulated Emission of Radiation” (vagyis „fénykibocsátás indukált emisszióval”) kifejezésnek a rövidítéséből származik [1], mely nagyon pontosan írja le az elvet. Az első lézert az amerikai Theodore H. Maiman fejlesztette ki 1960-ban, mely egy rubin lézer volt. Itt a rubinkristály valójában króm atomokkal szennyezett Al_2O_3 (alumínium oxid) kristály. Ennek a lézernek a hullámhossza 694,3 nm volt, mely mélyvörös színt mutat. A lézerek 1960-as megjelenésük óta igen nagy fejlődésen mentek keresztül. Fontos, hogy a lézerek működési elvének alapjait megértsük, ezért néhány alapvető fogalmat részletesebben ismertetni fogok. A lézerek működését három főbb jelenség teszi lehetővé: a spontán emisszió, az indukált emisszió és az abszorpció. Ezen jelenségeket vázolom az első fejezetben, majd a lézerek fajtáiba adok betekintést, hogy könnyebben megértsük a kitűzött irányokat.

Két különböző úton közelítettem meg a problémát. Az egyik probléma, hogy a fegyverek területén, és a kommunikációban alkalmazott jelenlegi lézerberendezések többsége nagy tömegű, ezért csak nagyméretű pilóta nélküli robotjárműveken lehet alkalmazni őket. Ebből kifolyólag a lézerek méreteinek és energiafelhasználásának csökkentése a biztos működés megőrzése mellett igen fontos feladat. A másik probléma a kommunikáció megvalósítása. A mai robotjárművek közötti kommunikáció elsősorban rádiós úton történik, melynek óriási hátránya, hogy illetéktelen személyek feltörhetik, illetve lehallgathatják őket. A lézeres kommunikációval ez gyakorlatilag teljesen megakadályozható. A lézeres kommunikáció alapjainak megértéséhez fontos tényező a hullámhossz reflexiótól való függése. A cikkben az ehhez kapcsolódó számításomat a Sellmeier együtthatók segítségével oldottam meg táblázatos formában.

A LÉZEREK MŰKÖDÉSÉHEZ SZÜKSÉGES FOGALMAK ÉS A LÉZEREK FAJTÁI

A spontán emisszió

Spontán emisszió alatt értjük valamilyen halmazállapotú (folyékony, gáznemű vagy szilárd) anyag gerjesztett állapotba való átvitelét energia befektetéssel. Az anyagokat gerjesztett állapotba hozhatjuk fénnyel, melegítéssel, elektromossággal vagy elektromágneses hullámokkal. Ez egyatomos gázoknál jól leírható úgy, hogy az atommag körül egy jól meghatározott távolságban keringő elektronok az energia befektetés hatására távolabb kerülnek az atommagtól, mint alapállapotban. Fontos megjegyezni, hogy itt nem stabil állapotról beszélünk, hiszen az atom, ami a legkisebb energiájú állapot, igyekszik visszakerülni az alapállapotba az energiaminimum elvének megfelelően. Ugyanakkor spontán bekövetkezhet az alapállapotba visszatérés a gerjesztést előidéző hatás folyamata alatt is. Az adott anyag atomjainak vagy molekuláinak gerjesztett állapotának stabilitása az adott anyagra jellemző tulajdonság függvénye. Amikor egy atom visszatér az alapállapotba, akkor a gerjesztett állapotú atomból egy foton távozik. Amekkora volt az energiakülönbség a gerjesztett és az alapállapotú atom között, akkora az energiája a kilépő fotonnak. Így a kilépő foton energiája megegyezik a gerjesztett pályára került elektron és alapállapotú pályán lévő elektron potenciális energiakülönbségével. Ezt a következő egyenlettel tudjuk kifejezni:

$$E_2-E_1= h*f,$$

ahol E_2 a gerjesztett atom energiája, E_1 az alapállapotban lévő atom energiája, h a Planck állandó ($6{,}626*10^{-34}$ J*s) és f a távozó foton frekvenciája [2]. Az egyes anyagok gerjesztés hatására a rájuk jellemző hullámhosszokon emittálnak fotonokat.

Indukált emisszió

Indukált emisszióról akkor beszélünk, ha egy h*υ energiájú foton elmegy a gerjesztett állapotban lévő atom mellett és azt leviszi a gerjesztett állapotból. Eközben pontosan olyan tulajdonságú fotont bocsát ki az alapállapotba visszaugró atom, mint amilyen tulajdonsággal az őt leverő foton rendelkezett. Ebből az következik, hogy a keletkezett foton a terjedési irányában, polarizációjában, fázisában és hullámhosszában megegyezik az őt keltő fotonnal.

Abszorpció

Abszorpcióról akkor beszélünk, amikor az atom gerjesztett állapotba kerülhet, ha ütközik a fotonnal és eközben a foton elnyelődik. Ekkor a foton az elektronok potenciális energiájává konvertálódik.

Ezen jelenségek lehetővé teszik a lézerek működését. Ha van egy adott térfogatnyi gázunk, melyet gerjesztünk, akkor ebben kialakulhat a spontán emisszió. Az így keletkezett fotonok elnyelődnek vagy indukált emissziót idéznek elő. Fényerősítés viszont csak akkor valósulhat meg, ha a gázban a gerjesztett atomok aránya jóval nagyobb, mint az alapállapotban lévőké. Amikor több gerjesztett atom van az adott térfogatnyi gázban, mint ahány alapállapotú atom, akkor a spontán emisszióban létrejött fotonok hatására nagyobb eséllyel valósul meg indukált emisszió, és az indukált emisszióban keletkezett fotonok pedig nagyobb eséllyel idéznek elő újabb indukált emissziót. Ebből kifolyólag ez az állapot elengedhetetlen a lézerek működéséhez. Így leegyszerűsítve kimondhatjuk, hogy ha a közegünkben több gerjesztett állapotban lévő atom van, mint alapállapotban lévő atom, akkor létrejött a populáció inverzió [2]. Azt a közeget, ahol ez megvalósult, erősítő közegnek (aktív közegnek) nevezzük.

Egy lézer megépítéséhez szükséges egy optikai rezonátor. Ez gondoskodik a fotonok aktív közegbe való visszavezetéséről és a teljesítmény kicsatolásáról. Egy optikai rezonátor két teljesen párhuzamos tükörből áll, ahol az egyik közel 100%-os reflexióval bír, míg a másik alacsonyabb reflexiójú. A két tükör között helyezkedik el az aktív közeg, mely különböző hosszúsággal bírhat.

Ha egy monokromatikus fény sugara I_0 intenzitással áthalad az aktív közeg x hosszán, akkor a kapott intenzitás $I(x)= I_0*e^{-\alpha x}$ lesz, ahol α a közeg abszorpciós együtthatója [2]. Minél nagyobb utat tesz meg a foton az aktív közegben, annál jobban erősödik a fénysugár. Fontos megjegyeznünk, hogy az úthossz növelést nem az aktív közeg hosszának megnövelésével érjük el elsősorban, hanem a tükrök alkalmazásával. Itt a kisebb reflexiójú tükör a kimeneti csatoló, hiszen ott lép ki a lézersugár. A pumpáláshoz egy másik lézert vagy villanó fényforrást használunk.

A lézerberendezések osztályozása különösen fontos feladat. Így összegezve legegyszerűbben hét főbb szempont alapján tudjuk őket felvázolni [1]:

Működési mód:

- CW- „continuous wave”, melyet folyamatos lézersugárzásnak hívunk;
- IPM-impulzus lézer, ahol a fényforrás csomagokban bocsájtja ki a koherens fényt.

Hullámhossz: Napjainkban több ezer lézerrendszer ismeretes, melyek hullámhossztartománya 10 nm és 500 μm közé esik. Így tehát hullámhosszuk alapján megkülönböztetve beszélhetünk ultraviola (UV), látható tartományú, infravörös (IR) és röntgen lézerekről.

Monokromatikus (egyszínűség), ahol a $\Delta\nu \approx 1$ MHz – 1 GHz

Irányítottság: Jó rezonátoroknak és megfelelő nyílásátmérőknek köszönhetően a lézerfény rendkívül párhuzamos nyalábban terjed tova. A szögeltérés a következőképpen számítható ki: $\delta\theta=\lambda/d\approx 1$ mrad-1 μrad, ahol λ a lézer hullámhossza, d pedig a sugárátmérő.

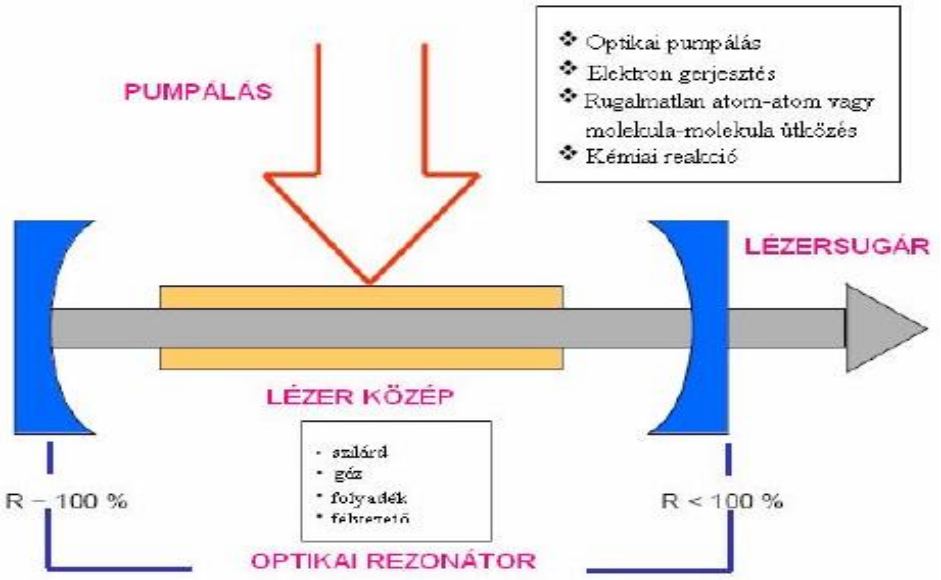
Koherenciafok: (a fázistartó képességére utal). A koherencia idő (amíg a fázis kevesebbet fordul, mint 180°).

Koherencia hossz: $\Delta Z = c*\Delta\tau \approx 300$ m (ekkora távolságon belül hologram képes).

Spektrális fényesség (β), ami nem más, mint egységnyi szteradiánban egységnyi frekvenciaintervallumban kisugárzott fényteljesítmény. Nd:üveg lézernél, $\beta = 108$ W/cm^2 sr Hz.

A Nap esetében $\beta = 10–12$ W/cm^2 sr Hz.

Az 1. ábra a lézer általános működési sémáját mutatja be.



1. ábra. A lézer általános működési sémája [1]

A lézereket fajtáik és alkalmazásaik alapján is csoportosítjuk:

- *Szilárdtest lézerek:* A szilárdtest lézereknél a közös vonás az, hogy az aktív közegük valamilyen kristályos anyag. A Maiman által megépített első lézer szintén ilyen. Ezen lézerek működhetnek impulzussal, de a dióda lézerek (melyek ugyanúgy idetartoznak) folytonosan is működhetnek. Az impulzusüzemmel rendelkező szilárdtest lézerekre jellemző a nagy intenzitás és nagy energiájú impulzus. A szilárdtest lézerek optikai gerjesztéséhez általában egy másik lézer vagy egy erős villanócsövet használnak fel. Alkalmazásaik: anyagmegmunkálás, célmegjelölés, holográfia, katonai alkalmazás területén a LIDAR.
- *Félvezető lézerek:* Gerjesztésük elektromos árammal történik. Alkalmazásaik: Gyógyászat, CD, DVD, Blu-Ray, lézermutatók.
- *Gázlézerek:* Gázlézereknél általában alacsony nyomású gázban hozunk létre populáció inverziót nagyfeszültségű generátor és vákuumforrás segítségével, ahol a gerjesztés általában rádiófrekvenciás vagy elektromos úton valósul meg. Alkalmazásaik: színképelemzés, holográfia, gyógyászat, anyagmegmunkálás.
- *Vegyi lézerek:* Energiájukat kémiai reakcióból nyerik. Általában igen nagy teljesítményű berendezések, melyek magában foglalják a kémiai szállító rendszert, egy szuperszonikus áramoltató rendszert és természetesen egy optikai rezonátort. Ha a kémiai reakció kedvező (nagyobb belső energiát produkálva az állapotok fölött, mint amekkora a külső energia), a populáció inverzió megvalósítható. [3] Alkalmazásaik: anyagkutatás, fegyverkutatás.
- *Folyadéklézerek (festéklézerek):* A festéklézereknek az aktív közege folyékony halmazállapotú, ahol a populáció inverziót elsősorban optikai gerjesztéssel szokták megvalósítani. Ennek egyik módszere (hasonlóan a szilárdtest lézerek gerjesztési elvéhez), hogy a kristály helyett most egy zárt kvarc küvettát helyezünk, amibe

helyezett oldószerben oldott festéket teszünk. Ezeket UV fénnyel gerjesztjük. Egy másik módszer alapján a gerjesztést lézeres pumpálással oldjuk meg. Az lézeres pumpálással működő festéklézerek működhetnek impulzusos vagy folytonos üzemmódban is. A festéklézer abban is különleges, hogy a rezonátorban erősített hullámhosszt ki lehet választani, így a lézer hullámhossza hangolható. Alkalmazásaik: alapkutatások, spektroszkópia

A lézerek a gerjesztés módja alapján lehetnek fénnyel, elektromosan, kémiai úton és rádióhullámokkal is gerjesztettek.

A lézerek különböző feladatokat láthatnak el a hadseregben, mint például felderítés, célmegjelölés, kommunikáció és szolgálhatnak egyenesen irányított energiájú fegyverként. A LIDAR (Light Detection And Ranging) technológia és a repülőgépre szerelt lézeres célmegjelölők napjainkban használatos technológiák. A LIDAR egy optikai érzékelőből és egy lézeres adóból áll, melyek segítségével az adott célpontok távolságát meg lehet határozni 10 μm és 250 nm közötti hullámhossz tartományban. Ez magasabb frekvencián működik, mint a radarok általában. A LIDAR aktív távérzékelési rendszerekhez tartozik, mely alapján a felvevő rendszer saját energiaforrással rendelkezik. A lézerimpulzusok kibocsátása és visszaverődése közötti időintervallum a rendszerben rögzítésre kerül, így a pontos távolság meghatározható az adó és a megjelölt objektum között. A terepi tárgyak térbeli elhelyezkedésének pontos meghatározásához azonban már a szenzor helyének, helyzetének pontos ismeretére van szükség. [4] Jelenleg használatban lévő pilóta nélküli robotjárművekre már akna-és akadály felderítő lézerberendezéseket is alkalmaznak.

A katonai alkalmazásban, haditechnikában a lézerek alkalmazása a kézifegyvereken is megjelenik. Nagyobb hatótávolságú fegyvereknél 650 nm-es hullámhosszú lézert alkalmaznak általában, mert a vörös hullámhossz tartományban halad legkönnyebben át a levegőn a fény. Kisebb hatótávolságú fegyvereken zöld lézert is alkalmaznak, mert a zöld hullámhossz tartományra a legérzékenyebb az emberi szem. (Az emberi szem csúcsérzékenysége 550 nm). A lézeres távolságmérők mind polgári, mind katonai alkalmazásban léteznek igen széles körben. Működési elvük hasonló, hisz az adott objektumra vetített lézernyaláb segítségével megméri az objektum távolságát és ennek eredményét vetíti ki a berendezésnél ugyancsak jelenlévő elektronikus kijelzőre.

Ugyancsak elterjedtek a katonai területen a csapásmérő fegyvereknél alkalmazott lézeres célmegjelölők. Ez lehet a fegyveren, mely a céltárgyon tartja a sugarat a becsapódásig, vagy lehet a rakéták fején, mely önrávezető módon a célról visszavert jelre vezeti rá magát. Alapvető építőelem lehet a saját-ellenség azonosító rendszerekben is, de a nem halálos fegyverek létrehozásában is alkalmazásokra talált.[5]

A NEMCSOMÓSODÓ FOTONNYALÁB ÉS A LÉZERES KOMMUNIKÁCIÓ

A lézerfizikai berendezések a kommunikációban is megoldást hozhatnak. Hatalmas előnyt jelentene a különböző robotok közötti lézeres kommunikáció bonyolult megzavarása és még inkább annál körülményesebb lehallgatása illetéktelenek által. Különösen fontos adatvédelmi probléma a robotok közötti kommunikáció felderíthetőségének csökkentése, a lehallgatásuk megakadályozása és szándékos zavarok elleni védelem megoldása. Természetesen a hátrányokat is fontos kiemelnünk a lézerekkel történő kommunikáció területén. Jelentős adatveszteséget okozhat, ha szabad ég alatt, rossz időjárási viszonyok uralkodnak, mint például eső vagy köd. Szintén hasonló probléma jelenik meg a távolság növekedése esetén fellépő nyalábszélesedés következtében, hisz minden lézernyalábnak van divergenciája. Így ha a nyaláb átmérője túl széles lesz a vevő detektorába való érkezéskor, akkor ugyancsak adatveszteség léphet fel. Számolni kell továbbá a detektorba érkező zajokkal. Előfordulhat

ugyanis, hogy máshonnan is érkezik foton a detektorba. Ekkor háttérzajról beszélünk. Kritikus hiba lehet a lézerekkel való pontatlan célzás. Ennek könnyítésére megoldást hozhat egy olyan optika kialakítása, mely összegyűjti a lézernyaláb nem pontosan odavetített részét és lefókuszálja a detektorba. Mindezekkel együtt, nagyon sok lehetőséget rejt a robotok közötti lézeres kommunikáció, hisz számtalan előnye is van.

A lézeres kommunikáció alkalmazását a világűrben is kipróbálták. 2004 májusában a NASA útnak indították a Messenger űrszondáját a Merkúr felszínének feltérképezésére. Alig több mint egy évvel később (ekkor 25 millió km-re volt már a Földtől) a tudósok leteszteltek az űrszonda fedélzetén lévő Mercury Laser Altimeter (MLA) berendezést, melyet a Merkúr felszínének feltérképezésére használtak. Ennek segítségével lézerimpulzusokat küldtek vissza a NASA tulajdonában lévő Goddard Geophysical and Astronomical Observatory nevű csillagvizsgálóba [6]. Ez volt az első igazán oda-vissza működő űrbeli lézeres kommunikációs kísérlet.

A védett kommunikáció kialakítási lehetőségeinek vizsgálata során, korábbi kutatások eredményeképpen körvonalazódik a nemcsomósodó fotonnyaláb használata a lézeres kommunikáció céljaira. Ez kvantumoptikai úton valósítható meg és kvantumtitkosítási módszerekkel biztosítható az összeköttetések lehallgatás elleni védettsége. Gyakorlatilag lehetetlen a megfejtése, illetve dekódolása illetéktelenek által. Csak azok ismerhetik a robotok közötti kommunikáció eljárásának részleteit, akik ismerik a rendszerben lévő összes optikai elem reflexiós és transzmissziós képességét, illetve az egyes késleltető egységekben a tükrök a polarizációs nyalábosztóktól való pontos távolságát. Fontos kiemelnünk, hogy a hullámhossztól függ a reflexió. Az ehhez kapcsolódó számításom ezt pontosan kimutatja. Azonban itt a változás olyan kicsi, hogy csak akkor vesszük figyelembe, ha nagyon precízek akarunk lenni. A kiértékeléshez, és a függvény elkészítéséhez az Origin nevű programcsomagot, a számításokhoz pedig BK7-es üveget használtam fel. Az Origin programcsomagban különböző fizikai vagy matematikai értékek bevitelével függvények, illetve folyamatok ábrázolására nyílik lehetőség 2-és 3 dimenzióban is. A programcsomagot a Microcal fejlesztette és tette közzé 1992-ben.

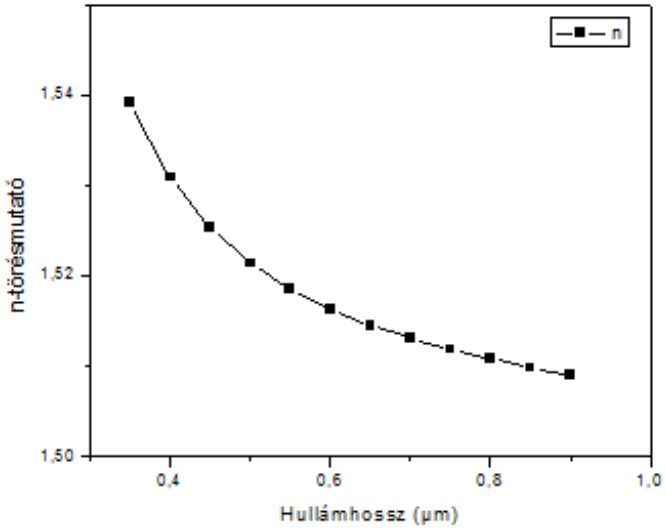
n(Y)	hullámhossz(X)	B1(Y)	B2(Y)	B3(Y)	C1(Y)	C2(Y)	C3(Y)
1,53917	0,35	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,53085	0,4	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,52532	0,45	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,52141	0,5	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,51852	0,55	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,51629	0,6	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,51452	0,65	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,51306	0,7	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,51184	0,75	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,51078	0,8	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,50984	0,85	1,03961	0,23179	1,01047	0,006	0,02002	103,5607
1,509	0,9	1,03961	0,23179	1,01047	0,006	0,02002	103,5607

1. táblázat. A törésmutató meghatározása a hullámhossz függvényében Sellmeier együtthatók segítségével

A táblázatban az n(Y) a törésmutató BK7-es üvegnél, a hullámhossz értékei pedig μm-ben vannak. A B1, B2, B3 és a C1, C2, C3 a Sellmeier együtthatók, melyeket fel kellett használni a méréshez. [7] A Sellmeier együtthatók a Sellmeier egyenletből származó együtthatók, melyek leírják a törésmutató és a hullámhossz közötti empirikus kapcsolatot egy adott átlátszó közegre vonatkozólag. Itt a következő egyenletet használtam:

$$n^2(\lambda) = 1 + \frac{B_1\lambda^2}{\lambda^2 - C_1} + \frac{B_2\lambda^2}{\lambda^2 - C_2} + \frac{B_3\lambda^2}{\lambda^2 - C_3},$$

Ezt az egyenletet felhasználva a 2. ábrán látható függvényt kapjuk, mely a törésmutató hullámhossztól való függését ábrázolja.



2. ábra. A törésmutató változása a hullámhossz függvényében BK7-es üvegnél

A nemcsomósodó fotonnyaláb bevezetéséhez fontos megemlítenem a foton korrelációs mérést, melynek alapjait Robert Hanbury Brown és Richard Q. Twiss brit fizikusok fektették le úttörő kísérletüknek köszönhetően. A kvantumoptika tán a legjobban alkalmazott eszköze lett a foton korrelációs mérés. Egy olyan elrendezés megvalósítását tervezték meg 1956-ban, melynek segítségével meg lehet mérni a Szíriusz csillag átmérőjét. A kísérleti elrendezés alapján egymástól 6 méterre elhelyeztek két, a Szíriusz felé irányított detektort. A kísérlet várt eredménye az lett volna, hogy a két detektorba érkező fotonok teljesen különböző időpillanatokban csapódnak be. Valójában azonban a becsapódó fotonok között interferenciát sikerült észlelni, mely egy pozitív korrelációban valósulnak meg [8].

„Belátható, hogy a sugárzás fluktuációja szoros kapcsolatban van az intenzitás <I(t+ t)I(t)> autokorrelációs függvényével, amely végül is a fotonszám korrelációját írja le, ugyanis a kvantumelmélet szerint az intenzitás arányos a fotonsűrűséggel. A < > csúcsos zárójel klasszikus vagy kvantummechanikai átlagképzést jelöl. Ez a mennyiség annak a valószínűségét méri, hogy a t időpontban detektáltunk egy fotont, és a t + τ időpontban is detektálunk egy következő fotont. A beérkező jeleket a két detektorról arra használjuk, hogy elindítsanak és megállítsanak egy idő-amplitúdó konvertert, ami kimutatja az időkésést a két jel között. Ennek eredményeképpen megszámlálhatóak azok a fotonok, amelyek beérkezésük közti késés pontosan τ. Az ilyen típusú korrelációs és koincidenciakísérletek történetében úttörő jelentőségű volt Ádám András, Jánossy Lajos és Varga Péter 1955-ben publikált koincidenciakísérlete, amelyben először használtak fotoelektron-sokszorozót, s ezzel jelentősen megnövelték a detektálás érzékenységét." [9]

A NEMCSOMÓSODÓ FOTONNYALÁB ELMÉLETE ÉS KÍSÉRLETI MEGVALÓSÍTÁSÁNAK ALAPJAI

A nemcsomósodó foton magába foglalja, hogy egy olyan nyalábot akarunk előállítani, amelyben igen szigorúan meghatározott időpillanatban érkeznek a fotonok. A nemcsomósodás jelenségének megértéséhez fontos definiálnunk a csomósodás jelenségét, illetve azt, hogy mi a Poisson eloszlás. Itt diszkrét valószínűségi eloszlásról beszélünk, mely a binomiális eloszlás

határeloszlása. Kifejezi az adott idő alatt egymástól függetlenül megtörténő (teljesen véletlenszerű) események bekövetkezésének számát. A csomósodás jelenségét pedig leginkább a szuper-Poisson típusú fényforrással tudjuk párosítani, mely akkor valósul meg, hogyha annak a valószínűsége, hogy még egy fotont detektálunk abban az időintervallumban, ahol az első fotont detektáltuk nagyobb annál a valószínűségnél, hogy az első fotont egy másik időintervallumban (ebben több impulzus is lehet) detektáljuk. A nemcsomósodás jelenségét leginkább a szub-Poisson eloszlással lehet definiálni. Ez a jelenség akkor valósul meg, ha az a valószínűség, hogy még egy fotont detektálunk ugyanabban az időintervallumban, ahol az első jött, kisebb, mint az a valószínűség, hogy az első fotont más időintervallumban detektáljuk. [10] Ahhoz, hogy ez megvalósuljon, a kibocsátott fotonok mindegyikét optikailag késleltetnünk kell. Ez az egyik lehetséges változata a kísérlet megvalósításának. Mindezek hátterében természetesen egy koherens fényforrásra (lézer) van szükség. Koherens fénynél tudni kell, hogy a fotonok véletlenszerűen emittálódnak, ezért lehetőségre van a késleltetésre külön-külön. A fényforrás tehát fotonpárokat bocsát ki. Ez azt jelenti, hogy most már biztosan tudhatjuk, hogy érkeznek fotonok, csak azt nem tudjuk, hogy pontosan mely időpillanatokban.

A nemcsomósodás jelenségére több definíció is napvilágot látott. Jelen cikkben három kerül ismertetésre. A leginkább ismert definíciók a másod rendű intenzitás korrelációs függvényre épülnek.

I. Definíció: Foton nemcsomósodás akkor lép fel, ha az intenzitás-korrelációs függvény $G^2(t,t+\tau)$ kezdeti értéke $\tau=0$-ról:

$$G^2(t,t+\tau)>G^2(t,t), \tag{1.1}$$

ahol

$$G^2(t,t+\tau)=\langle \hat{a}^\dagger(t)\hat{a}^\dagger(t+\tau)\hat{a}(t)\rangle \tag{1.2}$$

Az első egyenletet fel lehet írni másképpen is:

$$g^2(t,t+\tau)>g^2(t,t), \tag{1.3}$$

ahol

$$g^2(t,t+\tau)=G^2(t,t+\tau)/[G(t)]^2 \tag{1.4}$$

A $g2(t,t+\tau)$ függvényében található elsőrendű korrelációs függvény nem más,mint a fotonszám várható értéke:

$$G(t)=\langle n(t)\rangle=\langle \hat{a}^\dagger(t)\hat{a}(t)\rangle. \tag{1.5}$$

Megfigyelhetjük, hogy a normalizáció független τ-tól. A G^2-re és g^2-re vonatkozó egyenlőtlenségek ugyanazt a hatást írják le abban az esetben, ha $G(t)\neq 0$ [9]

II. Definíció: Foton nemcsomósodás akkor is felléphet, ha a normalizált intenzitáskorrelációs függvény

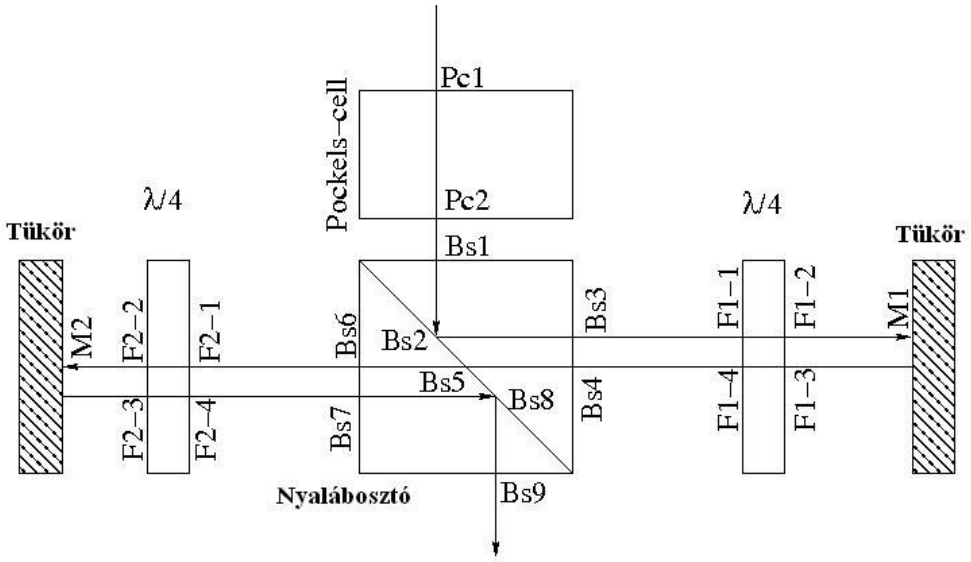
$$g^2(t,t+\tau)=G^2(t,t+\tau)/G(t)G(t+\tau). \tag{1.6}$$

III. Definíció: A szub-Poisson fotonstatisztikát (ezt is nemcsomósodásnak hívják) kétféleképpen is definiálhatjuk. Vagy azt mondjuk, hogy $Q(t)<0$ vagy pedig azt, hogy $g^2(t,t)<1$. [11],[12]

Elmondhatjuk, hogy az egyes és kettes definícióval nem egyezik a hármas definíció, mert itt az egy-időre korrelált függvény különbözik a két-időre korrelált függvényektől, amelyeket az egyes és kettes definícióban használtunk [13]. Azonban az egyes és kettes definíció megegyezik. A különbség köztük csak abban rejlik, hogy míg az egyes esetben a normalizált

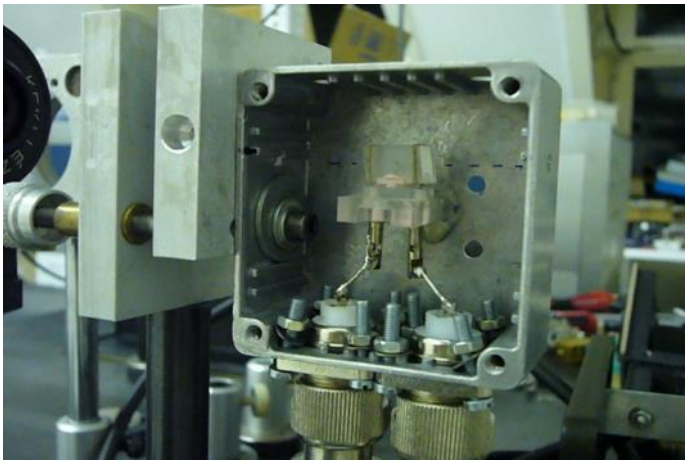
korrelációs függvényről beszélünk, addig a második esetben a normalizált korrelációs függvényt használjuk. [12]

Az eredeti elképzelés alapján a kísérletben a fotonpárok véletlenszerűen érkeznek Optikai Parametrikus Oszcillátor segítségével (OPO). Itt viszont a méretcsökkentés előtérbe helyezése miatt egy új eljárás keresése a kitűzött cél. Nagyon fontos figyelembe venni, ha a fotonokkal bármilyen kölcsönhatásba lépünk, akkor tulajdonságai megváltoznak. Ez azért fontos, mert ha útjuk során detektáljuk őket, akkor elektronokká alakulnak, és mint foton megszűnnek létezni. A detektáláshoz célszerű fotoelektron sokszorozót (vákuum fotocella) és fotodiódát használni. Maga a kísérleti elrendezés így egy optikai késleltető rendszert is magában foglal. Ez Pockels-cellák és polarizációs nyalábosztók, tükrök és λ/4-es hullámlemezek segítségével megvalósítható. A Pockels-cella (ami egy kristálymodulátor) nagyban meghatározza a rendszer állapotát. Ha a feszültséget rákapcsoljuk a rendszerre, akkor lehetővé válik, hogy a továbbhaladó fény, aminek már megváltozott a polarizációja eltérüljön az útjába helyezett polarizációs nyalábosztón. Ha az a célunk a kommunikációt illetően, hogy a fény késleltetés nélkül haladjon tovább, akkor nem kapcsolunk feszültséget a Pockels-cellára. A polarizációs sík elforgatásához nagyfeszültségű (5000 V) impulzusgenerátorra van szükség. A 3. ábrán az optikai késleltető rendszernek egy optikai késleltető egységét láthatjuk. Minél több ilyen egységet építünk ki egymás után, annál nagyobb késleltetés hajtható végre.

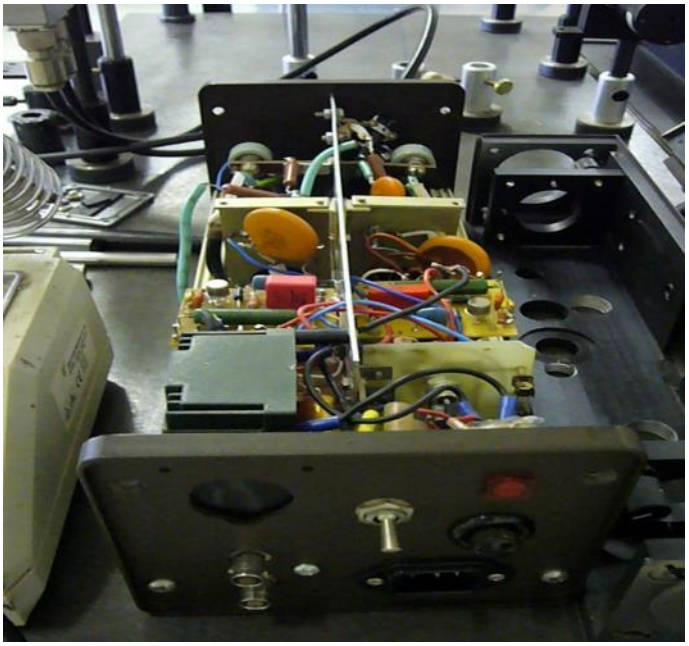


3. ábra. Egy optikai késleltető modul vázlata [9]

Ennek fejében a polarizációs sík nem változik meg, tehát a fény nem térül el. Azonban ha a fény eltérül, akkor lehetőség van arra, hogy a fény útjába a nyalábosztótól megfelelő távolságra λ/4-es lemezeket és tükröket helyezzünk. Ezen áthaladva a hullám cirkulárisan poláros lesz. Így az optikai késleltetés megvalósul. Egy ilyen adott késleltetés után a foton visszatérve a nyalábosztóba újra eltérül és folytatja az eredeti útját a következő eltérítő egységeken keresztül. Ezen módszerrel a fotonon újabb késleltetést hajtunk végre. Ahhoz, hogy mindez sikeresen megvalósuljon fontos, hogy a legelső Pockels-cella legyen a leggyorsabb, ugyanis ez határozza meg, hogy beléphet-e egy újabb foton a rendszerbe, avagy sem. Az 4. ábra a Pockels cellát, a 5. ábra pedig a nagyfeszültségű impulzusgenerátor kísérleti elrendezését mutatja.



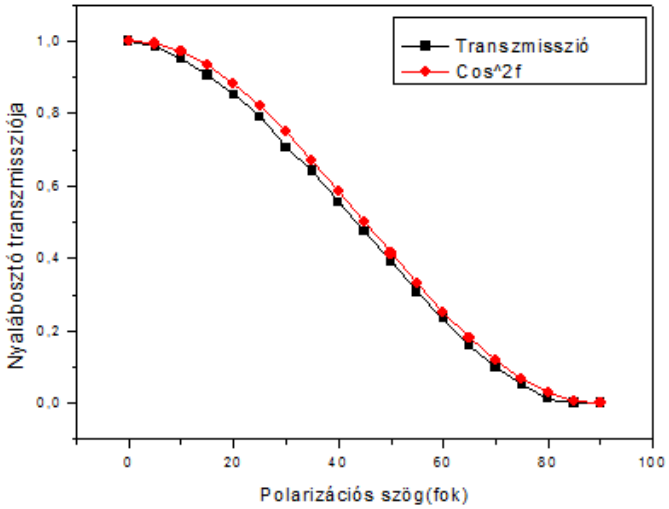
4. ábra. A Pockels cella [10]



5. ábra. A Pockels-cella vezérlő egységének (nagyfeszültségű impulzusgenerátor) kísérleti elrendezése [10]

A most következő mérés egy adott polarizációs nyalábosztó transzmissziójának változását határozza meg a polarizációs szög függvényében. Ezekre leginkább azért volt szükség, hogy minél pontosabb képet kapjunk az esetleges hibaforrásokról a kísérleti elrendezés megvalósítása során. A 6. ábrán a felhasznált nyalábosztó transzmissziójának változását láthatjuk a polarizációs szög függvényében.

A mérések végrehajtásához egy megközelítőleg 100 mW teljesítményű, 780 nm hullámhosszú lézermodul került felhasználásra fel. Szükség volt továbbá egy polarizációs nyalábosztóra és egy teljesítménymérőre.



6. ábra. Nyalábosztó transzmissziója a polarizációs szög függvényében [10]

Elméletileg jósolt eredmény: a kapott függvénynek a $\cos^2 f$-nek kéne megfelelnie. Az ’f ’az olvasott szögek 180°-hoz viszonyított különbségeinek eredménye radiánban. Így tudjuk ellenőrizni, hogy pontosan úgy viselkedik-e, mint egy klasszikus (kalcit alapú) polarizátor. Ha eltér, akkor van érdemi tartalma. Ha ráillik, akkor pontosan úgy viselkedik. Fontos megemlíteni, hogy itt nem kalcit alapú prizmának, hanem egy vékony-réteg szerkezetű polarizációs nyalábosztónak az alkalmazására került sor. Ennek technikájától függ, hogy mennyire tökéletesen polarizál nem pont 45°-os beesésnél. A harmadik képen a méréshez használt lézermodul, a teljesítménymérő és a nyalábosztó látható.

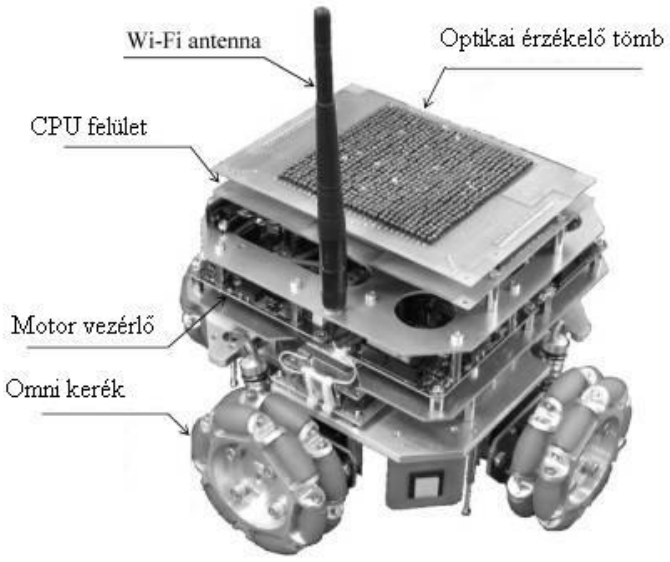
7. ábra. A méréshez használt teljesítménymérő, polarizációs nyalábosztó és a 780 nm-es lézermodul kísérleti elrendezése [10]

A szárazföldi robottechnikai eszközöknél további lehetőségek rejlenek a fedélzeti lézerek használatában, ha például a különböző akadályok felderítésében gondolkodunk. Ilyenek lehetnek a magas aljnövényzetek, sziklák, kövek vagy akár a kisebb-nagyobb domborzatok.

Az automatikusan vezérelt szárazföldi robotoknál különösen fontos feladat, hogy minél gyorsabban érzékelje a maga körül lévő akadályokat. Erre már 3D-s lézer szkenner berendezéseket alkalmaznak. A lézerrel való navigálás és tájékozódás már a 90-es évek elejére is visszanyúlik, ahol forgótükrökkel reflektálták a lézerfényt. Ezáltal 360°-ba lehetett a készülékkel tájékozódni [14]. Sanjiv Singh és Jay West kutatók a Carneige Mellon egyetemen, Pennsylvaniában egy lézer szkennert szereltek fel az általuk készített robotra és ennek

köszönhetően a készülék az útjába eső akadályokat képes volt felderíteni, illetve meg tudták határozni annak helyzetét az adott térképen. Az optikai távolságmérő 3-50 m távolságig tudott mérni +/- 15 cm-es pontossággal. A lézer maga 900 nm-es hullámhosszon üzemelt 7200 Hz-es ismétlési rátával.

Megvalósítható navigációs eljárás a szárazföldi robotoknál a roboton kívül helyezett lézeres navigációs rendszer is. [15] A 8. ábrán egy ilyen robotot láthatunk. Ez esetben bizonyított a megvalósíthatósága annak, hogy a robot kövesse a szkennelő lézerpontot a robotra szerelt optikai érzékelő tömb segítségével.



8. ábra. Optikai érzékelő tömbbel felszerelt robot [15]

A rendszer kétdimenziós mozgást vezérel a lézerforrás segítségével.

A 3D-s lézeres felderítésnek már sokkal több előnye van és egyben sokkal nagyobb figyelem is irányul ma rá. Újabb kutatások azt mutatják, hogy ilyen lézerrendszer sokkal gyorsabban vissza tudja juttatni az információt a különböző akadályokról, illetve részletes 3D-s feltérképezést tud nyújtani a környezetről. [16] Az 9. ábra két részből áll. A felső része egy rendes fénykép egy adott teremről, az alsó pedig annak egy 3D-s lézeresen feltérképezett változata.

9. ábra. Egy terem és annak 3D-s lézer szkennerrel letérképezett változata [16]

ÖSSZEGZETT KÖVETKEZTETÉSEK

A cikkben betekintést kínáltam a lézerek alapjaiba, fajtáiba és kiemelten foglalkoztam a lézeres felderítés, illetve a lézeres kommunikáció megvalósítási lehetőségeiről és az eddig megjelent eredményekről. A legnagyobb hangsúlyt a nemcsomósodó fotonnyaláb elméleti és technikai részleteire fordítottam. Ennek előállítása ígéretes lehetőség a lézerekkel történő titkos kommunikáció megvalósításához, ez azonban nagyon pontos ismereteket követel a rendelkezésre álló optikai eszközök tulajdonságairól.

Az egyik legfontosabb és leginkább várható eredmény a kijelölt kutatási területen a különböző robotok fedélzeti lézerfizikai eszközeinek méretcsökkenésre történő javaslatok kidolgozása a teherviselés megkönnyítése érdekében. A méretcsökkenés szempontjából kifolyólag itt lényeges lépés az adott berendezések energiafelhasználásának minimalizálása a nagy hatékonyság és a megbízható működés megőrzésével párhuzamosan. A másik legfontosabb várható eredmény pedig a különböző robottechnikai eszközök közötti védett lézeres kommunikáció eljárásainak kidolgozása, és a robotok biztonságos közlekedésének megvalósítása lézerfizikai eszközök segítségével.

Felhasznált irodalom

[1] Nánai László: A lézerek és katonai alkalmazásaik
http://www.szrfk.hu/rtk/kulonszamok/2005_cikkek/nanai_laszlo.pdf,
letöltés ideje: 2013.október 9.

[2] Subhash Chandra Singh, Haibo Zeng, Chunlei Guo, and Weiping Cai: Lasers: Fundamentals, Types, and Operations pp.1-3, 2012
http://www.wiley-vch.de/books/sample/3527327150_c01.pdf,
letöltés ideje: 2013. október 12.

[3] Glen P. Perram: Chemical lasers pp.1-7
http://www.afit.edu/en/docs/CDE/Chemical%20LasersWeb.pdf,
letöltés ideje: 2013. október 13.

[4] Verőné Wojtaszek Margorzata: A lézer alapú távérzékelés. In: Fotointerpretáció és távérzékelés 3. Nyugat-magyarországi Egyetem, 2010
http://www.tankonyvtar.hu/hu/tartalom/tamop425/0027_FOI3/ch01s03.html,
letöltés ideje: 2013.október 11.

[5] Ványa László: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. PhD értekezés, ZMNE 2003. p. 200.

[6] Kher Than: Record Set for Space Laser Communication, 2006.január 5
http://www.space.com/1900-record-set-space-laser-communication.html,
letöltés ideje: 2013.október 12.

[7] Schott glass made of ideas ,3 és 13.o
http://www.schott.com/advanced_optics/us/abbe_datasheets/schott_datasheet_all_us.pdf
letöltés ideje: 2013.október 12.

[8] Varga Péter: A Jánossy- kísérletek a fizikai optikában, Fizikai Szemle 1998/7. 225.o, MTA Műszaki Fizikai és Anyagtudományi Intézet, Budapest

[9] Varró Sándor, Dombi Péter: A fény klasszikus fizikai és kvantumelméleti jellemzése, Természet világa, 137. évfolyam, 4. szám, http://www.termeszetvilaga.hu/szamok/tv2006/tv0604/varro.html, letöltés ideje: 2013.október 13.

[10] Kurilla Boldizsár, Diplomamunka: A nemcsomósodó fotonnyaláb előállítása, Pécsi Tudományegyetem, 2009. június

[11] A. Miranowicz †, J. Bajer ‡, H. Matsueda †, M. R. B. Wahiddin § and R. Tanas : k Comparativenstudy of photon antibunching of non-stationary fields. J. Opt. B: Quantum Semiclass. In: Department of Information Science, Kochi University, 2-5-1 Akebono-cho, Kochi 780-8520, Japan; Laboratory of Quantum Optics, Palack´y University, 772 07 Olomouc, Czech Republic; Institute of Mathematical Sciences, University of Malaya, 50603 Kuala Lumpur, Malaysia; k Nonlinear Optics Division, Institute of Physics, Adam Mickiewicz University, 61–614; Pozna´n, Poland Opt. 1999

[12] A. Miranowicz (1), J. Bajer (2), W. Leonski and R. Tanas (3): Various approcaches to photon antibunching in second-harmonic generation (1997) In: Clarendon Laboratory, Department of Physics, University of Oxford; OX1 3PU Oxford, U.K.; Laboratory of Quantum Optics, Palack´y University, 772 07 Olomouc, Czech Republic; Nonlinear Optics Division, Institute of Physics, Adam Mickiewicz University, 61-614 Pozna´n, Poland

[13] X. T. Zou and L. Mandel: Photon-antibunching and sub-Poissonian photon statistics, Journals, Phys. Rev. A 41, 475–476 Department of Physics and Astronomy, University of Rochester, Rochester, New York 14627, 1990

[14] Sanjiv Singh and Jay West: Cyclone: A Laser Scanner For Mobile Robot Navigation. In: The Robotics Institute Carnegie MelIon University Pittsburgh, Pennsylvania 15213 (September 1991)

[15] Keigo Hara, Shoichi Maeyama, and Akio Gofuku: Navigation Using a Laser for a Mobile Robot with a Optical Sensor Array. In: Graduate School of Natural Science and Technology, Okayama University 3-1-1 Tsushima-Naka, Okayama 700-8530, Japan, 2008

[16] Julian Ryde and Huosheng Hu: 3D Laser Range Scanner with Hemispherical Field of View for Robot Navigation. In: Proceedings of the 2008 IEEE/ASME International Conference on Advanced Intelligent Mechatronics July 2 - 5, 2008, Xi'an, China

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Prisznyák Szabolcs
prisznyak.szabolcs@bv.gov.hu

A BVOP INFORMATIKAI KÖZPONTJÁNAK KOCKÁZATELEMZÉSE

Absztrakt

A cikk bemutatja a büntetés-végrehajtási szervezetnél megvalósított informatikai fejlesztést. A centralizált rendszerek üzemeltetése során új kockázatok váltak ismertté. Ezt követően ismerteti a Büntetés-végrehajtás Országos Parancsnokságának informatikai központjára vonatkozó kockázatelemzést. Az elemzés az ISO/IEC 27005 (2008) szabvány előírásai szerint készült. A cikk végén összegzi a tapasztalatokat, továbbá ismerteti a szükséges fejlesztési lehetőségeket.

The article presents the IT-development at the Hungarian Prison Service. At the operational of centralized IT-system transpired several new risks. After then the author shows the risk analysis of headquarters of Hungarian prison system by ISO/IEC 27005 (2008) standard. The author concludes the article by summarising the experience gained and outlining the prospects for further development.

Kulcsszavak: *büntetés-végrehajtás, informatikai fejlesztés, információ-technológia, kockázatelemzés ~ prison service, IT-development, information technology, risk analysis*

BEVEZETÉS

A büntetés-végrehajtási szervezet informatikai történetében mérföldkőnek számít a „Felelősen, felkészülten a büntetés-végrehajtásban” elnevezésű, EKOP-1.1.6-09-2009-0001 azonosítószámú, az Európai Unió támogatásával megvalósult informatikai fejlesztési projekt [1]. A projekt keretében közel 1,5 milliárd forint értékben megújult a büntetés-végrehajtási szervezet teljes informatikai rendszere. A fejlesztés azonban olyan rendszertechnológiai változásokat is magával hozott, amely újabb feladat elé állítja a szakembereket a nagy rendelkezésre állású központi informatikai üzemeltetés megvalósítása során.

Jelen publikációban bemutatom a megvalósított fejlesztés elemeit, illetve ismertetem, hogy ennek – és a változásokhoz illeszkedő logikai módosítások - eredményeként összességében milyen rendszertechnológiai, logikai változások következtek be [2]. Az erősen centralizálttá vált rendszer esetében kulcsfontosságú, hogy a Büntetés-végrehajtás Országos Parancsnokságának (BVOP) informatikai központja nagy rendelkezésre állással szolgálja ki a teljes szervezet információigényét. A rendelkezésre állás biztosításához szükséges felmérni a BVOP-n meglévő kockázatokat. A felmérés első lépéseként meghatároztam az informatikai rendszer működése szempontjából megvalósított funkció szerinti legmagasabb kockázatú helyiség, amely a BVOP központi gépterme. Ezt követően elvégezhető a helyiségre vonatkozó kockázatelemzés az IEC/ISO 27005 (2008) szabvány szerint. A kockázatelemzést jelen esetben kizárólag a központi gépterem esetében végzem el. A további helyiségek, helyiségcsoportok vizsgálata nem része jelen publikációnak.

Összképet adok a nagy rendelkezésre állást biztosító működés feltételeinek meglétéről, illetve ismertetem a szükséges fejlesztéseket.

A cikk elkészítéséhez feldolgoztam a témakörrel kapcsolatos tudományos publikációkat, valamint a kapcsolódó jogszabályokat. Az objektív kockázatelemzéshez figyelembe vettem Kerti András közleményében foglaltakat [3]. Tanulmányoztam a jelzett fejlesztés során keletkezett műszaki dokumentációkat. A több éves projektben, mint a BVOP informatikai fejlesztési osztályvezetője vettem részt. Ennek következtében munkám során fontosabb támasznak bizonyultak a megvalósítás és az üzemeltetés során szerzett személyes szakmai tapasztalatok.

A BÜNTETÉS-VÉGREHAJTÁS SZERVEZETI FELÉPÍTÉSE

A büntetés-végrehajtás állami, fegyveres, rendvédelmi szerv, amely külön jogszabályban meghatározott szabadságelvonással járó, büntetéseket, intézkedéseket, valamint büntetőeljárási kényszerintézkedéseket, továbbá elzárást hajt végre [4].

A büntetés-végrehajtási szervezet kormányzati irányítását a Belügyminisztérium végzi. A szervezet központi vezető szerve a Büntetés-végrehajtás Országos Parancsnoksága, amely főosztályai révén a büntetés-végrehajtási intézetekben folyó szakmai munka felügyeletét, ellenőrzését végzi. A büntetés-végrehajtási intézetek ellátják a büntetések és intézkedések végrehajtásával kapcsolatos feladatokat. A büntetés-végrehajtás a legtöbb magyarországi közigazgatási és rendvédelmi szervezettől eltérően nem három, hanem kétszintű szervezet. A központi (országos) szervezet alárendeltségébe közvetlenül a területi jogállású szervezetek tartoznak.

Magyarországon 28 önálló jogállású büntetés-végrehajtási intézet, 5 – egészségügyi és oktatási – intézmény, valamint 11 gazdasági társaság működik. Az informatikai szakterület kompetenciája a gazdasági társaságokra nem terjed ki, azok a büntetés-végrehajtási szervezet informatikai rendszerétől független önálló, elszigetelt rendszereket alakítottak ki.

A FEJLESZTÉS MEGVALÓSÍTÁSA

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtási szervezet eddigi legnagyobb és legátfogóbb informatikai beruházása. Ha hálózatokról beszélünk, külön kell választani a helyi hálózatokat (LAN), és a táv-adatátviteli hálózatot (WAN). Az EKOP-1.1.6 projekt keretében a helyi hálózatok fejlesztésére volt lehetőség. A táv-adatátviteli (WAN) hálózatot külső – kormányzati – szolgáltató üzemelteti, ugyanis a 346/2010 (XII.28.) Kormányrendelet 3.§ (1) bekezdés értelmében „…kormányzati célú hírközlési tevékenységet kizárólag a kormányzati célú hírközlési szolgáltató és az elkülönült hírközlési tevékenység végzésére jogosultak végezhetnek.” [5]. A hivatkozott kormányrendelet nevesíti a kormányzati célú hírközlési szolgáltatót, amely a Nemzeti Infokommunikációs Szolgáltató Zrt.

A helyi hálózatok fejlesztésénél elsődleges cél volt a homogén aktív eszköz park kialakítása. Ennek értelmében valamennyi switch cserére került, az új eszközök azonos gyártónak a termékei. Végeredményben modern, szabványos helyi hálózatok álltak rendelkezésre, amelyek kialakítása szakszerűen, igényesen történt.

A szerverpark kialakítása során a BVOP-n – a már meglévő gépteremben, amelynek kialakítására 2007-ben került sor - egy blade centerben 10 db új szerver üzembeállításával történt a központi infrastruktúra kialakítása. Az intézetek részére összesen 128 db rack szekrénybe helyezhető szerver került beszerzésre. Ez intézetenként 4 db szervert jelent (a pályázat benyújtásának időpontjában működő 32 intézettel számolva).

Munkaállomás oldalon szintén a szerverekkel azonos gyártótól kerültek beszerzésre az eszközök. A projekt keretében összesen 1200 db vékonykliens, 300 db asztali munkaállomás, valamint a működésükhöz szükséges 1500 db LCD monitor illetve 100 db notebook került beszerzésre.

A fejlesztéssel elértük, hogy egységes szerver infrastruktúra áll rendelkezésre, amely konszolidált módon, valamennyi helyszínen klimatizált gépteremben került elhelyezésre. A munkaállomások nagy része cserére került, így a karakteres Unix terminálok helyett megjelentek a grafikus operációs rendszerek és felhasználói programok futtatására is alkalmas eszközök. Az azonos gyártótól származó eszközök biztosítják a homogenitást, interoperabilitást, a felcserélhetőséget, átcsoportosíthatóságot.

A rendelkezésre állást biztosító eszközcsoport részeként beszerzésre került valamennyi szerverpark mellé 1 db szünetmentes tápegység, amely áramkimaradás esetén – terheléstől függően – 5-15 percig képes a folyamatos működést biztosítani. Ez elegendő lehet a pillanatnyi áramkimaradások áthidalására, illetve hosszabb áramkimaradás esetén elegendő áthidalási időt biztosít az áramfejlesztő készülék (aggregátor) indulásáig. Egységes platformra került az intézeti adatmentés is, egy jó minőségű hálózati mentőegység beszerzésével, és üzembeállításával. Ez az eszköz elegendő a teljes intézeti adatvagyont növekményes mentésére, szükség esetén visszaállítására.

A BVOP-n pedig egy nagy teljesítményű áramfejlesztő berendezés került telepítésre, amely áramkimaradás esetén a központi gépterem mellett a telefonközpont, valamint a 24 órában üzemelő ügyeleti helyiségek informatikai és biztonságtechnikai eszközeit is képes kiszolgálni.

A szoftver alapinfrastruktúrát tekintve a korábbi heterogén működés felszámolásra került. Kialakítottuk az országos címtárat, amelyet Microsoft Active Directoryval valósítottuk meg. Valamennyi szerveren Microsoft Windows Server 2008R2 operációs rendszer fut. Munkaállomás oldalon a vastag klienseken Windows 7 Professional operációs rendszer és Microsoft Office 2010 irodai programcsomag került telepítésre. A vékonyklienseken egy speciális Linux típusú operációs rendszer – eLux RL Lite – fut, amelynek alapfunkciója, hogy RDP kliensként képes terminal szerverhez kapcsolódni. Fontos eredmény, hogy valamennyi adat és program központi tárolásúvá vált, így lehetőség nyílt az adatvagyon képzésre, ennek

redundáns tárolására, mentésére. Az állománystruktúra a büntetés-végrehajtási szervezet Szervezeti Működési Szabályzatnak [6] megfelelő hierarchia szerint került kialakításra.

Az alkalmazásfejlesztések során megvalósult a FŐNIX rendszer, amely a korábbi fogvatartotti alrendszer korszerűsítése, rendszertechnológiai megújítása, funkcionális bővítése.

Szintén megvalósult a humán erőforrás adminisztrációt támogató alrendszer korszerűsítése, funkcionális bővítése. Ez a rendszer egy általános személyügyi rendszer követelményein túl megfelel a büntetés-végrehajtási szervezet – jogszabályból következő [7] - speciális igényeinek is, ennek alapján a következő modulokból épül fel: személyügyi modul, szolgálatszervezési modul, fegyelmi modul, egészségügyi-, fizikai-, pszichikai állapotfelmérés nyilvántartása modul.

Mindkét rendszer esetében azonos a központban történő programfuttatás, adattárolás, valamint a szerepkörök szerinti differenciált hozzáférés, amelynek alapja az Active Directory.

A BVOP HELYISÉGEINEK BESOROLÁSA FUNKCIÓK ALAPJÁN

A fejlesztés eredményeként a büntetés-végrehajtási szervezet teljes informatikai környezete megváltozott. A korábbi decentralizált szigetszerű informatikai rendszerek helyett egy erősen központosított megoldás került kialakításra. Az új megoldás egységes, homogén rendszer, azonban üzemeltetési szempontból kulcsfontosságúvá vált a BVOP informatikai központjának elérése. A minél nagyobb rendelkezésre állás biztosításához szükséges a BVOP kockázatelemzése az informatikai rendszer vonatkozásában. A kockázatelemzés során legcélszerűbb az IEC/ISO 27005 (2008) szabvány előírásait alkalmazni. A kockázatelemzés megkezdése előtt a BVOP helyiségeit az informatikai üzemeltetés szempontjából betöltött funkcióik szerint fel kell mérni, majd a rendszerben betöltött szerepük szerint csoportokba kell sorolni. Az informatikai rendszer működése, rendelkezésre állása szempontjából a legkritikusabb helyiség a BVOP központi gépterme. A további helyiségek csoportokba sorolása jelen publikációnak nem része.

A központi gépteremben az informatikai működés központja található, kiesése a büntetés-végrehajtási szervezet informatikai működését rövid időn belül ellehetetleníti.

A BVOP KÖZPONTI GÉPTEREM KOCKÁZATELEMZÉSE

A kockázatok elemzését az ISO/IEC 27005 (2008) szabvány C függelékében foglalt „Leggyakoribb fenyegetések” alapján végzem [8]. Az elemzés rendszer szintű kockázatelemzés, bizonyos esetekben – amennyiben az szükséges – részletes kockázatelemzésre is sor kerülhet. Az egyes fenyegetések bekövetkezésének valószínűségét 1-5 skálán sorolom be, ahol a bekövetkezés legkisebb valószínűsége 1. Ezt követően ismertetem a környezeti tényezőket és/vagy a tett intézkedéseket. Amennyiben szükséges ismertetem a kockázatok valószínűségének és/vagy hatásának csökkentéséhez esetlegesen szükséges további intézkedéseket.

Fizikai károk

- *Tűzkár:* bekövetkezés valószínűsége: 2. A helyiségnek megtörtént a tűzveszélyességi besorolása, a helyiségben éghető anyagok tárolása nem történik, a helyiség tűzálló ajtóval védett. A helyiségben automatikus oltóberendezés működik. További intézkedés nem szükséges.
- *Vízkár:* bekövetkezés valószínűsége: 1. Sem a helyiségben, sem a közvetlen környezetében – alatta, fölötte, mellette – nincs vízvezeték. A helyiségben nincs központi fűtés. A helyiség vízszint érzékelővel felszerelt, amely – a padozaton víz jelenléte esetén – riasztást végez. További intézkedés nem szükséges.

- *Szennyezés okozta kár:* nem releváns esemény, bekövetkezés valószínűsége: 1.
- *Berendezések megrongálódása, elvesztése:* bekövetkezés valószínűsége: 3. Az informatikai berendezések használat során tönkremehetnek, ennek ellensúlyozására a rendszerek szinte valamennyi esetben megfelelő redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre. Szükséges intézkedés: redundancia kialakítása valamennyi rendszer esetén.
- Por, rozsda, fagyás okozta károk: bekövetkezés valószínűsége: 1. A por és rozsda okozta károk nem releváns események. A fagyás valószínűsége is rendkívül alacsony, szükség esetén a redundáns klímaberendezések fűtésre is alkalmasak. További intézkedés nem szükséges.

Természeti esemény

- *Éghajlati jelenség*: Magyarország éghajlata kontinentális, szélsőséges éghajlati jelenségek előfordulása nem jellemző, így a kockázat nem releváns.
- *Szeizmikus jelenség:* Magyarországon a szeizmikus jelenségek (földrengések) nem jellemzőek, így a kockázat nem releváns.
- *Vulkanikus jelenség:* Magyarország területén nincs működő vulkán, a kockázat nem releváns.
- *Meteorológiai jelenség:* bekövetkezés valószínűsége: 1. A meteorológiai jelenségek közül a villámcsapás, amely lehetséges fenyegetés, ellene az épület villámvédelmének kiépítésével védekezünk, amely megfelelő műszaki színvonalon megoldott. További intézkedés nem szükséges.
- *Árvíz okozta károk:* bekövetkezés valószínűsége: kevesebb, mint 1. Az árvíz nem releváns fenyegetés, mert a BVOP épülete magasabban fekszik, mint a legmagasabb mért árvíz plusz egy méter, nagyon alacsony kockázati tényezőt jelent, hogy az épület a Dunától kb. 150 méter távolságra található, így esetleges kockázatot jelenthet egy árvíz másodlagos hatása. További intézkedés nem szükséges.

Kulcsfontosságú szolgáltatás kiesése

- *Légkondicionáló vagy a vízvezeték rendszer meghibásodása okozta kár:* bekövetkezés valószínűsége: 2. A vízvezetékrendszer meghibásodása nem releváns az informatikai rendszer működése szempontjából. A gépterembe 2013-ban új légkondicionáló berendezések kerültek telepítésre. A berendezések rendszeresen ellenőrzöttek karbantartottak. Két berendezés működik párhuzamosan, egyik kiesése esetén a tovább működő egység képes biztosítani a megfelelő működési hőmérsékletet. További intézkedés nem szükséges.
- *Áramellátás hibája (áramszünet):* bekövetkezés valószínűsége: 3. A BVOP épülete a múlt század elején épült, villamosítása az 1940-es, 1950-es években történhetett, azóta csak egyes szakaszok újjáépítése, javítása, bővítése történt meg. Az épület teljes elektromos felújítására évtizedek óta nem került sor. A kockázatot tovább növeli, hogy a belvárosban az épület környékén több nagy volumenű ingatlanfejlesztés is zajlik, és az építkezések során több esetben előfordul figyelmetlenségből vagy a megfelelő műszaki dokumentumok hiányából adódó vétlen nagyfeszültségű vezetékrongálás, amely áramkimaradást eredményezhet. A kockázatot csökkenti, hogy az informatikai központ teljes nagyfeszültségű kábelrendszere megújításra került, a BVOP épületének további rendszeritől függetlenítve. Beszerzésre került egy szünetmentes tápegység, amely a központi géptermet ellátja. Szintén beszerzésre került egy nagy teljesítményű áramfejlesztő berendezés (aggregátor), amely áramkimaradás esetén is biztosítja a központi gépterem áramellátását. További szükséges intézkedések: szünetmentes tápegység kapacitásának növelése.

- *Telekommunikációs berendezések meghibásodása:* bekövetkezés valószínűsége: 3. A telekommunikációs berendezések a BVOP telefonközpont rendellenes működéséből következhetnek. A telefonközpont redundáns. Meghibásodás esetén a tartalékegység (amely egy büntetés-végrehajtási intézetben található) automatikusan átveszi a vezérlést. További szükséges intézkedések: a telefonközpont teljes és alapos felülvizsgálata az üzemeltető NISZ Zrt. által a hibás működés esetszámának csökkentése érdekében. A redundancia logikájának felülvizsgálata, az automatikus folyamatok üzembiztos működésének kialakítása érdekében (jelenleg a rendellenes működést követő helyreállítás legtöbb esetben manuális beavatkozást igényel).

Sugárzás miatti zavar

- *Elektromágneses sugárzás okozta kár:* a kockázat nem releváns.
- *Hő sugárzás okozta kár:* a kockázat nem releváns.
- *Elektromágneses impulzus okozta kár:* nem releváns.

Információ kompromittálódás

- *Kompromittáló kisugárzott jelek elfogása*: a bekövetkezés valószínűsége: 1. A BVOP nem alkalmaz vezeték nélküli eszközöket. A gépterem az épület belső részén helyezkedik el. Az ingatlan területére ellenőrzötten, dokumentáltan történik a beléptetés. A múlt századi építészeti megoldások következtében a 80-100 cm-es falvastagság is csökkenti a jelfelderítés valószínűségét. További intézkedés nem szükséges.
- *Távoli kémkedés okozta kár*: a bekövetkezés valószínűsége: 1. A BVOP a kormányzati hálózat része, amelyet a NISZ Zrt. üzemeltet. A hálózat a távoli behatolás ellen több szintű logikai és fizikai védelemmel ellátott. További intézkedés nem szükséges.
- *Lehallgatás okozta kár:* a bekövetkezés valószínűsége: 1. A lehallgatáshoz a hálózatra fizikailag kell rácsatlakozni. Az épület fent ismertetett védelme jelentősen csökkenti a kockázatot. További intézkedés nem szükséges.
- *Média (adathordozó) vagy dokumentumok ellopása:* a bekövetkezés valószínűsége: 2. A kockázatot elsősorban a saját dolgozók jelentik. Az épületbe, az informatikai helyiségekbe a belépés korlátozott. Az adathordozók biztonságosan tároltak (lemezszekrény, páncélszekrény). A dolgozók tájékoztatása, oktatása megtörtént. További szükséges intézkedések: Az informatikai biztonsági oktatások számának növelése, rendszeressé tétele, a megszerzett ismeretek ellenőrzése. A dolgozókban a felelősségtudat kialakítása.
- *Berendezések ellopása: a bekövetkezés valószínűsége: 2*. A tett és a szükséges intézkedések azonosak a fenti pontban megfogalmazottakkal.
- *Kidobott, újrafelhasznált média (adathordozó) helyreállítása:* a bekövetkezés valószínűsége: kevesebb, mint 1. Minden használatból kivont adathordozó esetében adat helyreállítást lehetetlenné tevő roncsolásra kerül sor. További intézkedés nem szükséges.
- *Árulás, információk közzététele:* a bekövetkezés valószínűsége: 2. A dolgozók felkészítése, oktatása megtörtént. További szükséges intézkedés: további rendszeres oktatások a dolgozók részére, a tudatos magatartás kialakítása.
- *Megbízhatatlan forrásból származó adat:* a bekövetkezés valószínűsége: 2. A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.

- *Hardverek működésének befolyásolása*: a bekövetkezés valószínűsége: 2. A központi gépteremben található hardverekhez csak a kijelölt állomány férhet hozzá. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.
- *Szoftverek működésének befolyásolása:* a bekövetkezés valószínűsége: 2. A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A szoftverekhez csak a kijelölt állomány férhet hozzá. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. Problémát jelenthetnek a nem a BVOP állománya által felügyelt szoftverek.További szükséges intézkedések: tudatos magatartás kialakítása oktatással. A vírusvédelmi rendszer rendszeres ellenőrzése. A külső – szoftvereket telepítő, üzemeltető – partnerek esetében a megfelelő együttműködés kialakítása.
- *Pozíció (hely) kinyomozása*: a bekövetkezés valószínűsége: 1. A BVOP elhelyezkedése ismert, nyilvános információ, de ebből nem következik egyenesen a központi gépterem elhelyezkedése. A kockázatot csökkenti az épület védelme, a ki- és beléptetés szabályrendszere, annak betartása. További intézkedés nem szükséges.

Technikai meghibásodás

- *Eszközök, berendezések meghibásodása*: a bekövetkezés valószínűsége: 2. Az informatikai eszközök, berendezések használatuk során meghibásodhatnak, ennek kezelésére a központi rendszer elemei szinte valamennyi esetben megfelelő redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre. Szükséges intézkedés: redundancia kialakítása valamennyi rendszer esetén, a rendelkezésre állás további növelése.
- *Üzemzavar, hibás működés:* a bekövetkezés valószínűsége: 2. A fenti pontban megfogalmazottakkal azonos intézkedések történtek és szükségesek.
- *Információs rendszer telítettsége:* a bekövetkezés valószínűsége: 1. A rendszer folyamatosan ellenőrzött, mind automatikusan, mind humán erőforrás bevonásával. Szükség esetén a rendszerek automatikus megelőző figyelmeztetést küldenek. További intézkedés nem szükséges.
- *Szoftverek hibás működése:* a bekövetkezés valószínűsége: 2. A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. Problémát jelenthetnek a nem a BVOP állománya által felügyelt szoftverek. További szükséges intézkedések: A vírusvédelmi rendszer rendszeres ellenőrzése. A külső – szoftvereket telepítő, üzemeltető – partnerek esetében a megfelelő együttműködés kialakítása.
- *Az információs rendszer helyreállíthatóságának megsértése:* a bekövetkezés valószínűsége: 2. Az adatbázisokról, adatállományokról rendszeres, automatikus, több generációs mentéssel rendelkezünk. A mentések megfelelő helyen őrzöttek. Szükséges intézkedések: mentési rendszer kialakítása távoli telephelyre.

Illetéktelen cselekedetek

- *Illetéktelen eszközhasználat*: a bekövetkezés valószínűsége: 2. Az eszközök be- és kivitele az épületbe történő be- és kiléptetés során ellenőrzésre kerülnek. A gépterembe történő belépés korlátozott. Az eszközök hálózatra csatlakoztatása sem lehetséges a fizikai címre (MAC address) történő szűrés alapján. Egyes esetekben kockázatot jelenthet az USB alapú eszközök használata. Szükséges intézkedések: az USB alapú

eszközök egyedi azonosító alapján személyekhez rendelt módon történő központi felügyeletének kialakítása.

- *Szoftverek illegális másolása*: nem releváns esemény, bekövetkezés valószínűsége: 1

- *Hamis szoftverek használata*: nem releváns esemény, bekövetkezés valószínűsége: 1
- *Adatok elrontása (meghamisítása):* a bekövetkezés valószínűsége: 2. A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.
- *Illegális adathasználat (adatfeldolgozás)*: fentivel azonos.

Funkció kompromittálódása

- *Használat közbeni hiba*: a bekövetkezés valószínűsége: 3. A központi rendszer elemei szinte valamennyi funkciót tekintve redundánsak, illetve szükség esetére tartalék eszköz, alkatrész áll rendelkezésre. További szükséges intézkedések: újabb redundáns megoldások kialakításának folyamatos vizsgálata.
- *Jogokkal való visszaélés*: a bekövetkezés valószínűsége: 2. A jogosultsági rendszer úgy került kialakításra, hogy minden felhasználó csak a munkavégzéséhez szükséges jogosultsággal rendelkezik. További szükséges intézkedések: tudatos, felelősségteljes magatartás kialakítása oktatással, ellenőrzéssel.
- *Jogokról való megfeledkezés*: a bekövetkezés valószínűsége: 2. Fentivel azonos kockázat és intézkedések.
- *Tevékenység megtagadás*: a bekövetkezés valószínűsége: 1. A szervezet jellegéből adódóan nem releváns kockázat. További intézkedés nem szükséges.
- *Személyes hozzáférés megakadályozása*: a bekövetkezés valószínűsége: 1. Több személy is rendelkezik rendszerfelügyeletet és rendszerkonfigurációt biztosító jogosultságokkal. A rendszerek jól dokumentáltak. Amennyiben fizikai hozzáférési probléma történik (pl. elromlik a központi gépterem ajtajának zárja és az nem nyitható), annak kijavításáig távoli adminisztrációval biztosítható a rendelkezésre állás. További intézkedés nem szükséges.

ÖSSZEGZÉS

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtás történetének eddigi legnagyobb informatikai fejlesztése. Ebből következően – mivel az informatika szinte valamennyi munkafolyamat támogatásában érintett – döntően befolyásolja a szervezet működését. A fejlesztés rendszertechnológiai változásokat is magával hozott, amelynek következtében megváltoztak az informatikai rendszer működésének, elérésnek feltételei is.

Az új – erősen centralizált – környezetben kulcsfontosságú, hogy a központi rendszer a lehető legnagyobb rendelkezésre állású legyen. A rendelkezésre állás biztosításához, növeléséhez elengedhetetlen a teljes rendszer, illetve annak egyes elemeinek a felülvizsgálata. Az egyes kockázatok elemzéséhez, a kockázatok bekövetkezési valószínűségének csökkentéséhez, illetve a bekövetkezett események hatásának csökkentéséhez megtett és a jövőben szükséges intézkedések meghatározásához a nemzetközileg elfogadott ISO/IEC 27005 (2008) szabványt választottam.

Bízom benn, hogy elemzésem eredményeként rávilágítottam a fejlesztendő területekre, és felszínre kerültek olyan problémák is, amelyek a szabvány következetes – pontról pontra – történő alkalmazása nélkül csak egy már bekövetkezett esemény után derültek volna ki.

Véleményem szerint a kockázatelemzés eredményét és módszerét célszerű figyelembe venni más rendvédelmi (és/vagy közigazgatási) szervezet hasonló volumenű informatikai fejlesztése, vagy a meglévő rendszerek vizsgálata során. A szabványban meghatározott elvek és módszerek alkalmazásával magasabb rendelkezésre állású, biztonságosabban üzemeltethető informatikai infrastruktúrák alakíthatók ki.

Felhasznált irodalom

[1] SEBESTYÉN Attila: Büntetés-végrehajtás informatikai fejlesztési projekt. = Kommunikáció 2009, 2009 Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó - ISBN 978-963-7060-70-0

[2] A büntetés-végrehajtás országos parancsnokának 1-1/13/2011.(III. 22.) OP intézkedése a büntetés-végrehajtási szervezet informatikai biztonsági szabályainak kiadásáról

[3] KERTI András: Az információbiztonsági kockázatkezelés oktatásának buktatói = Kommunikáció 2013: Communications 2013, 2013 Nemzeti Közszolgálati Egyetem, pp. 53-60. - ISBN:978-615-5305-16-0

[4] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről

[5] 346/2010 (XII.28.) Kormányrendelet a kormányzati célú hálózatokról 3.§ (1)

[6] A büntetés-végrehajtás országos parancsnokának 1/2011. (V.6.) BVOP utasítása a Büntetés-végrehajtás Országos Parancsnoksága Szervezeti és Működési Szabályzatának kiadásáról

[7] 1996. évi XLIII. törvény a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

[8] International Standard ISO/IEC 27005 Information technology – Securtity techniques – Information security risk management

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Schüller Attila
schuller.a@gmail.com

ANALYSIS OF USER BEHAVIOUR FROM THE POINT OF VIEW OF INFORMATION SECURITY

Abstract

In information security, the human factor is the biggest threat as is true for the whole of safety technology. There are numerous regulations and recommendations that are intended to eliminate human errors and irresponsible behaviour. Some bad user behaviour is surveyed in this article, which points out that it has not been possible to reduce human errors to an acceptable level using current methods.

Ahogy a biztonságtechnika egészére igaz, úgy az információbiztonság részterületére is, hogy a legnagyobb veszélyt az emberi tényező jelenti. Számtalan szabályzás és ajánlás létezik, amely az emberi hibákat és felelőtlenségeket szándékozik kiküszöbölni. A cikk néhány rossz felhasználói viselkedést mér fel, ami arra hívja fel a figyelmet, hogy az emberi hibákat nem sikerült elfogadható szintre csökkenteni a jelenlegi módszerekkel.

Keywords: *információbiztonság, adatbiztonság, emberi tényező, felmérés ~ information security, data security, the human factor, survey*

INTRODUCTION

The discipline of information security has quite an old origin, as information security techniques were in use in the ancient world, such as cryptography (encryption) and steganography (data hiding). However, since its inception the problem has been in all systems and processes the people, that is, human frailty (e.g. corruptibility, carelessness, laziness, vulnerability to blackmail) can weaken the protection.

However, in many cases, the owners of information (companies, organizations, or individuals) do not pay enough attention to eliminating the negative effects of the human factor. Measures are often introduced for the sake of appearances but they are not able to protect against cybercrime.[1]

Cybercrime can cause damage of up to $600 billion a year worldwide according to the latest survey carried out by Symantec. [2] Although the number of reported security incidents has increased only marginally the amount of financial losses from intrusion appears to have been greatly reduced. However, because most companies do not use a common methodology when measuring these losses the data are only partially reliable.

In analysing the current situation, I examined the results of other research, before conducting my own survey of user habits. In addition, I analyzed people's actual behaviour using empirical methods, and I compared this with the answers that they gave in the survey.

ANALYSIS OF USERS' HABITS

The "Global State of Information Security Survey 2013" was carried out worldwide by CIO (Chief Information Officer News and Insight), CSO (Chief Security Officer Magazine) and PwC (PricewaterhouseCoopers). From their findings I would highlight the following. Most respondents believe their organizations have instilled effective information security behaviours into the organizational culture. The people carrying out the survey categorized respondents according to the way they describe their approaches to security. "Frontrunners (42%) say their organization has 'an effective strategy in place and is proactive in executing the plan.' These are key elements of true security leadership. Strategists (25%) say they are 'better at "getting the strategy right" than executing the plan,' while tacticians (16%) rate themselves 'better at "getting things done" than at defining an effective strategy.' Firefighters (16%) admit that they 'do not have an effective strategy in place and are typically in a reactive mode.' Based on these qualifications, the analysis reveals that only 8% of respondents rank as true leaders."[2] [3]

ISACA (Information Systems Audit and Control Association) is an international professional association that focuses on IT Governance. This organization also prepares an annual survey about information security.

According to the 2011 survey, 82% of companies with foreign shareholders have an information security strategy, this figure is only 59% for firms in 100% Hungarian ownership, while this figure is 61% for the respondents as a whole. However, only 18% of the respondent institutions aimed to develop a comprehensive information security strategy. Even worse is the case with the security awareness program, which is in place in 37% of the institutions, and only another 19% were planning its implementation. In terms of human factors, the worst situation was in the background checks as part of the admission procedure, only 17% of respondents carried out such checks. [4]

---

[1] By computer crime we mean crime committed for the purpose of profit or causing harm to IT systems to managed data confidentiality, authenticity, integrity, and availability, as well as the availability and functionality of system components or crimes committed using IT tools. [1]

[2] True leaders: „an elite group with the vision, determination, skills, and support to create the most effective security organizations." [3]

According to the 2012 survey, Hungarian companies have begun to realize the importance of an information security strategy, but we are still far from the cutting edge in terms of concrete steps. The use of administrative tools is more widespread than the use of technological tools. For example, nearly 50% of the companies surveyed have an overall information security strategy but only 14% of them have vulnerability analysis tools, as compared with the 46% internationally. [5] We should point out, however, that this result is worse than last year's, because 61% of the respondents had an overall information security strategy in 2011 [4], the rate has fallen, therefore, by 11%. The rate of application of vulnerability analysis tools was 25% [4], so this figure has also fallen by 11% in one year.

The situation has also deteriorated in respect of the IT risk assessment at an adequate depth. As shown in figure 1, the proportion of institutions where risk assessments are carried out regularly has decreased by 7% and the percentage of those which have no plans to introduce them has increased by 5%.

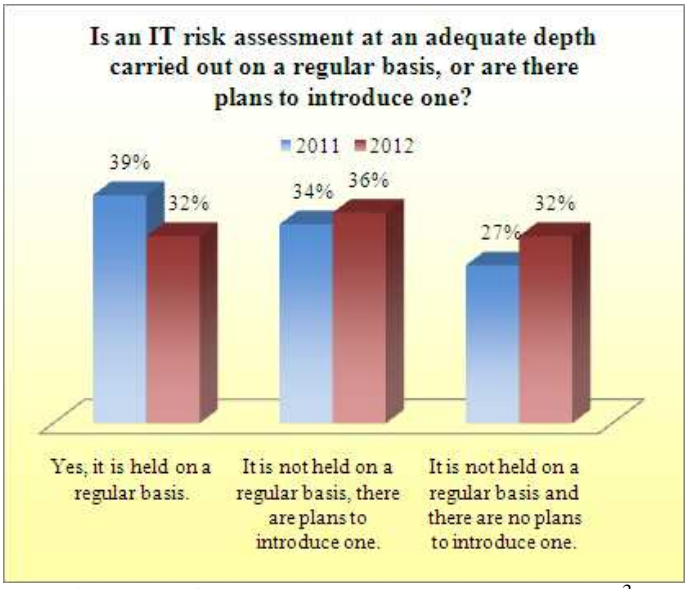


Figure 1. Changes in the IT risk assessment[3]

These surveys have been carried out at management level. They are, therefore, more likely to give information about what steps the company has taken to ensure information security and how strong it considers itself to be in this area. However, a bottom-up analysis of the organizations should be carried out to provide answers about how to ensure that the employees comply with the rules established. I have created a questionnaire to assess this and I examine the key indices for this.

I produced my questionnaire, which was in English and Hungarian, in such a way that people could fill it in online and their responses could be recorded directly in a database. Thus, after the data had been collected they could be easily evaluated using any spreadsheet software. These were two reasons for collecting data online: firstly I wanted to make use of modern technology as I have described above and secondly several of the questions were of a type that the majority of people either would not answer or would answer untruthfully if I had asked them personally. In [6] we learn that in China, for example, during the Cultural Revolution using traditional questionnaires it was almost impossible to gather valid and reliable data about the lives, opinions and attitudes of the Chinese with respect to the Communist regime.

I have previously investigated the attitude of the young with respect to information security (Hadmérnök 2/2011). During my present investigation I wanted to get as broad a picture as possible of the current situation. This is why I did not want to narrow it down by strictly defining

[3] This figure has been compiled by the author using sources [4] and [5].

the participants. I sent out the questionnaires not in a targeted, personalized way. Instead I asked the recipients to invite their friends to fill out the form, and I sent the Internet address of the questionnaire to on-line forums and a newsgroup too. Therefore is not possible to determine the exact number of respondents.

I received 139 responses after excluding those that contradicted themselves. They can be broken down into the following demographic groups. 87 women (63%) and 52 men (37%) replied. Among these 17 were under 15 years of age (12%), 33 were in the age group 16-20 (24%), 28 in the age group 21-25 (20%), 30 in the age group 26-30 (22%), 15 in the age group 31-40 (11%), 9 in the age group 41-50 (6%) and 7 were over 50 years of age (5%). 114 were born in Hungary (82%), 115 are at present living here (83%). 58 live in capital cities (42%), 22 live in other large cities (16%), 35 live in towns (25%) and 24 live in smaller locations (17%). It is also worthwhile to compare the distribution of persons of Hungarian origin and currently living in Hungary[4] with statistical data of the Hungarian population. I compare of these from different aspects. 36% (41) of the group of this respondents are male and 64% (72) of them female, while based on data from the population census 2011 [7], 47% of the Hungarian population are male and 53% of them are women. 43% (49) of Hungarian respondents live in Budapest, a further 10% (11) of them in other major cities, 27% (30) in small town, 20% of them in other settlements, by contrast, these rates were 17%, 20%, 32% and 31% respectively in the most recent census [8]. Other discrepancies can be seen in the field of educational qualifications. 40% (45) of the group containing members of Hungarian origin and currently living in Hungary completed primary school, 24% (27) of them completed high school and 36% (41) of them completed college or university, in contrast to the census statistics [9] in which the respective data were the following: 60%, 30% and 10%.

It can be seen from the data that the survey is not representative. Nevertheless, dividing the data to take into account differences with respect to age and gender may provide an opportunity to study and analyse the characteristic behaviour of the different groups. However, during my present investigation my aim was to measure the general risk to information security posed by the human factor, so I did not do this.

38% (57) of the respondents believe that their home PC or work computer cannot be attacked. This is the illusion of invulnerability: people believe – wrongly – that bad things can only happen to others. This unrealistic optimism has been shown in connection with several beliefs: people expect fewer health problems, fewer and less severe accidents, fewer failures etc. in their own future than what they might expect to happen to an average person similar to themselves. This behaviour is a natural defence against stress. [10] In the same way that people see themselves as better drivers and more cautious than they are in reality, this is also true for information security: if an antivirus and a personal firewall are installed on their computers, they think that this will protect them against all dangers. The illusion of invulnerability is also present at management level, when, after introducing robust information security rules, the managers sit back and relax, neglecting the considerable risk posed by the employees' non-compliance with these rules.

According to the Norton Cybercrime Report 2012, 14 adults become victims of cybercrime every second somewhere in the world. This means everyday more than a million people, which is twice as many as the number of newborn babies. 69% of adults surveyed had experienced cybercrime at some point in their lives. Compared with the 2010 survey overall, cybercrime increased by 3%. Over the 12 months examined, 15% of adults surveyed suffered a crime in the real world and 44% of respondents experienced cybercrime. [2] These data show that we are slow to respond to the challenge posed by the rapid increase in cybercrime. This lack of suspicion and preparedness are part of the reason why cybercrime is so effective.

[4] This figure is 113.

It is interesting to note that according to my survey, 17% (24) of respondents do not believe that the computers at their workplace are targets for hackers. They think, however, that their home PC is in danger. A workplace computer contains more important and (from the economic point of view) more valuable data, therefore, respondents presumably have concluded that their company computers are equipped with some serious protection, and are therefore much harder to access electronically.

41% (56) of users do not comply with the security measures. 4% (5) of them because they regard them as excessive, 37% (51) of them understand the need for regulations, but despite this, they do not pay attention to them. This very high ratio shows that with regulations alone, only a false sense of security can be achieved. In addition to the regulations, methods need to be developed and implemented that take away from the users the option to transfer their rights to another person, whether deliberately or through careless behaviour. Results were poor for those who declared in the questionnaire that they respect the information security measures. 29% (24) of these users use the same password everywhere, 20% (17) of them choose simple passwords, and 4% (3) of them leave their passwords in a place that is easily accessible. The above careless behaviour demonstrates that some people have a false sense of security and think that they are behaving in a responsible manner with regard to information security, while in reality they are making fundamental errors.

8% (11) is the number of those who – with or without permission – take home data from their workplace, although they do not comply with the security measures as they admitted in their response to a further question. One way for companies to protect themselves is if they do not allow corporate documents to leave the premises physically or electronically. According to the Kaspersky Lab survey, 29% of the companies surveyed prohibit, and a further 19% of them restrict the use of removable media (flash drives, external hard drives etc.) in one way or another. In 49% of the companies the FTP (File Transfer Protocol) connection, in 50% of them the cloud storage solutions, in 52% of them personal e-mail are prohibited or restricted. [11]

Biometric authentication within the enterprise could enhance information security in several ways. Thereby the access to data and the verification of the documents issued and updated by the user can be done easily and securely, however, partly due to legal regulations, and partly because of the users' aversion to such a method, in practice it is not used widely. The survey I conducted shows that 49% (68) of users would not be disturbed if biometric identification were employed at their workplaces, 16% (22) of them would be disturbed and 29% (41) of them would react positively or negatively depending on the method of identification. 6% (8) of the respondents did not answer this question.

Based on the survey data, 36% (50) of people do not give their passwords to anyone. This means the remaining 64% (89) of them are willing to reveal their passwords: 1% (2) to anyone, 39% (54) only to a trustworthy person, and 24% (33) only if after using it they change it immediately (figure 2). In my daily work, I experience worse rates: a significantly lower proportion of the people I come in contact with are unwilling to provide their access data, and at least 6-8% of them reveal their password without justification (in even worse cases, they add that they use the same password everywhere).

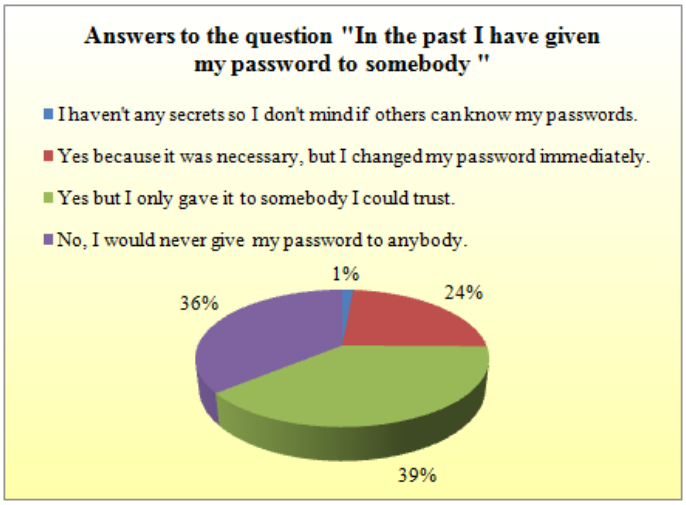


Figure 2. Willingness to reveal passwords

I got the following answers for the way people treat their passwords (figure 3). 4% (6) of the users write down their passwords in a place that is easily accessible. This can be very dangerous because it could easily fall into the wrong hands, allowing unauthorized access to the system. A better solution would be if the user wrote down their passwords in a way that nobody else could make sense of (e.g. the last 4 letters are the true password in a 7 character word). 6% (9) of the respondents said they use this method. 29% (40) of the respondents use the same password everywhere, so if access data for a system are obtained by unauthorised people they could easily penetrate the rest of the system too. 20% (28) of the survey participants choose simple passwords that are easy to figure out/decrypt/remember by somebody observing them. Only 5% (7) of users change their passwords regularly, but if more users did so, this would increase security significantly.

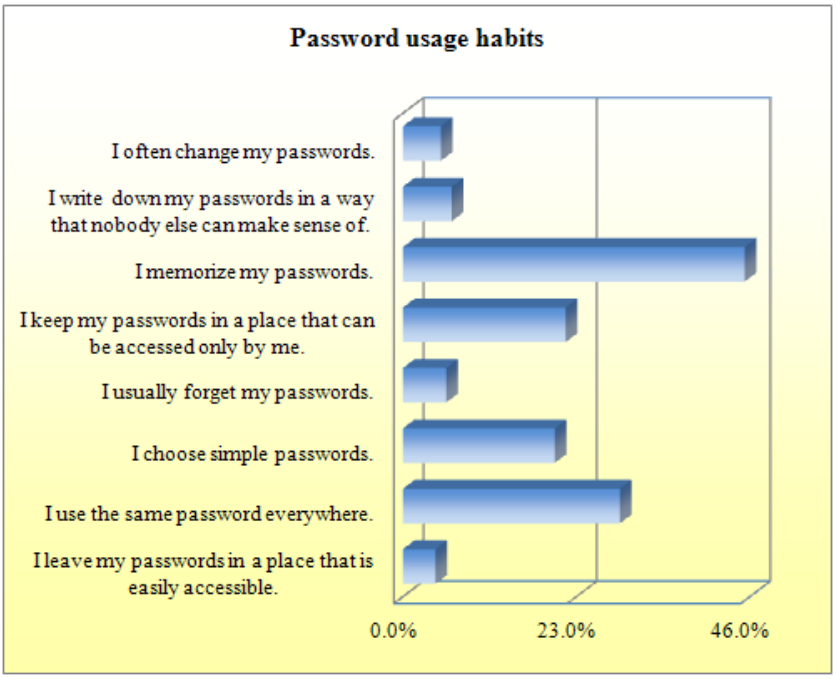


Figure 3. Password usage habits

I used an anonymous online questionnaire to collect data, because with it I was more likely to get true answers than if I had asked people personally. Nevertheless, the replies were often over-optimistic, which is also clearly visible in responses given about social networking sites. 6% (8) of respondents accept the fact that everybody can see their personal data, 27% (38) of

them say they have not given personal data, and 59% (82) of them have made them available only for their friends. 65% (90) of the survey participants claim that they only accept somebody as a friend if they actually know them and only 4% (5) responded that they accept everybody, even if they do not know them. I chose an empirical method to test this information. I created a fictitious person on one of the most popular social networks and I requested to be the friend of 60 people chosen at random. The first acceptance arrived within 4 minutes. I had 7 friends in 2 hours, and in the end I made 33 friends, so 55% of the people I chose accepted my request to be their friend, although we were complete strangers. Two other people accepted me as a friend without my request. On analyzing the data, I found that of these people, more than 60% (21) of them made available to strangers their place of residence, workplace and qualifications, 57% (20) of them revealed their marital status and birth place and 6% (2) of them their birthdays. Of course, this figure is higher for their friends, for example 89% (31) of them allowed their friends to read their birthday data. According to my survey on Facebook 71% (25) of users publish their e-mail addresses and/or telephone numbers, but only 3% (1) of people who make these data visible to anyone. 94% (33) of people upload photos of themselves and 89% (31) of them so that anybody can see them. In figure 4 I compared the answers of persons filling out the questionnaire with data experienced in reality. There were significant differences between the two groups. This does not mean that the respondents wanted to falsify the results, but they are not aware of the concept of personal data, so they believe that they have not given such information.[5]

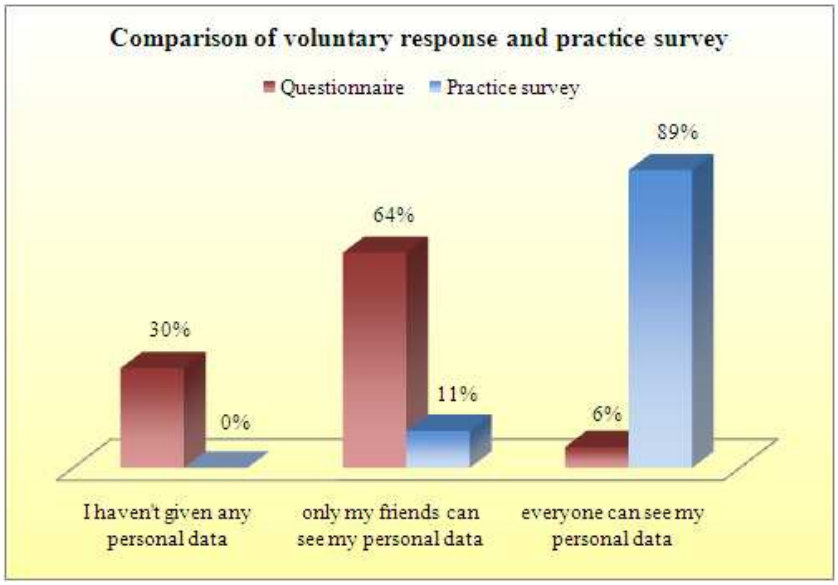


Figure 4. Indications of the human factor in the responses

The Hungarian Data Protection Act defines personal data as follows: data relating to the data subject, in particular the name and identification number of the data subject, as well as one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject. [12] It would be difficult to provide any data on this basis that is not considered personal data. People ought to be aware of the personal nature of same of their data (e.g. date of birth, marital status), however, the responses show that the majority of people do not consider such data personal, which they publish without any particular reservations.

[5] Of course I did not take into account the name in the survey because this piece of data is displayed in all cases. Users can register with a fake name, but I could not check up on this. However, they did not use a fake ID (e.g. the name of a film character) and I ignored other potentially dubious data (e.g. university studies in Bogota).

People give positive answers to some extent instinctively. The following factors can influence their judgement.

The *availability heuristic* can cause inaccuracies in the probability estimation: when applying it, the judgment of the frequency of an event depends on how imaginable the event is, how easy it is to remember, how interesting and how stimulating it is. People consider the very rare causes of death (e.g. murder) to be more frequent than they are in reality and consider the very common causes (e.g. heart disease) to be less frequent than they actually are. [10]

It is a typical and dangerous error when a specialist is overconfident in the correctness of their judgment *(overconfidence effect).* This group tends to trust too much in the results of science and fail to recognize the excessive complexity of the operating mechanisms of technical systems. Because of this feeling of security the experts are not encouraged to doubt their own opinions or to obtain additional information. [10] It is essential to bear this in mind because human behaviour is more complex and unknown than technical systems. The overconfidence effect can be experienced when the management is satisfied with the introduction of new security measures, but compliance with them is not checked.

The *wish for certainty* leads people to reduce the anxiety caused by uncertainty with an exaggerated and unfounded sense of security. Victims of flooding (wrongly) believe that the same disaster cannot happen to them again. [10] In information technology, it is the case that some people do not care about secure password management, despite the fact that their e-mail address or account for a social network has been used illegally previously.

CONCLUSION

Quantitative research is suitable for the investigation of certain areas, but we cannot rely only on surveys conducted among managers, because they examine information security from the point of view of the actions taken and planned, so they form a picture about the position they would like to reach, rather than the real state of affairs. Therefore, more emphasis should be placed on an analysis of the real situation, evaluating the results obtained and with continuous monitoring. In addition to the collection of questionnaire data, empirical research should be carried out, because responses may also be distorted unwittingly, as an inherent result of human nature.

„Too many cooks spoil the broth." I consider it to be a serious problem that IT professionals also believe that if a separate information security department has been created in their companies, then they do not have to deal with this area. In particular, because in many cases within the company the tasks of the information security department are interpreted in different ways. Many people expect this department only to ensure IT security, but in some companies its primary task is only the prevention of industrial espionage, while in others, this department only concentrates on checking the employees.

However, there is considerable overlap between information security and IT security, so the IT department is obliged to deal with confidentiality, integrity and availability as part of their duties, even if other departments carry out these tasks in the rest of the company.

The effect of the Internet also can be felt in relation to the careless handling of data, because in cyberspace, people give personal information to strangers more readily than if for example somebody went up to them in the street. The lack of personal contact reduces caution, and makes establishing contacts easier and less inhibited. This allows information to be extracted from unsuspecting users.

As my survey also revealed, despite the existence of strict information security rules the users do not always respect them. Security could be increased by reducing the human factor. There are various technical solutions which would remove the process of identification from people and thus reduce the danger of unauthorised persons gaining access. One possibility is

the use of biometrics, but people's aversion to such technologies and the lack of an appropriate legal framework still cause difficulties.

This article is supported by tender TÁMOP 4.2.2./B-10/1 (Risks and Answers in the Field of Talent Maintenance: "KOVÁSZ")

References

[1] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve. Verlag Dashöfer Szakkiadó, Budapest, 2000-2005

[2] Symantec: Norton Cybercrime Report 2012 http://us.norton.com/cybercrimereport/promo (16.06.2013)

[3] CIO, CSO, PwC: Changing the game. Key findings from The Global State of Information Security Survey 2013 http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf (10.06.2013)

[4] ISACA Információbiztonsági helyzetkép 2011 http://www.kpmg.com/HU/hu/IssuesAndInsights/ArticlesPublications/Documents/Informaciobiztonsagi-helyzetkep-2011.pdf (10.06.2013)

[5] ISACA Információbiztonsági helyzetkép 2012 http://letoltes.etrend.hu/Hetpecset/ppt_LIV_5/InfoBizt_helyzetkep.pdf (10.05.2013)

[6] Babbie, Earl: A társadalomtudományi kutatás gyakorlata. Balassi Kiadó, Budapest, 2003.

[7] KSH population census 2011: Population by citizenship and sex http://www.ksh.hu/nepszamlalas/docs/tables/regional/00/00_1_1_2_2_en.xls (26.02.2014)

[8] KSH népszámlálási adatok 2011.: A népesség számának alakulása, népsűrűség, népszaporodás településtípusonként http://www.ksh.hu/nepszamlalas/docs/tablak/demografia/04_01_01_01.xls (26.02.2014)

[9] KSH population census 2011: Population by education and age group http://www.ksh.hu/nepszamlalas/docs/tables/regional/00/00_1_1_4_1_en.xls (26.02.2014)

[10] Zoltayné Paprika Rita: Döntéselmélet. Alinea Kiadó, Budapest, 2005.

[11] Kaspersky Lab: Global IT Security Risks: 2012 www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf (16.06.2013)

[12] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Sergyán Szabolcs – Szénási Sándor - Vámossy Zoltán
sergyan.szabolcs@nik.uni-obuda.hu - szenasi.sandor@nik.uni-obuda.hu - vamossy.zoltan@nik.uni-obuda.hu

A GRAFIKUS HARDVEREN (GPGPU) IMPLEMENTÁLT ALKALMAZÁSOK SEBEZHETŐSÉGEI

Absztrakt

A grafikus kártyák eredetileg a képernyőn látható kép megjelenítéséért feleltek, az utóbbi évtizedben azonban ez a szerep jelentősen megváltozott, egyre több funkció végrehajtására lettek alkalmasak. Az első 3D gyorsítókártyák megjelenése (majd integrálása) jelentősen átalakította a GPU-k (grafikus vezérlő egységek) piacát. Napjainkban pedig a GPGPU (általános célú grafikus vezérlő egység) programozás már egyre inkább általánosnak tekinthető, különösen a nagy számításigényű alkalmazások területén. Míg azonban a játékprogramok és a kezdeti kutatások során a biztonság kérdése nem jelentett különösebb problémát, napjainkban már számos GPGPU alkalmazás dolgozik érzékeny (személyes, üzleti, állami) adatokkal. Emiatt érdemes foglalkoznunk az ezen a területen megjelenő biztonsági résekkel és lehetséges támadási módszerekkel.

Traditionally, graphics cards were responsible for the visualization of the content in the screen; however these devices have more and more tasks in the last few decades. The appearance of the first 3D accelerator cards changes the video adapter industry, in the next few years these new functions had been integrated into the GPUs (Graphical Processing Units).Nowadays GPGPU (General Purpose Graphical Processing Unit) programming becomes more and more general, especially in the field of High Performance Computing. In the first time, in case of games and initial research projects, data security was not an important factor. However nowadays, there are several GPGPU applications working with sensitive (personal, business, governmental) data. This paper deals with several questions of possible security holes and attack methods.

Kulcsszavak: *GPGPU, grafikus kártya, CUDA, biztonság ~ GPGPU, graphics card, CUDA, security*

BEVEZETÉS

A grafikus kártyák eredetileg a képernyő memóriában (karakteres és grafikus) található adatoknak a monitoron való megjelenítéséért feleltek, a 90-es évek közepén azonban ez fokozatosan kibővült számos egyéb funkcióval. Ezek közül a leglátványosabb és legismertebb a 3 dimenziós megjelenítés gyorsítása. Számos indok segítette elő ezen funkció kialakulását, egyrészt akkoriban egyre inkább elterjedtek a 3D grafikát tartalmazó játék és tervezőprogramok [1], másrészt jól látható, hogy a különböző alkalmazások 3D megjelenítési moduljai egymáshoz nagyon hasonlóak (még akkor is, ha maguk a programok teljesen különbözőek is voltak), illetve ez a funkció nagyon jól párhuzamosítható. Így először külön, majd integrált megoldásként megjelent ennek hardveres gyorsítása. A CPU-khoz hasonlóan itt is megjelentek az egyre több végrehajtóegységgel bíró változatok, hiszen a jól párhuzamosítható 3D megjelenítést jól lehetett gyorsítani a többmagos eszközökkel [2].

Az első generációkban ezek a kártyák különálló, egymástól jelentősen különböző alkatrészeket tartalmaztak a különféle feladatok végrehajtásához: vertex shaderek végezték a 3D-2D leképezést, pixel shaderek végezték az árnyékolást, textúrázást, illetve a geometry shaderek végezték a modellek módosításával kapcsolatos teendőket. A gyakorlatban azonban kiderült, hogy nagyon nehéz ezen eszközök megfelelő arányainak megtalálása, hiszen feladatonként nagyon változó, hogy hány darab vertex, illetve pixel shaderre van szükség. A több éves fejlődés folyamán a megoldást végül az jelentette, hogy ezek az eszközök az egyes generációk során egyre közelebb kerültek egymáshoz, majd végül megjelent az úgynevezett unified shader model, ahol már elmondhatjuk, hogy tulajdonképpen azonos típusú, általános célú eszközök helyezkednek el a kártyákon, amelyek mindegyik feladat végrehajtására alkalmasak.

Ezzel pedig elérkezett az idő, hogy már nem csak grafikai, hanem tetszőleges alkalmazásokat lehetett futtatni a grafikus kártyákon. A GPGPU program legfontosabb célja a minél nagyobb teljesítmény elérése, illetve az ennek leginkább megfelelő modell kidolgozása [3]. Ennek érdekében pedig a fejlesztők gyakran minden más tényezőt figyelmen kívül hagytak, köztük a biztonságot is. Az esetek jelentős részében (pl. játékprogramok esetén) ez nem jelent problémát, de mivel egyre több ipari alkalmazásban jelennek meg ezek az alkalmazások (pl. bankok, elemző és biztonságtechnikai cégek), mindenképpen érdemes részletesebben foglalkozni a biztonságpolitikai kérdésekkel is [4].

NEM SZÁNDÉKOS HIBALEHETŐSÉGEK

Szoftver biztonság területén általában elsőre mindenki a külső támadásokra gondol, azonban legalább ennyire fontos az is, hogy az egyes programok mennyire képesek a stabil működésre. Ez jelentős részben a programfejlesztői környezeten múlik, hogy mennyire tudják a fejlesztőket segíteni abban, hogy hibátlanul működő kódokat készítsenek [5].

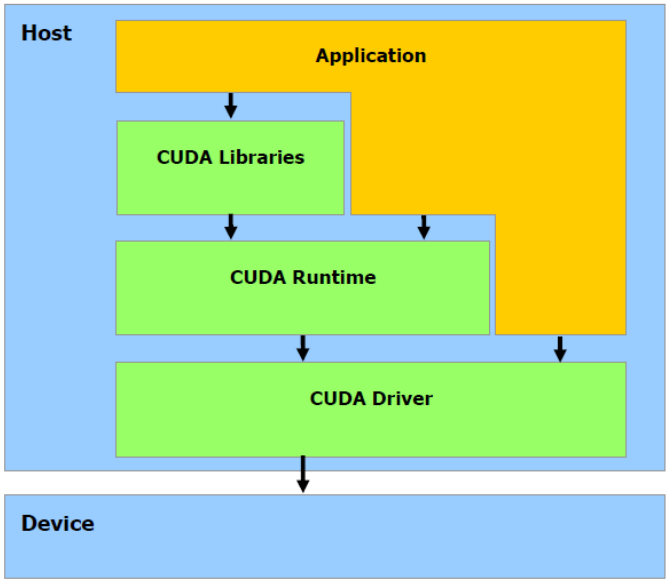
Hardver és szoftver hiányosságok

A GPGPU-ra való fejlesztés napjainkban már egy hétköznapi tevékenységnek számít, a fejlesztőeszközök azonban még nem tudták elérni azt a szintet, amit a hagyományos nyelveknél megszokhattunk. Rendelkezésre állnak ugyan a szükséges eszközök (fordítóprogram, nyomkövető program, teljesítménymérő program), ezek azonban nem mindig teljesen megbízhatók, és általában csak korlátozott funkciókkal bírnak (ami részben persze természetes, hiszen pl. a kód optimalizálás területén a C fordítóknak több évtized előnyük van).

A programkód felépítésénél ugyan rendelkezésre állnak már a modern programozás eszközei, akár objektum-orientált programok készítésére is lehetőség van a grafikus kártyán, ezek azonban még mindig nem terjedtek el teljesen. Maga a kódolás sok szempontból egy több

évtizeddel ezelőtti stílust idéz (globális változók, mutatók intenzív használata, kézi memória foglalás és felszabadítás, optimalizálás az áttekinthetetlenség árán is).

Mindezek a jellemzők azzal a káros következménnyel járnak, hogy a GPGPU kódok gyakran jóval megbízhatatlanabbak, mint hagyományos társaik. Érdemes megfigyelni a modern programozási nyelvek fejlődését (Java/C#), amelyeknél alapvető tervezési szempont volt a biztonságos kód készítésének lehetősége (szemétgyűjtő mechanizmus, mutatók elhagyása, OOP alapok, fejlett kivételkezelési technikák stb.), ezek azonban a grafikus kártya kódoknál egyelőre még hiányoznak.



1. ábra. A grafikus kártya elérésének szintjei.

A magasabb szintek az alattuk lévőkön keresztül férnek hozzá a tényleges eszközhöz.[6]

Grafikus kártya, mint fekete doboz

A grafikus kártyák programozása során számos olyan lépés jelenik meg, amelyeket a programozó nem tud pontosan befolyásolni, így az általa készített, majd továbbított programkód se lehet mindig teljesen megbízható. A felsorolt problémák között talán ezt tekinthetjük a legenyhébbnek, de mindenképpen érdemes említést tenni róla.

Ezen a területen még kevésbé terjedtek el a teljesen ingyenesen elérhető fordítóprogramok, osztálykönyvtárak, amelyekre bármikor lehet alapozni, hiszen a forráskód elérhető, bármikor áttanulmányozható. Egy kritikus rendszer fejlesztése során ez alapvető szempont lehet, és ezt a napjainkban legelterjedtebb CUDA programozási környezet nem teljesíti. Az Nvidia által készített eszközök, fordítóprogramok, osztálykönyvtárak nagyon jól használhatók, azonban azok pontos működése nem teljesen áttekinthető. A program írásához számos szintet igénybe vehet a fejlesztő, de mindig lesznek olyan területek, ahol nincs teljes átlátása a folyamat felett (Ábra 1.).

Hasonló problémát jelent a program futtatása is. A GPGPU kódok nem közvetlenül az operációs rendszer által kerülnek végrehajtásra, hanem az egész folyamatban lényeges szerepet játszik a grafikus kártya meghajtó program. Az indítandó kernelek ugyanis mindig ezen keresztül jutnak el a GPU-ra, és mindez megint csak felvet biztonsági problémákat. A szándékos károkozás mellett érdemes kitérni a hibalehetőségre is, ugyanis maguk a szerzők is találkoztak már olyan esetekkel, amikor egy egyébként tökéletes(nek tűnő) program egy meghajtó program frissítése után már hibás adatokat szolgáltatott.

Indeterminisztikus végrehajtás

Számos definíció létezik az algoritmus fogalmára, alapvetően az alábbi tulajdonságokat tekintjük mérvadónak: egy függvény kiszámítására szolgáló, véges számú, jól definiált utasítás sorozat; amely egy kezdőállapotból indul, az utasítások meghatározzák a végrehajtás menetét, majd véges számú lépést követően megáll a végső állapotban. Általában azt feltételezzük, hogy az egyik állapotból a másikba való átlépés determinisztikus, alapvető, hogy az algoritmus nem tartalmazhat nem pontosan definiált utasításokat. Ha egy utasításnak mégis több lehetséges kimenete van, akkor is önkényesen választanunk kell ezek közül egyet.

A fentiekből kiindulva, általában azt feltételezhetjük, hogy egy algoritmus mindig ugyanazt a kimenetet fogja visszaadni azonos bemeneti adatok esetében (még abban az esetben is, ha létezik több érvényes megoldás) [7]. Ez általában igaz is a tradicionális szekvenciális algoritmusokra, a többszálú megvalósítások esetében azonban már jóval összetettebb lehet a helyzet. A szálak pontos ütemezése ugyanis már nem a programozón múlik, hanem mindez futásidőben, a processzor aktuális terhelésének megfelelően történik meg (amit számos, az aktuálisan vizsgált programon kívüli körülmény is befolyásolhat). Természetesen írhatunk olyan programokat, amelyek kiküszöbölik ezeket az ütemezési különbségeket, de ez általában csak a teljesítmény nagyon erőteljes leromlásával együtt valósítható meg.

Érdemes persze azt is megjegyezni, hogy ezek a programok nem feltétlenül rosszabbak, mint a hagyományos programkódok. Elképzelhető, hogy az alkalmazás minden egyes futtatás során más-más eredményt ad vissza, ez azonban nem jelenti azt, hogy az eredmény hibás. Gondoljunk csak egy egyszerű példára: adjuk vissza egy szám valamelyik osztóját. Abban az esetben, ha több osztó is van, akkor több megoldás is elképzelhető. Szekvenciális algoritmusok esetében célszerűen egy egyszerű ciklussal megpróbáljuk megkeresni az első valódi osztót, míg párhuzamos algoritmusok esetén esetleg megpróbáljuk felbontani a lehetséges osztókat tartalmazó intervallumot több kisebb részre, és ezeken belül egy időben több processzorral is keresünk. Fontos különbség, hogy az első esetben a program minden egyes alkalommal ugyanazt a legkisebb osztót fogja visszaadni, míg a második esetben elképzelhető, hogy minden futás során mást, attól függően, hogy éppen milyen ütemezéssel futottak le a konkurens szálak. Azonban lényeges megjegyezni, hogy a feladat eredménye szempontjából a második eredmény semmivel se tekinthető rosszabbnak, mint az első.

A gyakorlatban azonban mégis jóval több problémát okoz egy ilyen nem determinisztikus algoritmus, aminek a legfőbb oka, hogy meglehetősen nehéz tesztelni. A tesztelés során általában elvárjuk, hogy ha egy megadott bemenetre a program hibásan válaszolt (vagy nem válaszolt), akkor újabb futtatásokkal tudjuk reprodukálni ezt a hibát. Alapvetően ezen a tényen alapulnak a különféle hibakereső eszközök is (töréspont, nyomkövetés). Mivel a GPU alkalmazásoknál előfordulhat, hogy ugyanazokra az adatokra egyszer jó, egyszer pedig hibás adatot ad válaszként a rendszer, ez jelentősen megnehezíti a biztonságos, garantáltan jól működő alkalmazások fejlesztését.

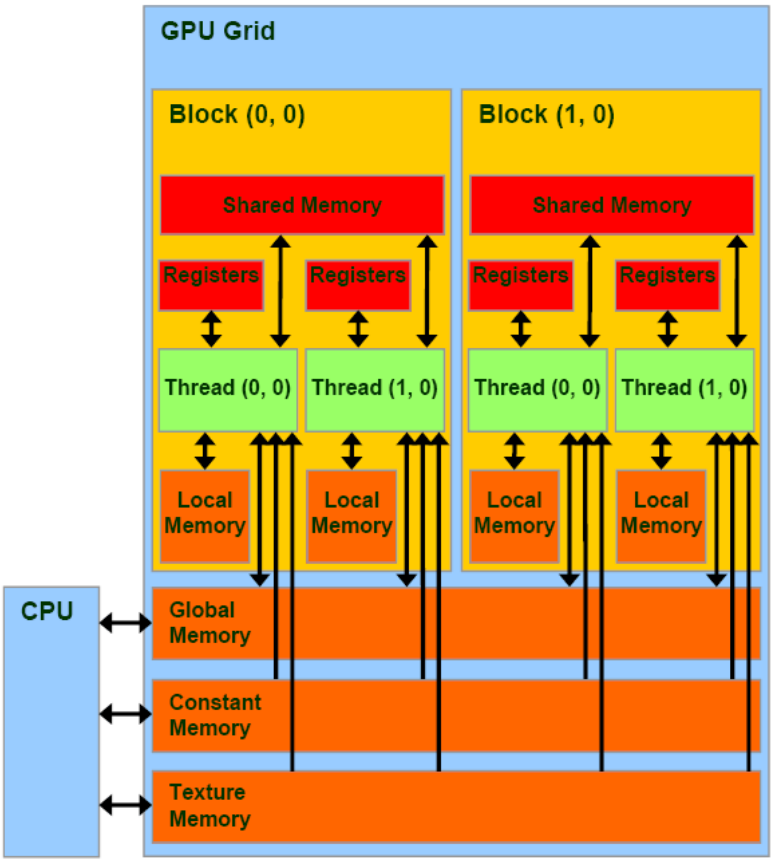
A tesztelés mellett ugyanis a hibakeresés ugyanilyen problémákat jelenthet. Még ha találunk is egy olyan bemenetet, amely hibás kimenetet okoz, akkor is meglehetősen nehézkes lehet a hiba helyének megkeresése. A klasszikus nyomkövető eszközök ugyan már rendelkezésre állnak többszálú környezetekben is, azonban semmi se garantálja, hogy a nyomkövetés során pont ugyanazt az eredményt adja majd az algoritmus, és így magát a hiba keletkezésének helyét is megtaláljuk majd. Arról nem is beszélve, hogy magának a nyomkövetésnek a használata már önmagában is hatással van a rendszer működésére, tehát lehet, hogy egészen más eredményekhez juthatunk a segítségével.

SZÁNDÉKOS TÁMADÁSOK

A fentieket ugyan meglehetősen kellemetlen, de mégis kezelhető problémáknak tekinthetjük, amelyeket kellő odafigyeléssel és időráfordítással meglehetős biztonsággal kezelhetünk. Ezeknél jóval veszélyesebbek a szándékos támadások, hiszen azok lehetnek egészen váratlanok, illetve jellegükből adódóan nehezen felderíthetőek. Maga a GPU a támadások eszköze is lehet [8], de egyben a támadás célpontja is, mi csak ez utóbbi lehetőséggel foglalkozunk most.

Memory leaking – globális memória

Alapvető biztonsági követelmény, hogy ha egy számítógépen (multitaszk környezetben) egyidőben több alkalmazást futtatunk, akkor azok egymás adataihoz ne férjenek hozzá (hacsak nem ez a kívánt állapot). Természetesen ugyanez igaz a grafikus kártyákra is, hiszen nyilvánvaló biztonsági kockázatot [9] jelent, ha pl. egy GPGPU alapú titkosító program által lefoglalt memória régiókhoz hozzáférhetnek más programok is, ezzel még a titkosítás előtt el tudják lopni az értékes információkat.



2. ábra. CUDA memória hierarchia [10]

A probléma megoldását a *process isolation* jelenti, amely garantálni tudja, hogy egy processz ne tudjon hozzáférni más processzek munkájához. A gyakorlatban ez számos szoftver és hardver alapú módszer összehangolását foglalja magában. Magát az izolációt különféle szinteken tudjuk megvalósítani, lehet akár hardveres, operációs rendszer szintű, vagy akár alkalmazás szintű is (pl. egy böngésző esetén lényeges, hogy egy esetleges kártékony oldalt megjelenítő ablak ne férhessen hozzá egy másik oldalon megnyitott banki információkhoz).

GPU-k esetében a különféle technikák még meglehetősen kezdetlegesnek tekinthetők, bár megjelentek előrelépések aziránt, hogy az egyes GPU alkalmazások ilyen téren is biztonságosak legyenek, azonban ez még mindig számos támadási pontot rejt magában.

Az egyik támadási lehetőség a GPU globális memóriájának elérhetőségében rejlik (Ábra 2.). Különféle tesztek segítségével nagyon könnyen ellenőrizhető, hogy amennyiben egy CUDA alkalmazással lefoglalunk, használunk, majd felszabadítunk memóriát, akkor a következő, az előzővel paramétereiben megegyező memóriafoglalás nagy valószínűséggel ugyanazt a GPU memóriaterületet fogja majd visszaadni. Mivel a memória felszabadítás során nem történik meg az érintett területek törlése (nullákkal való feltöltése), így a következő lefoglaláskor az előző alkalmazás által hátrahagyott memóriatartalom érintetlenül olvasható.

Ebben az esetben szerencsére egy egészen egyszerű megoldással sokat lehet tenni, a kernel futását követően, még a kilépés előtt (de mindenképpen a memória felszabadítása előtt) érdemes nullákkal feltölteni a használt memóriaterületet. A CUDA környezet természetesen csak akkor tudja odaadni az előzőleg használt memóriaterületet egy következő alkalmazásnak, amikor az előző azt már felszabadította, ennek köszönhetően a kernel futása közben ettől a támadástól még nem kell tartani, a kernel leállításakor kitörölt memóriatartalomnak köszönhetően pedig utána sem jelent veszélyt.

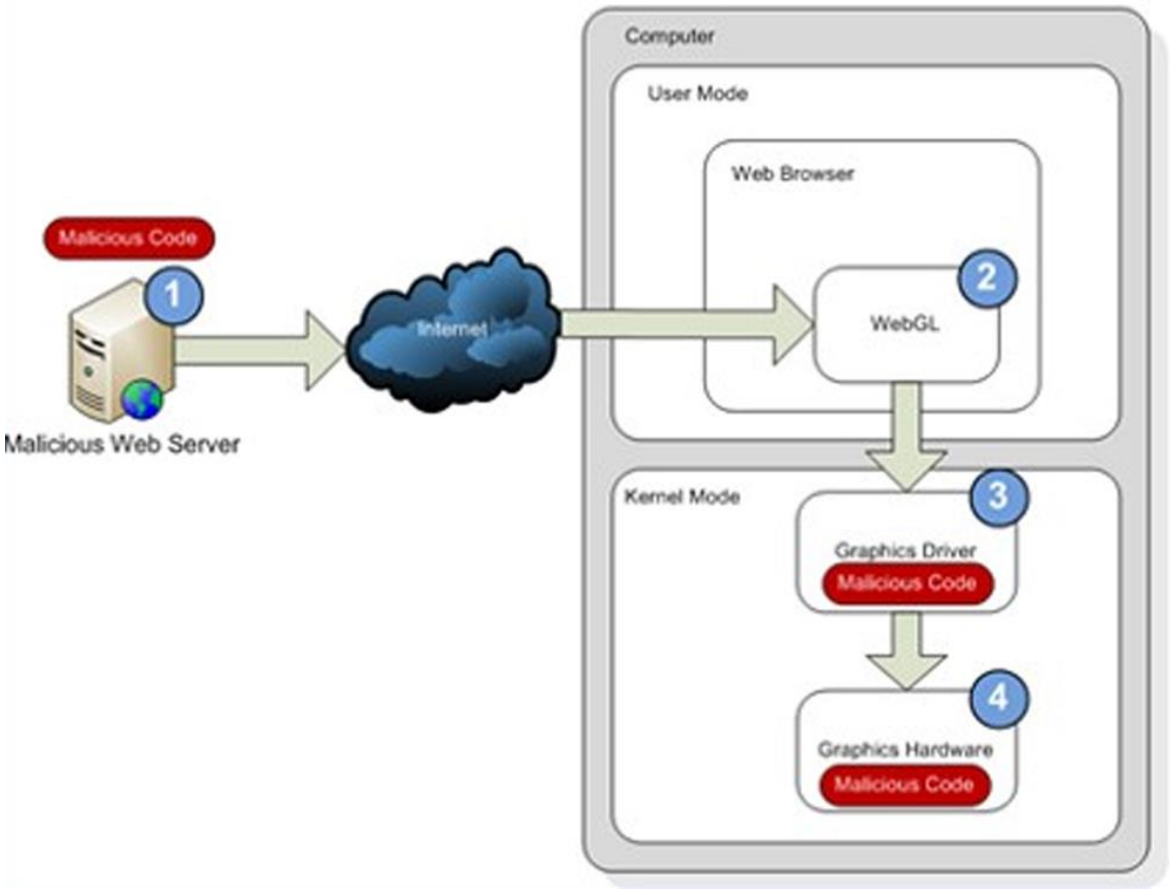
Memory leaking – megosztott memória

A GPU-k meglehetősen összetett memória hierarchiával rendelkeznek (Ábra 2.). A legnagyobb területet az úgynevezett globális memória teszi ki, amely elérhető mind a CPU, mind pedig a GPU számára. A GPU-k emellett rendelkeznek egy úgynevezett megosztott memória (shared memory) területtel is, ami valamilyen szinten megfelel a CPU-k esetében jól ismert gyorsítótárnak, habár működésük jelentősen különböző.

A megosztott memóriában tárolt adatok jelenleg szintén nem tekinthetők teljesen biztonságosnak. A GPU működéséből az ütemező ugyanazokat a végrehajtó-egységeket egymást követően más-más kernelek futtatására jelölheti ki. Ezek a kernelek érkezhetnek különböző kontextusból is, és amennyiben nem történt meg a megosztott memória törlése, a kontextusváltást követően az aktuálisan futó szálnak lehetősége nyílik arra, hogy hozzáférjen az előző szálak által használt adatokhoz.

Ahogy Roberto Di Pietro et al. [11] mintaprogramok segítségével is meg tudta mutatni, ennek az a negatív hatása, hogy a káros programok az ilyen kontextusváltásokat követően is hozzáférnek az előző alkalmazások adataihoz.

A globális memóriában látható hasonló eseményekhez viszonyítva ez számos pozitív és negatív tulajdonsággal bír. A pozitív, hogy a megosztott memória a CPU számára teljesen láthatatlan, az csak a GPU kerneleken keresztül érhető el. Így az itt eltárolt adatok kiolvasásához is GPU kernelek futtatására van szükség. A jelenség meglehetősen nagy hátránya azonban az, hogy a GPU szálak számára a kiolvasás megoldható, és ami még kockázatosabb, hogy mindez futásidőben történik, tehát a kernel leállításakor történő törlés már nem elégséges, a kiolvasás addigra esetleg már rég megtörtént (érdemes egyébként megjegyezni, hogy a kernel leállításakor a megosztott memóriában a GPU meghajtó eleve végrehajt egy törlést, tehát ezt nem is szükséges explicit módon kiadni).



3. ábra. WebGL támadás vázlata. 1) A felhasználó megtekint egy weboldalt, ahol WebGL script található 2) a WebGL-en keresztül ez feltölti a szükséges kódokat a grafikus kártyára 3) ez a kód tartalmazhat ártó szándékú kódokat 4) ezen keresztül magát a grafikus hardvert lehet támadni (pl. lefagyasztani)[12]

DOS támadások

A Denial-of-Service támadás már mindenki számára ismerős, habár elsősorban más területeken találkozhatunk vele [13]. GPU-k esetében az alapelv tulajdonképpen azonos, magát az eszközt kell túlterhelni valamilyen formában annyira, hogy az ne tudjon válaszolni az őt érő kérésekre, így ne tudja elvégezni a neki szánt feladatokat. Ez főleg akkor lehet kritikus, ha egy számítógépben csak egy grafikus kártya található, és ezt sikerül annyira leterhelni, hogy az már nem képes ellátni az operációs rendszer által neki szánt megjelenítési feladatokat.

Mindez nem csak elméletben, hanem a gyakorlatban is nagyon könnyen tetten érhető. Különösebb támadási szándék nélkül is, egyszerűen a GPU fejlesztés során is néha előfordul, hogy az elkészített program tesztelése során valamilyen hiba történik, és a program túl sokáig nem válaszol. Ennek eredménye lehet egy egyszerű hibaüzenet, de szerencsétlenebb esetben az egész operációs rendszer összeomlása is.

Mindez támadási céllal is használható, miként azt Patterson [14] is bemutatta. Az általa készített segédprogram folyamatosan hívásokat intézett a grafikus kártya irányába, ami miatt az nem tudott válaszolni az operációs rendszer meghajtónak. Az operációs rendszertől függ az ilyen támadások kimenete. Az általunk is vizsgált Windows7 esetében be van építve egy védelem, aminek köszönhetően abban az esetben, ha a grafikus kártya meghajtó nem válaszol egy megadott időn belül (néhány másodpercre kell gondolni, de ez módosítható), akkor az operációs rendszer egy hibaüzenet megjelenítése mellett automatikusan leállítja és újraindítja a hibásan működő modult.

A gyakorlatban azonban ez számos problémába ütközhet. Egyrészt, maga a védelem nem tudta minden esetben meghiúsítani a támadást, bizonyos esetekben maga az operációs rendszer is összeomlott. Másrészt, bizonyos esetekben éppen az intenzív GPU használat miatt ki kell kapcsolni ezt a védelmet, mivel az leállítana minden, néhány másodpercnél tovább futó GPU kernelt (függetlenül attól, hogy azok éppen értékes munkát végeznek). Harmadrészt, valószínűleg ki lehet játszani ezt a védelmet egy olyan támadással, ami a néhány másodperces terhelések közé néha egy-egy kisebb szünetet iktat, ami miatt az operációs rendszer továbbra is üzemel, azonban a számítógép gyakorlatilag használhatatlanná válik.

A probléma részben orvosolható azzal az egyszerű megoldással, ha nem csak egy, hanem több grafikus kártyát használunk a gépben. Így a kártékony szoftverek csak a számukra kijelölt kártyát tudják túlterhelni, ez azonban nem befolyásolja a második, a képernyő megjelenítésért felelős kártya működését. Ez utóbbi célra gyakran még az alaplapra integrált, meglehetősen kis teljesítményű kártyák is alkalmasak lehetnek.

Malware támadások

GPU alapú kártevőkről napjainkban még nem igazán beszélhetünk, de ez nem zárja ki, hogy ezek nem jelenthetnek egészen komoly veszélyt a közeljövőben [15]. A legnagyobb problémát az jelenti, hogy napjaikban a vírusirtó eszközök nincsenek felkészítve az ezekhez hasonló károkozók keresésére, illetve ez technikailag is meglehetősen nehezen kivitelezhető, hiszen a GPU mind az adatok, mind pedig az aktuálisan futtatott programok szempontjából egy sokkal nehezebb kontrollálható eszköz, mint amit hagyományosan megszoktunk.

Részben persze megnyugtató, hogy maga a GPU egy alapvetően független eszköznek tekinthető, ami meglehetősen korlátos képességekkel bír. Így ugyanis attól nem kell tartanunk, hogy a GPU-n futó kódok közvetlenül kárt okozzanak a merevlemez tartalmában, vagy akár hálózati kommunikációt folytassanak, hiszen napjainkban erre egyszerűen nincs technikai lehetőségük. De érdemes megjegyezni, hogy a fejlesztések egyre inkább afelé haladnak, hogy a GPU-kat minél inkább függetleníteni tudjuk a CPU-któl, ez pedig óhatatlanul is az általuk elérhető egyéb erőforrások irányába vezet.

ÖSSZEGZÉS

Az önálló GPU alkalmazások napjainkban még ritkák, azonban az újszerű eszközök használata egyre gyakrabban jelenik meg különféle kiegészítő modulokban (megjelenítés, grafikus gyorsítás, adatpárhuzamos számítások stb.). Ennek megfelelően a támadásokról is ritkán esik szó, de érdemes felkészülni arra, hogy ezek a közeli jövőben megjelennek és folyamatosan egyre inkább elterjedhetnek.

Mindezt támogatják azok a törekvések is, amelyek afelé irányulnak, hogy a grafikus kártya minél inkább egy általános célú végrehajtó eszköz legyen. Ehhez már elkészült a megfelelő hardver és a szükséges szoftver környezet, és a jövőbeni tervek alapján hamarosan a GPU elszigeteltsége is változni fog. Hozzáférhet a PCI-E buszon keresztül a többi hardver elemhez, a központi memóriához, illetve várhatóan előbb-utóbb integrálva lesz a CPU mellé, ami újabb lehetőséget nyújthat majd a támadók számára.

Szoftver téren is egyre több helyen jelenik meg az új eszköz, a játékok már régóta használják a GPU-t a megjelenítés mellett a fizikai szimulációkra is, de pl. a MATLAB esetében is van már lehetőség GPGPU használatra a számítások végrehajtásakor. Napjainkban kezd terjedni a WebGL (Ábra 3.) komponens, amely lehetővé teszi, hogy weboldalakban letöltött JavaScript is hozzáférjen a grafikus kártyához, ami megint egy újabb potenciális csatornát nyithat a rosszindulatú kódok számára. Mivel ez a lehetőség az összes webportál típusnál adott [16], így ez különösen megkönnyíti majd az ilyen károkozók tevékenységét.

Felhasznált irodalom

[1] T. Hashimoto, T. Suzuki, H. Aoshima, A. Rövid, „Real-Time and High Precision 3D Shape Measurement Method”, Acta Polytechnica Hungarica, vol. 10, no. 8, 2013, pp. 139-152

[2] L. Vokorokos, E. Chovancová, J. Radušovský, M. Chovanec, “A Multicore Architecture Focused on Accelerating Computer Vision Computations”, Acta Polytechnica Hungarica, vol. 10, no. 5, 2013, pp. 29-43

[3] J Tick, C. Imreh, Z. Kovács, “Business Process Modeling and the Robust PNS Problem”, Acta Polytechnica Hungarica, vol. 10, no. 6, 2013, pp. 193-204

[4] V. Póser, T. Schubert, M. Kozlovszky, D. Prém, “Security on-demand megoldások az informatikai infrastruktúrákban”, Hadmérnök, vol. 8, no. 3, pp. 211-222

[5] H. Jeon, M. Wilkening, V. Sridharan, S. Gurumurthi, G. Loh, “Architectural Vulnerability Modeling and Analysis of Integrated Graphics Processors”, The 9th IEEE Workshop on Silicon Errors in Logic - System Effect (SELSE), Stanford, 2013

[6] CUDA Programming Guide, http://developer.download.nvidia.com/compute/cuda /3_0/toolkit/docs/NVIDIA_CUDA_ProgrammingGuide.pdf

[7] R. L. Bocchino Jr., V. S. Adve, S. V. Adve, M. Snir, „Parallel Programming Must Be Deterministic by Default”, HotPar ’09, Berkeley, 2009

[8] A. Keszthelyi, „About Passwords”, Acta Polytechnica Hungarica, vol. 10., no. 6, 2013

[9] E. Tóth-Laufer, M. Takács, I. J Rudas, “Interactions Handling Between the Input Factors in Risk Level Calculation”, 11th International Symposium on Applied Machine Intelligence and Informatics (SAMI 2013), Herlany, 2013

[10] J. van Oosten, „CUDA Memory Model”, 3D Game Engine programming, 2011

[11] R. D. Pietro, F. Lombardi, A. Villani, “CUDA Leaks: Information Leakage in GPU Architectures”, arXiv:1305.7383, 2013

[12] T. O’Brien, „WebGL flaw leaves GPU exposed to hackers”, www.engadget.com, 2013.11.

[13] Zs. Haig, „Classification of Information Based Attacks”, Hadtudományi Szemle, vol. 2, no. 3, 2009, pp. 9-14

[14] M. J. Patterson, „Vulnerability analysis of GPU computing”, MSc thesis, 2013

[15] G. Vasiliadis, M. Polychronakis, S. Ioannidis, “GPU-Assisted Malware”, 5th International Conference on Malicious and Unwanted Software (MALWARE), 2010

[16] S. Munk, M. Molnár, “Web portálok típusai, jellemzőik”, Hadmérnök, vol. 4, no. 1, 2009, pp. 235-253

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Tóth András
toth.hir.andras@uni-nke.hu

NATO LÉGI BÁZISOK KOMMUNIKÁCIÓJÁNAK BIZTOSÍTÁSA

Absztrakt

A cikk tárgya és célja bemutatni egy a modern kor hadviselésének megfelelő NATO légi bázis kommunikációs rendszereinek elvi és gyakorlati megvalósítását. A publikációban bemutatásra kerülnek a repülőtér egy elvi felépítése és annak informatikai, rádiós, mikrohullámú és műholdas összeköttetési lehetőségei.

The aim and the subject of this article is to show the theoretical and practical implementation of a NATO air base in mondern warfare. The publication presents a basic structure of the airport and its IT, radio, microwave and satellite communication possibilities.

Kulcsszavak: *NATO légi bázis, baráti erő követő rendszer, műszeres leszállító rendszer, művelet irányító központ – NATO air base, Blue Force Tracking System, Instrument Landing System, Operation Centre*

BEVEZETÉS

A világon napjainkban végbemenő katonai műveletek esetében, azok jellegétől függetlenül – háborús, vagy nem háborús – kiemelten fontos a légi utánpótlások és támogatások rendszere. Minden egyes esetben szükség van a személyi állomány, illetve a technikai eszközök folyamatos légi hídon történő mozgatására. Ennek előnye, hogy gyors és egy időben nagy mennyiségű anyagmozgást tesz lehetővé. A légi műveletek másik fajtája a terület(ek) légi műveletekkel történő támogatása repülők, harci helikopterek csapásaival. Ezek biztosításához egyebek mellett szükséges egy megfelelően kiépített kommunikációs és informatikai rendszer. Mivel ebben az esetben katonai műveletek közvetlen közelében elhelyezett repterekről beszélünk így a kommunikációs rendszerekben is többfajta hálózat jelenik meg. Szükség van egy a reptér védelmét szolgáló rendszerről, valamint a légi forgalmat támogató kapcsolatokról. A védelmi rendszer esetében többnyire egy minimálisan kétgyűrűs rendszerről beszélhetünk. Belülről kifelé haladva az első ilyen gyűrű a felszállópályák biztonságát szolgáló védelmi erők kommunikációját hivatott biztosítani, amíg a többi (egy, vagy több) külső gyűrű magának a teljes repülőtér és az azt kiszolgáló személyzet védelméért felesős szolgálatokat támogatja. A légi forgalmat támogató kapcsolatok nyújtják a kommunikáció lehetőségét a repülő eszközök részére légi és földi mozgásuk során egyaránt.

A KÜLSŐ VÉDELMI ERŐK KOMMUNIKÁCIÓJÁNAK BIZTOSÍTÁSA

Ebben az esetben többségében földi eszközök, valamint a kezelő személyzet részére biztosítandó kommunikációs rendszerekről beszélhetünk. Egy repülőtér külső őrzés-védelmi rendszere ugyanúgy kerül megszervezésre, mint egy bármilyen katonai tábor azonos szolgálata. Minden egyes ilyen jellegű objektum első és egyben legfontosabb pontjai a táborba történő beléptetést biztosító kapuk (ellenőrző-áteresztő pontok, továbbiakban EÁP). A kapuk a műveleti területet tekintve nagyon különbözőek lehetnek. Több esetben jellemző már, hogy kiépítésre került egy előretolt EÁP, ezt üzemeltethetik akár már helyi erők is. Ennek megfelelően a híradás szempontjából ez egy külön kommunikációs rendszer kiépítését vonja maga után, ahol csak a saját katonák által üzemeltetett kapu illetve az EÁP-on szolgálatot teljesítő erők tartják a kapcsolatot. Erre azért van szükség, hogy a helyi erőknek semmilyen körülmények között ne legyen lehetősége a szövetséges rendszerekbe történő belépésre. Ebben az esetben beszélhetünk mind vezetékes, mind vezeték nélküli összeköttetésekről is. A vezetékes kiépítéshez elégséges lehet akár csak egy pont-pont összeköttetéssel telepített tábori beszélő készülék is, mivel az EÁP állománya csak a kapun szolgálatot teljesítő állomány parancsnokával kell, hogy tudjon kommunikálni a felsőbb szintekre történő jelentést minden esetben ő fogja megtenni. Rádiós összeköttetés esetén elégséges csak egy kis hatótávolságú kézi rádióeszköz alkalmazása nyílt üzemmódban, mivel ezen a csatornán semmilyen rejtett információ nem kerülhet továbbításra.

A kapuk kommunikációja azok méretétől függően kerül kiépítésre. Amennyiben csak egy kisebb, pár főt foglalkoztató szolgálati helyről beszélünk nem szükséges a rádió összeköttetés a szolgálati személyek között. Ez a legritkábban előforduló eset. Amennyiben ez már egy területét tekintve nagyobb kapu, több szolgálati személlyel, szükséges úgyszintén a kézi rádiók alkalmazása. Itt már egy kulcsolt forgalmi rendszerről beszélünk, mivel ebben az esetben már előfordulhat az őrzés-védelmi tevékenységekkel összefüggő nem nyílt információk továbbítása is. A kapun minden körülmények között telepítésre kerül egy nagyobb teljesítménnyel bíró rádió eszköz a tábor területén telepített őrtornyokkal, illetve több kapu esetén az azokkal történő kapcsolattartásra. Egy hálózat kiépítésre kerül a műveletirányító központ irányába is, amely hivatott a szóbeli jelentések, utasítások adására-vételére. Ez minden esetben egy fixen telepített rádióval kerül telepítésre, zárt csatornán. A vezeték nélküli kommunikáció mellett szükséges a

vezetékes összeköttetés kiépítése is. Ebben az esetben már egy a tábor területén működő távbeszélő hálózatra történő csatlakozás alkalmazása tűnik a legmegfelelőbb megoldásnak, de amennyiben ez a hálózat a felhasználók száma miatt telített, akkor kiépítésre kerülhet egy a védelmi rendszert szolgáló hálózat is. Távközlő hálózatok mellett a kapukon megjelenik az informatikai hálózat is. Ezen keresztül küldhetőek a szükséges írásos jelentések, adatok. Úgyszintén ehhez kapcsolódhat a mostanában egyre több helyen jellemző biometrikus beléptető rendszer is.[1] Az informatikai rendszer a műveletirányító központtal biztosít összeköttetést, ahonnan minden egyes a feladat ellátásához szükséges információ érkezik. Ilyenek lehetnek az estleges veszélyfigyelmeztetések, lehetséges látogatók, katonai konvojok érkezése, a biometrikus rendszer adatbázisának frissítései. A kapun telepített számítógépek hálózatba kötésének legcélszerűbb formája egy optikai hálózat kiépítése, de a helyi sajátosságoknak megfelelően sok esetben az egy mikrohullámú összeköttetéssel kerül megvalósításra (lásd Kép 1, a felszállópálya alatt optikai kábellel került kiépítésre a hálózat, míg a baloldalon elhelyezett kapu irányába mikrohullámú összeköttetést alkalmazunk).

A műveletirányító központban található a tábor védelmi szolgálatának vezető eleme. Így minden egyes a saját csapatok, vagy a szövetségesek által ellátott szolgálat csatornái ide futnak be úgy a kapukkal, mint az őrtornyokkal, illetve a különböző reagáló erőkkel és táboron kívüli konvojokkal történő kapcsolattartást biztosító kommunikációs rendszerekkel. Az eddigieknek megfelelően itt is megtalálhatóak a vezetékes, a vezeték nélküli és az informatikai hálózatok egyaránt. A tábor és a koalíciós erők méretétől, a fenyegetettségi helyzettől és a műveleti tevékenységtől függően itt akár tíz, vagy annál több különböző méretű rádióforgalmi rendszer is megjelenhet, ami komoly technikai hátteret követel meg. Ez abból következik, hogy a műveleti központ nem csak a saját csapatok vezetését látja el, hanem kapcsolatot tart a szövetséges erők különböző erőivel és a helyi erőkkel egyaránt. Ennek biztosításához olyan eszközökre van szükség, amilyenekkel ezek a csapatok rendelkeznek, vagy kompatibilis ezekkel az eszközökkel. Azonban érdemes a szervezésnél figyelembe venni, hogy ha több alegység is található a körzetben, akivel összeköttetést szeretnénk kiépíteni és mindegyik különböző nemzethez kapcsolódik, a legjobb megoldásnak mindenképpen egy kompatibilis rádió mutatkozik. De sajnos ebben az esetben is problémát jelenthet a kulcsolás. Előfordulhat, hogy rendelkezünk olyan rádióval, amely kompatibilis egyes adásmódokban a másik rádióval, de amint egy rejtett vezetést szeretnénk létesíteni az eltérő kulcsolás miatt a kommunikáció nem lesz lehetséges, így csak nyílt csatornán tudunk beszélni. Mindezeket figyelembe véve, ha védett kommunikációt szeretnénk kiépíteni, találnunk kell egy olyan eszközt, amely képes számunkra ezt biztosítani. Napjainkban minden egyes NATO tagország rendelkezik már HARRIS[2] rádiókkal, ami megkönnyíti ezeket a szervezési eljárásokat, természetesen itt még felléphet az a probléma, hogy ugyanazon szoftvernek kell futni minden egyes készüléken, illetve rendelkezni kell az aktuális kulcsokkal.

Mivel jelen esetben csak kis távolságú kommunikációról beszélünk, a tábor felelősségi területét figyelembe véve körülbelül 20 kilométer, elegendő az ultra-rövidhullámú (továbbiakban: URH) eszközök alkalmazása.[3] Ebben a tartományban megtalálhatóak a kézi, a hordozható és a beépített verziójú rádiók egyaránt.

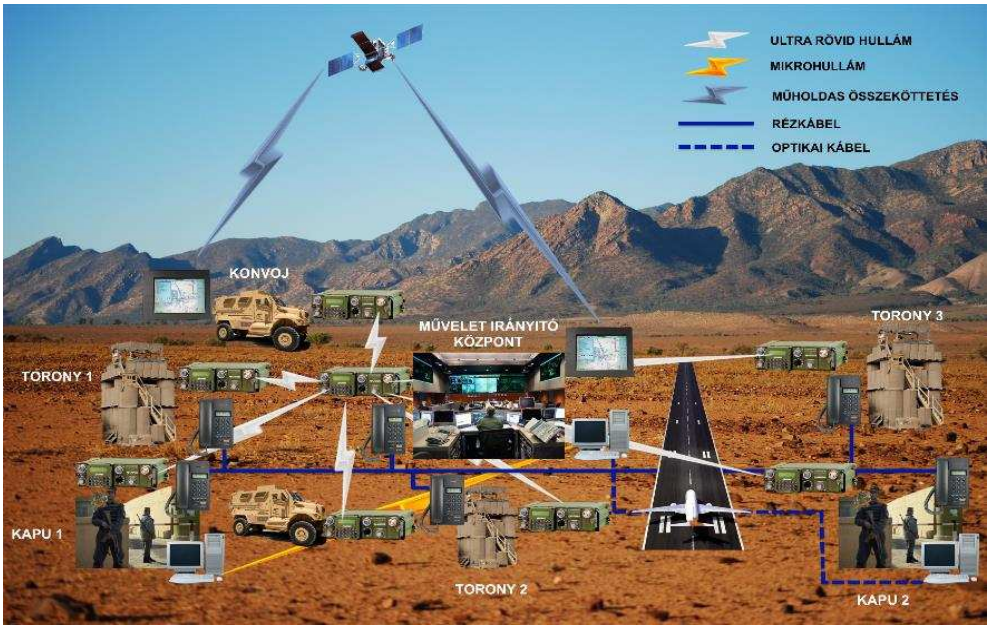
---

[1] "A biometrikus azonosítások az emberi szervezet, vagy viselkedés valamely egyedi jellemzőjének felismerésén alapulnak. Használunk arc-, hang-, írisz- retina-, kéz- és ujjnyomat azonosítást, DNS elemzést, de ide sorolhatjuk magát az aláírást, mellyel nap mint nap bizonyítjuk, hogy azonosak vagyunk saját magunkkal" - http://oktel.hu/szolgaltatas/belepteto-rendszer/biometrikus-azonositas/

[2] A HARRIS egy nemzetközi kommunikációs és információ-technológiai vállalat, amely kiszolgálja a kormányzati és kereskedelmi piacot a világ több mint 125 országában. A HARRIS a vezető harcászati rádió szállítója a NATO-nak és az Amerikai Védelmi Minisztériumnak. Összességében napjainkig több mint 450,000 Falcon szoftverrel ellátott rádió került leszállításra világszerte. – www.harris.com

[3] Az URH frekvenciatartomány 30-300 MHz-ig terjed, de jelen esetben csak a katonai alkalmazásban használt 30-88 MHz tartományt vettem figyelembe.

Úgyszintén telepítésre kerülhet a saját, vagy a felelősségi területre érkező konvojokkal történő kapcsolattartásra, követésére egy úgynevezett Blue Force Tracking System (BFTS – Baráti Erő Követő Rendszer)[4] amely egy számítógépen, térképi felületen mutatja a felelősségi területünkre és a saját és szövetséges csapatokra vonatkozó információkat a hasonló eszközzel rendelkező erőkről, eszközökről. A rendszernek nagy előnye, hogy műholdas jellege miatt alkalmas minden területi körülmények között az összeköttetés fenntartására, nem befolyásolja a hegyvidékes terep, és lakott területen belül is közel 100%-os biztonsággal használható.



1. ábra. Külső őrzés-védelmi vázlat

A FELSZÁLLÓPÁLYÁK KOMMUNIKÁCIÓS RENDSZEREI

A felszállópályák esetében is több hálózatról beszélhetünk. Minden egyes repülőtérrel rendelkező katonai bázison felállításra kerül egy olyan őrszolgálat, amelyik hivatott a felszállópályák biztosítását ellátni. Ők ellenőrzik a területre belépő személyeket, behajtó járműveket és magát a teljes területet. Ezekben az esetekben nem csak illetéktelen személyekről és járművekről beszélhetünk, hanem a légi forgalmat nagyban veszélyeztető felszálló pályára, vagy annak közvetlen közelébe tévedt állatokról. Minden ilyen esemény azonnali közbeavatkozást igényel, amely egy jól megszervezett kommunikációs rendszert követel meg. Az őrszolgálat rendszere az esetek nagy többségében nem a fent említett műveletirányító központba kerül bekötésre, mivel tevékenységük nem függ össze közvetlenül a felelősségi körzetben végbemenő műveletekkel, ezen feladatok ellátására egy felszállópálya biztosító központot hoznak létre. Az itt szolgálatot teljesítő katonák tartják a kapcsolatot a különböző helyeken felállított őrökkel, ide fut be minden egyes jelentés, és intézkednek a felmerült problémák elhárítására. Az összeköttetés URH rádiókkal kerül kiépítésre. Ezek többnyire kézi rádiók, de megtalálhatóak a harcjárműbe szereltek is amennyiben az őrség rendelkezik a szolgálat ellátásához rendszeresített eszközökkel, valamint megjelenhet a fixen telepített rádió is az őrtornyokban.

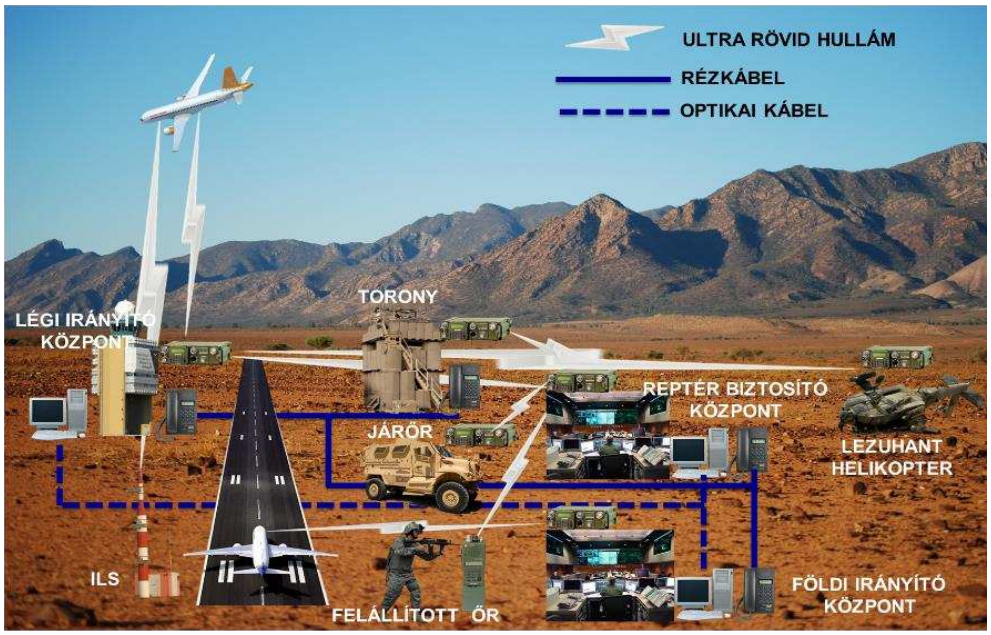
Az őrséggel történő kapcsolattartás mellett szükség van a földön közlekedő repülő eszközökkel biztosított kommunikációra is. Ez az összeköttetés úgyszintén indulhat a fent említett felszállópálya biztosító központból, de egy külön szolgálat is felállításra kerülhet. Innen

[4] A BFTS egy GPS-alapú baráti erő követő rendszer, amely a saját csapatok NATO egyezményes jelek szerinti kék színéről kapta nevét

kap meg minden szükséges információt a repülő eszköz személyzete a leszállástól egészen a felszállás megkezdéséig. A földet érést követően, miután az irányítótorony elirányította a gépet a leszállópályától, egy URH frekvencián irányítják a repülőgépet, vagy helikoptert a megfelelő parkolóhelyre és itt kap meg minden olyan információt, amely szükséges lehet például a kirakodás, vagy a berakodás megkezdéséhez. A felszállás megkezdése előtt ugyanezen a csatornán elirányítják a felszállópályához vezető utakra. Ezt követően az irányítótorony veszi át az irányításukat, tőlük kapják meg az információkat, hogy melyik úton közelítsék meg a felszállópályát, és sorrendben mikor kezdhetik meg a felszállást. Innentől kezdve a torony lesz az, aki a kapcsolatot tartja a gépekkel, amíg azok el nem hagyják a légteret, illetve a légtérbe érkezést követően úgyszintén a toronnyal kell felvenni az összeköttetést. A torony természetesen összeköttetésben áll minden egyes földi irányító központtal annak érdekében, hogy minden zavartalanul működjön az adott területen mind rádión, mind vezetéken egyaránt.

Mindemellett számos olyan rendszer üzemel még, amely segíti a légi forgalmat irányító személyzet munkáját. Ilyen például a műszeres leszállító rendszer, eredeti nevén Instrument Landing System (továbbiakban: ILS). Ez egy kétkomponensű rádió navigációs rendszer, amelynek a földi eleme biztosítja az információt a leszálló gépek számára, ezeket a jeleket a gépen elhelyezett ILS vevők veszik, kiértékelik és továbbítják a pilótának. A rendszer lényege, hogy segíti a pilótákat a leszállópálya helyes megközelítésében, amennyiben a látási viszonyok nem teszik lehetővé a normál leszállást. A rendszer olyan pontos, hogy az arra alkalmas robotpilóta is képes elvégezni a leszállást, akár emberi beavatkozás nélkül is.[5]

Működik egy olyan vészhelyzeti hálózat is, amely rendeltetése a légi járművek és azok kezelő személyzetének baleset esetén történő felkutatásának segítése. A rendszer lényege, hogy minden egyes eszköz, illetve a személyzet számára rendszeresített mellény rendelkezik egy adóval, amely például a helikopter lezuhanását követően automatikusan bekapcsol, a katonák esetében pedig egy gomb megnyomásával aktiválható. Minden egyes repülőtér irányítótornyában felállításra került egy olyan rádió, amely csak ezt a frekvenciát figyeli, és amint ezen megjelenik egy jellegzetes vészhelyzeti hang a reptér kijelölt személyzete háromszögeléssel képes meghatározni a jel forrását.



2. ábra. A felszállópálya kommunikációs hálózata

[5] http://hu.metapedia.org/wiki/M%C5%B1szeres_lesz%C3%A1ll%C3%ADt%C3%B3_rendszer

Mint az a fenti képekből látható a reptér üzemeltetésénél műveleti területen jelentős számú kommunikációs hálóról és irányról beszélhetünk, amelynek menedzselése komoly szakmai tudást és megfelelő technikai hátteret követel. Ennek végrehajtását a törzs egy kijelölt csoportja végzi, akik felelősek az összes üzemelő kommunikációs hálózatért. Frekvenciamenedzselési tevékenységet látnak el a zavarást végző szervezetekkel együttműködve, biztosítják az üzemeléshez szükséges összes forgalmi adatot, eszközt. A távbeszélő, valamint az informatikai rendszer zavartalan működése érdekében kapcsolatot tart az azokat üzemeltető személyekkel, szervezetekkel. Amennyiben szükséges felkészítést tart az újonnan érkezett állománynak a beosztásukhoz rendszeresített eszközök használatáról, illetve biztosít számukra minden olyan információt, amellyel munkájukat zavartalanul képesek ellátni.

ÖSSZEGZÉS

A cikkben bemutatásra került egy NATO légi bázis műveleti területen történő kiépítésének egy elvi vázlata, és annak minden irányú kommunikációs hálózata. A hálózat üzemeltetéséért a bázis törzsének kijelölt személyzete felelős, akik tartják a kapcsolatot a kezelő személyzettel, valamint az üzemeltetésért felelős személyekkel, szervezetekkel. Minden egyes hálózati elem beüzemelése (rádiók, telefonok, számítógépek) az ő engedélyükkel az eszköz hálózatra gyakorolt hatásának vizsgálata után lehetséges.

Felhasznál irodalom

[1] Farkas Tibor főhadnagy: A válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében, Doktori (PhD) értekezés; ZMNE Budapest; 2010

[2] Richard J. Dunn, III.: Blue Force Tracking. The Afghanistan and Iraq Experience and its impilcation of the U.S. Army, p.5-6

[3] http://www.casa.gov.au/wcmswr/_assets/main/pilots/download/ils.pdf, (2013. 12. 10.)

[4] FM 100-7 DECISIVE FORCE: The Army In Theater Operations Chapter 8: Military Operations Other Than War ; Headquarters Department of the Army Washington, DC, 1995

[5] http://harris.com/view_pressrelease.asp?act=lookup&pr_id=2961, (2013. 12. 10.)

[6] Dr Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23.

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Török Szilárd
torok.szilard@gmail.com

SZEMÜVEGGEL A BIZTONSÁGÉRT

Absztrakt

A gyors technológiai fejlődéssel együtt biztonsági kérdésekkel is szembesülnek az állampolgárok, cégek és kormányok. A magunknál tartott információk és adatok (dokumentumok, fényképek, levelezés, stb.) jelentős mennyisége önmagában hordozza a biztonsági kockázatokat, a visszaélés lehetőségét. Google kifejlesztett egy speciális szemüveget, amelynek célja a mobilitás, a kommunikáció és vizuális kijelzés új felhasználási területének megalkotása - önálló piac és hozzá tartózó igények megteremtésével. Jelen tanulmány a Google szemüveg biztonsági felhasználási lehetőségeit és kockázatait kutatja.

Together with the rapid technological advances citizens, corporations and governments faced with IT security. The usually carried information and data (documents, pictures, emails, etc.) itself has a lot of risks and possibility of abuse. Google has developed a special glasses based aims mobility, communication and augmented reality to create a new market with its own demands. In this publication security domains and risks of Google Glass will be explored.

Kulcsszavak: *Google szemüveg, Adatszivárgást megelőző rendszer vagy Adatszivárgás elleni védelem, kiterjesztett valóság (Augmented Reality), ellenőrzés, biztonsági ellenőrzés ~ Google Glass, Data Leak Prevention or Data Leak Protection (DLP), Augmented Reality, monitoring, security audit*

BEVEZETÉS

A technológiai fejlődéssel együtt mindannyian szembesülünk biztonsági kérdésekkel, legyen állampolgárokról, piaci működésről vagy éppen a közigazgatás területeiről szó. Sokféle adatot és információt tartunk magunknál, amelyek már mennyiségükből adódóan is jelentős biztonsági kockázatot hordoznak - növelve a visszaélés lehetőségét, a lehetséges veszteség nagyságát. Senki nem állíthatja meg a fejlődést biztonsági okokra hivatkozva, de a kontrollt, az adatvédelmet és az adatbiztonságot feladatkörök, jogosultsági szintek és folyamatok alapján szükséges kontrollálni.

2012 nagy újdonsága a Google által bejelentett Google Glass (továbbiakban rövidítve GG) [1]: kijelzőre vetített kép megvalósítása mellett GPS vevő, mikrofonnal és kamerával lett kiegészítve, kommunikációs oldalról pedig Wi-Fi és Bluetooth kapcsolattal rendelkezik a szemüveg. A felhasználási területeinek köre már most elképzelhetetlen sok lehetőséget és ötletet hozott ki a fejlesztők és a felhasználók táborából.

Magyarországon az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) [2], valamint a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat [3] rendelkezik az ország kibervédelmi szervezeti struktúrájáról, a felhasználandó ellenőrzési eljárásrend ugyanakkor tervezés alatt van.

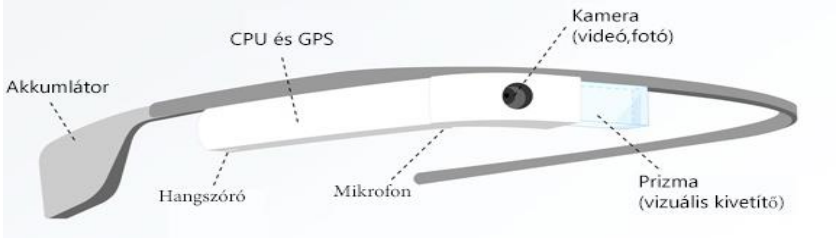
A tanulmány bemutatja magát a Google szemüveget, a biztonsági felhasználási lehetőségeit és kockázatait, amelyek összefüggésben lehetnek az új hazai szabályozási környezettel, akár technológiailag támogatva a bennük szereplő ellenőrzési és IT biztonsági folyamatokat.

GOOGLE GLASS BEMUTATÁSA

A lehetőségek felkutatásához először érdemes részletesen megismerni a már világ szinten bemutatott szemüveg paramétereit.

Google Glass műszaki paraméterei

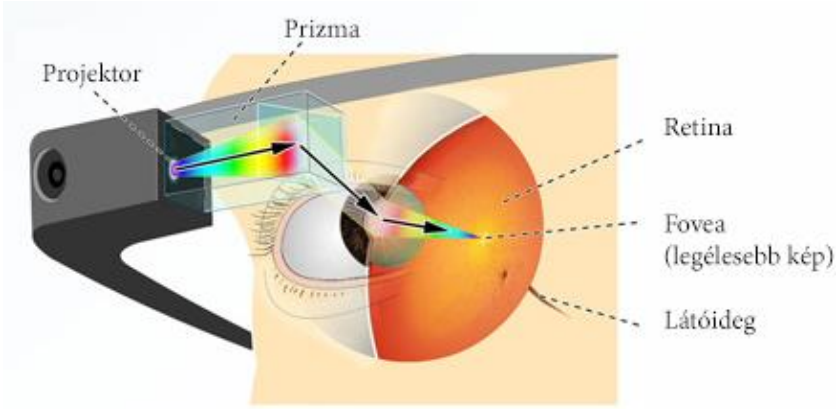
- A szemüveg kerete igen rugalmas, bármilyen arcformához jól illeszthető
- Kivetítőn látható képernyő megfelel egy 25”-os nagyfelbontású képernyő kb. 2,5 méter távolságból történő nézésével
- 5 Megapixeles kamera, 720p felbontású videó-felvétel készítése
- Vezeték nélküli kommunikációk: Wifi - 802.11b/g és Bluetooth
- 12 GB felhasználói memória, Google Felhő szinkronizálással (összesen 16GB)
- Akku kapacitása gyártó szerint egy teljes nap üzemidő, tipikus használat mellett (természetesen vannak olyan funkciói, amelyek jelentősebb akku terheléssel járnak – pl.GPS, videófelvétel, stb.)
- Micro USB csatlakozó és töltő
- Android 4.03 (Ice Cream Sandwich) OS vagy újabb verzió [4]



1. ábra. Google szemüveg fontosabb
Forrás: www.google.com/glass

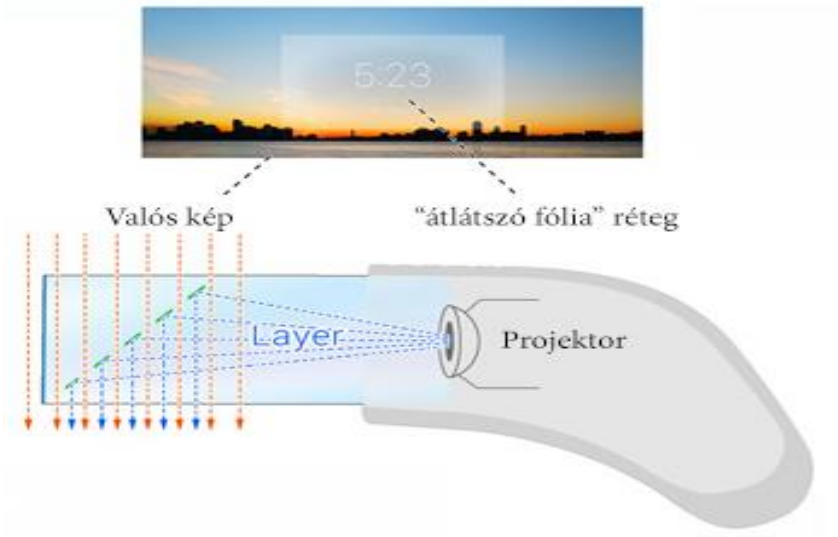
Google Glass kutatási-fejlesztési háttere

„Project Glass” néven ismert kutatás és fejlesztés programban készült el, amelyet azzal a céllal hoztak létre, hogy egy kibővített valóságot megjelenítő, fejre illeszthető kijelzőt alkossanak. Ezt akképpen valósították meg, hogy a szemüveg a rajta elhelyezett prizma segítségével közvetlenül a retinára vetíti a saját maga által alkotott vizuális képet – így az egy átlátszó fóliaréteghez hasonlóan kerül rá a valós képre.



2. ábra. Kivetített köztes vizuális réteg látóidegen történő megjelenítése
Forrás: www.google.com/glass

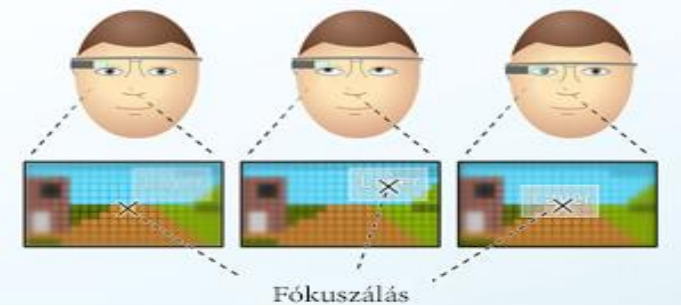
A szemüveg kijelzőjén megjelenő (okostelefon) adatokhoz és ikonokhoz hasonlóan képes megjeleníti a különböző információkat. Irányításának fő tulajdonsága hangvezérlés, azaz egyáltalán nincs szükség kézi irányításra. Android operációs rendszerre mellett a könnyű vezeték-nélküli csatlakozások támogatásával alkották meg a szemüveget a Google X Lab-ben (ugyanitt vezető nélküli autókat is fejlesztenek).



3. ábra. Valós és a szemüveg által készített virtuális réteg működése
Forrás: www.google.com/glass

A fejre illeszthető „kiterjesztett valóságot” mutató kijelzők ötlete bár egyáltalán nem újdonság, a Google szemüvegének kisebb méreteiből adódó jóval kényelmesebb viselés miatt is felkapottabb lett a sajtóban.

A termék mellé egyedi beviteli megoldások is felsorakoznak. Az AR (Augmented Reality – kiterjesztett valóság) rendszerű napszemüveg szemmozgással történő vezérlése túlságosan is megterhelő lehet, míg a puszta kéz felismerése és követése felesleges terhet róna a központi vezérlőegységre.



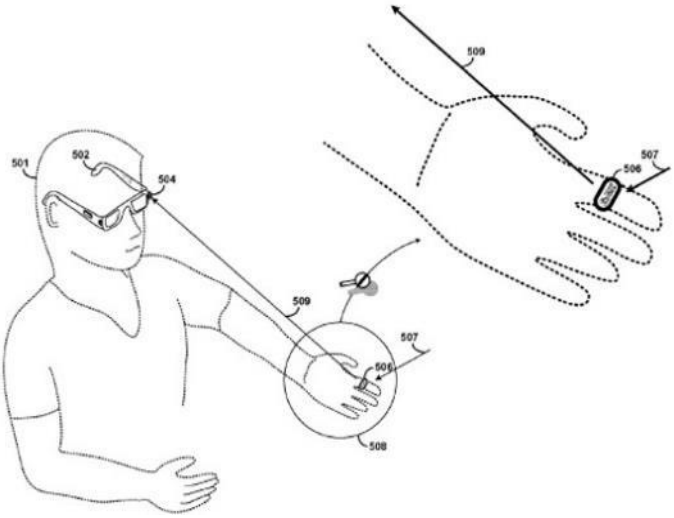
4. ábra. A fókuszálást követi a szemüveg vizuális rétegének kivetítése Forrás: www.google.com/glass

Összefoglalva: tulajdonképpen nincs másról szó, mint egy Google napszemüvegbe oltott telefonról, vagy ha úgy tetszik HUD (Head-up Display – fejmagasságú kijelzőről).

Az eredeti tervekben még a hagyományos szemüvegekre jellemzően a lencséket helyettesítették volna kijelzővel, azonban az újabb formatervezésnek is a technológia fejlődésének köszönhetően lehetővé vált a hétköznapi szemüvegekbe történő integrálása.

Az ipar pozitív visszajelzésekkel fogadta a termék megjelenését, ugyanakkor kritikák és a paródiák keresztttüzébe is került a termék - a lehetséges felhasználási területek és azokkal történő visszaélések miatt. Erre is reagálva a Google kijelentette, hogy nem fogja reklámozásra használni a készüléket. [5]

Google éppen ezért egy infravörös gyűrű bevetésében gondolkodik, amellyel térbeli elmozdulásokat lehet követni és erre alapozott kézmozgás alapú parancsokat definiálni és használni a szemüveggel. [6]



5. ábra. A szemüveg utasítása kéz és az infravörös gyűrű mozgatásával
Forrás: www.theverge.com/2012/5/17/3026571/google-project-glass-infrared-ring-patent

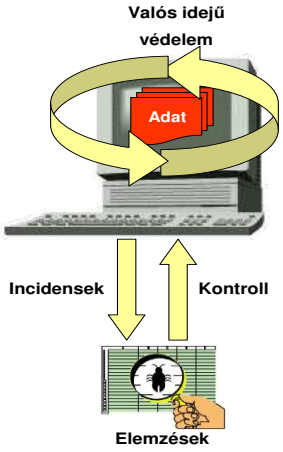
BIZTONSÁGI CÉLÚ FELHASZNÁLÁSI TERÜLETEK

Ebben a fejezetben kerül ismertetésre a Google Glass technológiára alapozott biztonsági vonatkozású lehetőségek és ötletek bemutatása – például az ismert adatbiztonsági és IT biztonsági területeken felhasznált rendszerek és megoldásokkal való összekapcsolásával.

Jelen tanulmányban szereplő kutatás célja, hogy az ismertetett GG alapú megoldás milyen módon tudja hasznosan kiegészíteni az ismert biztonsági és informatikai biztonsági feladatok elvégzését, szabályzások betartatását, továbbá milyen új lehetőségeket biztosíthat ezen a területeken dolgozó, például ellenőrzést végző szakembereknek. (Az ismertetésre került ötletek, megoldások bizonyos esetekben egymásra is épülnek)

Adatszivárgás elleni megoldások (DLP)

Az adatszivárgás elleni megoldások végponti és hálózati oldalon próbálják követni, elemezni vagy akár blokkolni az informatika által kezelt adatokat, azaz az IT biztonsági és adatbiztonsági szabályok betartását kontrollálni.



6. ábra. DLP megoldások magas szintű működése

DLP megoldások fontosabb jellemzői:

- Az információ keletkezésének forrásánál és mozgásánál szükséges jelen lenni. jelen: Kliens oldali és hálózati aktivitások monitorozásával (fájl mozgatása, másolása például hálózati meghajtóról lokálisan használt adattárolóra) egy-egy káreseményhez vezető tevékenységlánc kiinduló fázisában dönt – szabályrendszer alapján – a kockázat szintjéről, és a beavatkozás szükségességéről, ezáltal megelőzheti az adatbiztonságot sértő események bekövetkezését.
- IT biztonságpolitika betartatásának hatékony eszköze. A rendszer a felhasználó igényeinek megfelelően kell paraméterezhető legyen – a paraméterezés feladata a szervezet biztonságpolitikájának leképezése szabályokká, kontrolokká, melyek automatizmusok segítségével, minimális humán interakcióval gondoskodnak a szabályok betartatásáról.
- Nagy felhasználószámú hálózatok központi kontrollja: teljes értékű működési automatizmusok, prevenciók készíthetők, gyakorlatilag az adatvédelmi szabályzatot komplex mondatokba, „ha ez és ez történik, akkor tedd ezt és ezt” típusú elemi relációkba legyenek szervezhetőek. A riasztási, a távoli beavatkozási, és a megelőzési automatizmusok révén minimális személyi felügyelet szükséges akár nagy felhasználószámú rendszerek állandó kontrolljához.

A szervezet igényeinek megfelelően a felhasználói aktivitások mélyreható, illetve teljes naplózására kerül sor. A file- és alkalmazás műveletek, a billentyűzet használat, a ki és belépés idejének rögzítése lehetőséget biztosít számos hasznos elemzésre, lekérdezésekkel, üzleti intelligencia eszközökkel, illetve adatbányászati eljárásokkal magas szinten szintetizált információ nyerhető ki.

Google szemüveg - mint a DLP része

Hatékony segítsége lehet egy IT biztonsági vezetőnek vagy a területen dolgozó ellenőrzést végrehajtó IT biztonsági munkatárs számára egy Google szemüveg típusú megoldás.

Automatikus QR olvasó szoftvert szükséges telepíteni a szemüvegre, majd a felhasználási területen, például a szobák feliratozása mellet érdemes QR kódokkal ellátni. Ennek segítségével nem szükséges az akkut jelentősen terhelő GPS vevő használta, a szemüveg a folyósón, szobák táblái mellett elhelyezett kódokkal azonosítja az ellenőr épületben történő mozgását.

Hang vagy kézmozgás alapú utasításokkal lehetősége van az ellenőrzést végrehajtónak lekérdezni egy adott szobában elhelyezett felhasználók fotóit, a használt számítógépek és ismert, legálisan használható adathordózók típusát vagy akár fotóit egyaránt.

Gyakorlatilag egy igen gyors személyi és adatszivárgással kapcsolatos ellenőrzést lehet végrehajtani a szemüveget viselőnek: azonnal detektálhatja azon személyeket, akik nem a saját számítógépükkel dolgoznak, vagy az engedély nélküli adathordozó használatát.

Belső ellenőrzés IT támogatása

A megoldás informatikai alapú támogatást képes biztosítani egy szervezet belső ellenőrzését végző munkatársainak: az ellenőrzés folyamatát, státuszát, konkrét ellenőrzési listák elvégzését, vagy akár gyors videó konferencián történő egyeztetéseket képes az eszköz megjeleníteni, lebonyolítani.

A háttér informatikai rendszerekkel történő támogatás kiterjedhet a nyilvántartások online szintű ellenőrzésére, gyors-felmérések és azok visszaellenőrzésére is alkalmassá tehető.

Munkahatékonyság elemzés

Személyi ellenőrzéseken belül a hatékonyság ellenőrzése is lehetségessé válik a szemüveg használatával: azonosítható adott munkaterületen a személyek mozgása, számítógépes aktivitása, háttérben akár létszámellenőrzést is végezve.

A hatékonyság ellenőrzés kiterjedhet a munkafolyamatok (QR kódokkal azonosítva), munka időszakok (túlóra, késés, szünetek, stb.) területére is.

Vezeték nélküli hálózati ellenőrzések

A szemüvegbe beépített WiFi vevő segítségével könnyen, akár más folyamat végzése mellett automatikusan elvégezhető a vezeték nélküli hálózatok jelenléte, illegális használata (pl. munkahelyen: saját gépen, telefonon futtatva, zárt intézmény területére benyúló külső/kockázatos Wifi hálózatok kimutatása, stb.) A felmérés folyamatát, hatékonyságának növelését szintén pl. QR kódok elhelyezésével lehet támogatni.

Vezeték nélküli hálózati gyorsellenőrzés

Etikus hackerek munkája során – tipikusan az IT biztonsági sérülékenység vizsgálatoknál - jellemző igény nagyobb intézmények, szervezetek üzemeltetésének vonatkozásában a vezeték nélküli hálózatok feltérképezése: hozzáféréseik ellenőrzése, kvázi WiFi térkép összeállítása irodák, helységek, stb. vonatkozásában, lefedettség és felderíthetőség tulajdonságai, stb.

GG megoldás ilyen irányú felhasználásával a szemüveg beépített WiFi rendszere szkennerként történő alkalmazásával, az etikus hacker vagy az auditor gyorsan és kényelmesen elvégezheti a felmérést, eredményét rögtön képes kielemezni, akár módosítani a felmérés folyamatát, stratégiáját.

Alkalmazás audit

Szervezeteknél használt szoftveres megoldásokra jellemző az egyedi kialakítás, de webes és más keretrendszerek esetén egyedi design elemek (akár logók is) alkalmasak a vizuális beazonosításukra.

Ellenőrzés végzése során ismeretlen alkalmazás futtatását is lehetséges lehet a szemüveggel detektálni (kézjelzést követően központi képfeldolgozó rendszer összeveti a nyilvántartásban levő megoldások fontosabb képi elemeivel), vagy akár az ismeretlen szoftver futtatásának tényét rögzíteni. A megoldást a pontosság és hatékonyság elérése érdekében érdemes lehet QR kód alapú szoba és/vagy személy azonosítással összekapcsolni.

Igazságügyi szakértők támogatása

Informatikai igazságügyi szakértők mindennapos munkája során jellemzően hardvereket azonosítanak, a rajtuk tárolt adatokat és a futtatott környezetet vizsgálják meg, és az ügyfél vagy bírósági folyamatok alapján vizsgálati jelentést készítenek róla.

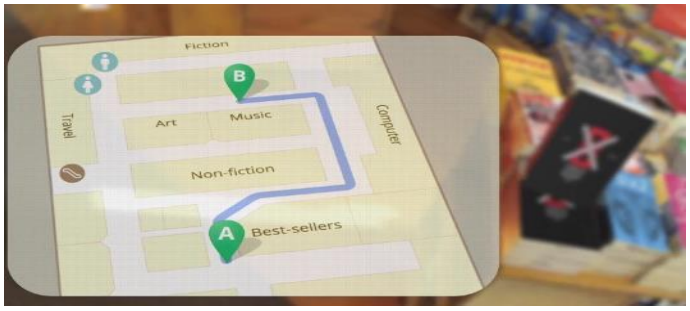
Informatikai vagy általános biztonsági események kapcsán a szemüvegbe épített kamera és videó alkalmas lehet (pl. megfelelő időbélyeg használata mellett) az ilyen típusú vizsgálati feladatok támogatására: adott megállapításokat képekkel, audio és videó felvétellel kiegészítve lehet rögzíteni, dokumentálni. A megoldás kiterjeszthető a rendvédelmi szervek nyomozásainak alátámasztására, támogatására, de akár annak utólagos ellenőrzésére is.

Leltározás

Vonalkódok vagy QR kódok használata mellett egy az általános leltározási folyamatnál jóval gyorsabb és hatékonyabb leltározás alakítható ki, ahol mind a leltározást végző és az abban közreműködő, vagy ellenőrző személy (pl. átadás-átvétel esetén az átvevői oldal képviselője) a HUD képernyőn a belső nyilvántartások adatait láthatja a kódok alapján, lekérdezéseket és saját kimutatásokat, összesítéseket is felvehet a leltározás közben a HUD képernyőjére. Megfelelő informatikai háttértámogatással a leltározás tulajdonképpen valós időben elvégezhetővé válhat.

Nyomozati szerep

Nyomozási folyamatok a GG rendszer használatával nagyobb támogatás biztosítható, hiszen adott helyszínen, a felismert eszköz (vonalkód, QR kód) alapján gyorsított keresések, kimutatások és navigáció jeleníthetőek meg a HUD kijelzőn. [7]



7. ábra. Tájékozódás épületen belül (Forrás: www.pcmag.com)

Lehetőség nyílik az online egyeztetésekre, akár operatív folyamatok irányítási és döntési támogatásainak kivitelezésére is.

Nyomozás során speciális kéz vagy hang alapú utasításokkal további utasítások adhatók ki a virtuális jegyzőkönyv számára, vagy későbbi feldolgozást végzők részére, illetve prompt hang és videó rögzítési funkciók is elérhetővé válhatnak.

Általános azonosítási eljárások támogatása vizuális és hang alapon

GG technológia felhasználásával és online kapcsolattal - például felhőbe feltöltött kép vagy hang alapján - lehetőség van személyek azonosítására, akár hang és arc mozgás kielemzésének felhőbe történő felküldésével és ott történő elemzésével hazugságvizsgálat és egyéb vizsgálatot támogató elemzés lefuttatására is.

Több lépcsős azonosítása és jogosultság kezelés támogatása

A szemüveg által látott például online grafikus jel, kód (pl. QR kód) és hangbevitel használatával (pl. a HUD kijelzőre tett felolvasandó szavak) együttesével igen összetett azonosítások alakíthatóak ki.

Az online informatikai rendszerkapcsolat meglétéből eredően többféle típusú kódok (szobák QR kódja, illetve egy fali kijelzőn online megjelenő QR kód) összevetése mellett további

relációk is megállapíthatóak. Például adott személy azonosítása a biztonsági kamera arc azonosításával, a HUD-on megjelenő kód vagy PIN begépelésével vagy bemondásával, szoba QR kódjának és a munkavégzést elkezdő engedélyének összevetése, vagy akár adott alkalmazás futtatása közben történő összetett jogosultság ellenőrzés végrehajtására is alkalmassá tehető egy GG-vel kiegészített informatikai rendszer.

Rejtett és bizalmas kommunikációk

Saját kézalapú kommunikációk felvételével, egyedi jelek definiálásával mások előtt rejtett jelek, üzenetek adhatók át más személy részére. Ez lehet például egy tárgyalás vagy felmérés során adott jelzés, ami a bizalmas kommunikációban résztvevő számára jelzést vagy információ lekérdezést is adhat a többiek részére.

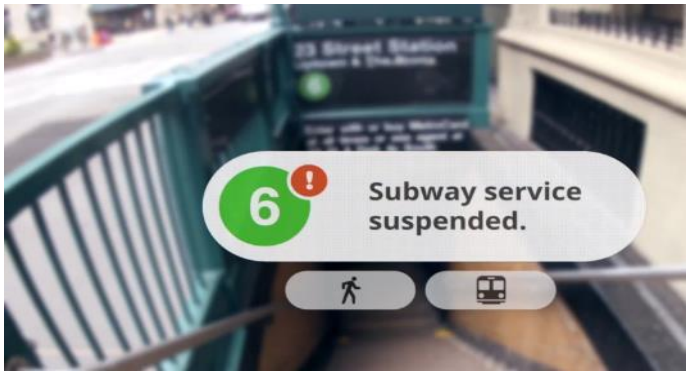
8. ábra: Videó konferencia lehetőségei a szemüveggel
Forrás: The Verge, www.theverge.com

Videó konferenciában levő személyek a szemüveg használatával meg tudják őrizni a másik fél inkognitóját, illetve a kéz és szemmozgás alapú utasításokkal bizalmas jelzéseket is tehet a részt vevők számára.

Riasztások kezelése

GG viselése esetén olyan alkalommal is megkaphatja felelős beosztásban levő személy egy rendszer riasztásait, amikor sem telefon, sem más kommunikációs csatornán nem érhető éppen el (életszerűen azonban WiFi elérés adott), valamint a felhasználó jelzéseivel akár részletesebb információkat is le tud kérni az eseménnyel kapcsolatosan, speciális folyamatok és kommunikációk elindítására is lehetőség biztosít az eszköz.

Lehetőség van távfelügyeleti rendszerbe ügyfélként, vagy felügyelet irányító biztonsági személyként belépni, konkrét vizuális információkat lekérdezni, azokra visszajelzéseket megfogalmazni, akár utasításokat kiadni a rendszer számára (pl. rendőrség értesítése, stb.)



9. ábra: Közlekedési irányítás és információ biztosítás
Forrás: www.pcmag.com

Nagy értékű szállítmányok biztosítása során a vagyonőr által viselt rendszer folyamatosan rögzítheti vagy akár továbbíthatja a képi felvételeket a bevetési irányítási központba.

Állampolgári bejelentések (intelligens 112)

GG hétköznapi használata lehetőséget biztosíthat rendvédelmi szervek, önkormányzatok felé történő jelzések, felvételek, bejelentések küldésére. Felvétel készíthető utcai balesetről vagy bűncselekményről – a telefon elővételének és kezünk lefoglaltságából eredő értékes másodperceket nyerve.

Önkormányzatoknál a helyi ügyek intézése, események bejelentése is lehetséges lenne. Budapesten jelenleg is vannak olyan kerületek, ahol kátyú, de akár hajléktalan és illegális hulladék bejelentés web-es formában létezik. GG-vel a bejelentés, de akár az arról kapott hivatali válasz megjelenítése is hatékony kommunikációt és ügyvitelt eredményezhet, a szemüveg folyamatos használata maga nagyobb bejelentési mennyiséget és hatékonyságot biztosíthat.

Élelmiszerbiztonság

Google Glass használata mindennapok biztonságát is növelheti élelmiszerekre vonatkozó és bolti hálózatbeli információk közvetítésével és elemzésével.

Adott élelmiszert felismerve (embléma, vonalkód, stb.) alapján tájékoztatást adhat étel allergiával kapcsolatban (pl. felhasználó által előre megadott listával történő összevetéssel), akár az adott vagy más bolthálózat által interneten közzétett árlisták alapján alternatívákat, sőt, kedvezőbb árakra is felhívhatja a figyelmet.

Fogyatékkal élők biztonsága

Lévén a szemüveg szárába a speciális hangkeltő a koponyacsontra támaszkodik, így a hangrezgéseket a középfül (légvezetés) megkerülésével tudja közvetíteni a belső fülbe. Ez azon túl, hogy nem korlátozza a környezeti hangok beáramlását, alkalmas lehet halláskárosodott emberek számára is további információs és biztonsági szolgáltatások nyújtására.

10. ábra. Valós idejű szövegfordítás az eredeti szöveg helyére illesztve
Forrás:Word Lens – www.wikipedia.org

Kiemelendő a képelemzéssel történő információk felhasználók részére történő közvetítésének lehetősége:

- pl. látáskárosult részére közlekedési és útviszony információk bemondása (akár lefordítása), amely közlekedési táblára vagy épp lépcsőre, kátyúra, hívhatja fel a figyelmet,
- élelmiszer felismerése és hangalapú ismertetése (látás és halláskárosult szempontjából is hasznos lehet az információ és a jelzés)
- személyek felismerése, vagy egyéb adatok (RFID, WiFi) alapján történő szociális információk továbbítása (kiterjedve a közelben levő ismerősről történő jelzésre, például segítségkérés okán)

FELHASZNÁLÁSI TERÜLETEK KOCKÁZATAI, VISSZAÉLÉSI LEHETŐSÉGEK

A kéretlen reklámokon túl, a Google magánszféra megsértésének, kvázi elleni induló hadviselésének tartják a Google szemüveg használatát, valamint a szemüveg információinak (kéretlenül végzett) begyűjtését együttesen.

Ezen félelmek jogosan kerültek felszínre, hiszen nem ismert, hogy maga a Google (mint marketing irányultságú szolgáltató), mire fogja felhasználni a szemüveg felhasználóinak adatait. [8] Ilyen például a földrajzi helyzet, a felvételek információ mellett további keresési és egyéb felhasználási területek információival történő összevetéséből adódó marketing adatokat is jelenthet, akár a különleges személyes adatokat is érinthet (tényleges politikai és világnézeti meggyőződés). [9]

A GG-re vonatkozó tilalmak, helyi szabályok is megjelentek, ami inkább a felhasználás formájára és területére is vonatkozik. Erre legjobb példa, hogy Kaliforniában megbüntetek egy hölgyet 2013 októberében, mert vezetés közben Google Glass-t viselt – egész pontosan mivel a vezető számára látható monitort viselt, amit az ottani közlekedési szabályok tiltanak. [10]

Valószínű az újabb és újabb biztonsági és egyéb kockázatok sora mind az új felhasználási területekből fognak adódni.

Ilyen például:

- bionikus retinaként jelent meg egy cég terméke, amely egy mesterséges retina funkcióit ellátva képi információkat képes továbbítani a látóidegeken keresztül az agy emberi számára. [11]
- Lehetséges kockázat: agyba bejutó képek megváltoztatása.
- Fordító program jelent meg a GG szemüvegre, amely grafikusan be is helyettesíti az idegen nyelvű szöveg helyére a lehetséges fordítást. [12]
- Azonnal adódik a hibás vagy félreérhető fordításokból eredő problémák sora, ami akár a szándékosan megváltoztatott információival történő visszaéléséig is elvezethet.
- Orvosi konzultációkra történő kísérletezések folynak külföldi egészségügyi intézményekben, amely során egy specialista orvos távolról tanácsot adhat, akár irányíthat műtétet (szóbeli utasításokkal) – interaktívan részt is vesz benne, pl. audio/vizuális közvetítés mellett. [13]
- Kockázat lehet a kommunikáció lehallgatása, egészségügyi információk szivárgása, extrém esetben szándékosan negatívan befolyásolt orvosi beavatkozással végzetes károsodás okozása a betegnek.

Elveszett GG (akár Android telefon) esetére a Google a „remote location”, azaz távolról történő helymeghatározás funkció használatát említi meg a Google Glass saját weboldalán. Lehetséges kockázatai a funkcióból rögtön eredő illegális helymeghatározás, üzenet küldés, akár a telefonon tárolt adatok teljes törlése lehet. [14]

Ugyancsak a GG Android operációs (4.04-es verzióra épülő) rendszeréből ered az a kockázat, hogy a letölthető applikációk ellenőrzésének hiányában a szemüveg tulajdonképpen bármilyen, a szemüveg képességeivel való visszaélésre használható lehet. Lehetséges kockázatok: legmagasabb szintű (root) hozzáférést követően bármilyen, a szemüveg által kezelt, lekért és elemzett adat kiszivárogtatható, akár az adatok feldolgozása alatt megváltoztathatóak, visszaélések kivitelezése a felhasználó tudta nélkül.

Symantech már beszámolt egy komoly IT biztonsági problémáról is: GG által beolvasott QR kód segítségével átkonfigurálható a WiFi beállítás, és így észrevétlenül átirányítódhat az internetes forgalma egy a támadó által lehallgatott, befolyásolt hálózat felé. [15]

A termékben rejlő végtelennek tűnő lehetőségek közül kiemelendő egy amerikai termék (Mutualink), amely segítségével valós időbeli multimédia kapcsolat segítségével hatékonyabbá tehető a közszféra biztonsági szakterületeinek munkája. Fontosabb példák a felhasználás területeire:

- tűzoltók az oltás megkezdése előtt láthatják az érintett terület, épület tervrajzát, leírásait, akár a tűzvédelmi leírásokat,
- Mentők a helyszínre érkezésig bezárólag információt kaphatnak az ellátásra szoruló személyek egészségügyi nyilvántartásaiból (vércsoport, gyógyszerallergia, nyilvántartott betegségek, stb.),
- Katasztrófavédelmi egységek a tájékozódásra, a helyismeret beszerzésére, de akár a műveletek irányításával kapcsolatos információk és utasítások továbbítására is használhatják. [16]

Természetesen a felsorolt felhasználási területek során kezelt információk kiszivárgása és befolyásolása (módosítása) igen jelentős kockázatot hordoz magában.

Egyesült Államokban adatvédelmi és adatkezelési kérdések merültek fel a szemüveg közterületen történő használata (pl. kávézóban videó felvétel készítése) kapcsán. Google Street View (3 dimenziós, térképhez kapcsolt multimédiás adatbázis) több problémát felvetett már, de azokat mindennapi szintű kiterjesztéseként vélik megjelenni a GG közterületi használata esetén – feltehetően a legtöbben nem kérnének engedélyt a szemüveg audio és videó felvételkészítése esetén az érintettektől, és nem is látszik a felvétel készítése (míg telefon és kamera esetén relatív egyértelmű milyen irányban készül a felvétel). [17]

A szemüveggel történő illetlen, modortalan felhasználásra vonatkozóan már külön angol elnevezés is elterjedt: „Glasshole”. Legismertebb, általánosan már elterjedt illetlen GG felhasználási területek:

- mosdó,
- kaszinó,
- udvarlási helyzetek,
- társasági beszélgetésben az online letölthető információkkal felvágni,
- pénzügyek intézése (pl. ATM)

GG típusú technológiák egyre szélesebb körű elterjedése átírhatja az eddigi munkahelyi előírásokat, és újabb személyiségi jogi kérdéseket vet fel. Az új eszközök a viselhető eszközök elterjedése a munkavállalói szerződések és a titoktartási szabályok felülvizsgálatára késztetheti a cégeket.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) megalakulása óta az internet és az új információs technológiák jelentette adatvédelmi kihívásokat is figyelemmel kísérik. Google prezentációt követően a NAIH elnökhelyettese a szemüveg valamennyi funkcióját kipróbálta. NAIH munkatársainak elsődleges érdeklődése az adatvédelmi aggályokra irányult, hiszen a szemüveg titkos megfigyelésekre is alkalmas lehet. [18]

Terjedőben van azon elvárás, hogy a szemüveg kifelé is adjon jelzést arról, hogy pl. videó felvételt rögzít a környezetéről – bár az interneten terjedő hackerek munkája alapján várhatóan ez is könnyen kikapcsolható utólagosan.

Ugyancsak megfogalmazódhat az összegyűjtött személyes adatok tárolása és felhasználása miatti aggály, azaz nem ismeret a sorsuk.

ÖSSZEGZÉS

A tanulmányon keresztül ismertetésre került a Google Glass megoldása, amelyet az újabb és újabb Google fejlesztési bejelentések érdemben nem befolyásolnak, legfeljebb a lehetőségeket listáját bővíthetik.

Az ismertetés kiterjedt a biztonsági és informatikai biztonsági irányú támogatások lehetséges köreire, a benne rejlő aktuális biztonsági célú felhasználású lehetőségek rövid tárházára. Áttekintésre kerültek az ismert adatvédelmi és IT biztonsági kockázatok, a felhasználási területekből adódó további problémák is.

Könnyedén belátható, hogy egy ilyen típusú eszköz (azaz beleértve a Google minden konkurenciáját is), az online számítógép rendszerek és teljesítményeinek összekötésével végtelen biztonságot támogató lehetőséget rejt magában, és pont ebből adódóan az informatikai kockázatok teljesen új dimenziói is megnyíltak.

A röviden ismertetésre került 16 biztonsági és ellenőrzési vonatkozású felhasználási és fejlesztési lehetőség messze nem fedi le az ilyen típusú technológiában rejlő perspektívákat.

Ugyanakkor a bemutatott példák alkalmasak arra, hogy miként jelenhet meg egy új technológia például az IT biztonság modern eszközeként a szervezetek szabályozásainak betartatásaként, ellenőrzési folyamatok, kommunikációk és irányítások támogatásaként, de akár a magánszféra néhány felhasználási területe is izgalmas kihívásokat biztosít a következő évekre.

Felhasznált irodalom

[1] Wikipedia, (2013. november 11.) *Google Glass*. letöltés dátuma: 2013. november 13., forrás: Wikipedia – The Free Encyclopedia: http://en.wikipedia.org/w/index.php?title=Google_Glass&oldid=581136709

[2] Magyar Kormány: A Kormány 1139/2013. (III.21.) határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Magyar Közlöny, 47. (2013) 6338.

[3] Magyar Kormány: „Az állami és önkormányzati szervek elektronikus információbiztonságáról” szóló törvény, 2013. április 25., 2013/69. 50241.

[4] Google, (2013. november 13.) *Google Glass Tech Spec*. letöltés dátuma: 2013. november 13., forrás: Google Support – Glass: https://support.google.com/glass/answer/3064128?hl=en&ref_topic=3063354

[5] Wikipedia, (2013. december 12.) *Google Glass*. letöltés dátuma: 2013. november 13., forrás: Wikipédia – A szabad enciklopédia: http://hu.wikipedia.org/w/index.php?title=Google_Glass&oldid=13784682

[6] Adi Robertson, (2012. május 17.) *Google Project Glass patent shows control system using infrared rings and fingernails*. letöltés dátuma: 2013. november 13., forrás: The Verge: http://www.theverge.com/2012/5/17/3026571/google-project-glass-infrared-ring-patent

[7] YouTube - Google, (2012. április 4.) *Project Glass: One Day*. letöltés dátuma: 2013. november 12., forrás: YouTube: http://www.youtube.com/watch?v=9c6W4CCU9M4

[8] David Streitfeld, (2012. március 12.) *Google Concedes That Drive-By Prying Violated Privacy,* letöltés dátuma: 2013. december 12., forrás: The New York Times: http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html?pagewanted=all&_r=3&

[9] Milo Ziannopoulos, (2012. április 2.) *Google Glass and Surveillance Culture,* letöltés dátuma: 2013. december 12., forrás: Slashdot: http://slashdot.org/topic/cloud/google-glass-and-surveillance-culture/

[10] Sky News, (2013. október 30.) *Google Glass Driver Gets Ticket From Police,* letöltés dátuma: 2013. december 12., forrás: Sky News: http://news.sky.com/story/1161741/google-glass-driver-gets-ticket-from-police

[11] Second Sight:*The Argus II Retinal Prosthesis System,* letöltés dátuma: 2013. december 12., forrás: http://2-sight.eu/en/argus-ii-rps-pr-en

[12] Kevin Kelleher, (2010. december 19.) *World Lens + Google Goggles = A useful augmented reality app,* letöltés dátuma: 2013. december 12., forrás: Reuters: http://blogs.reuters.com/mediafile/2010/12/19/word-lens-google-goggles-a-useful-augmented-reality-app/

[13] John Nosta, (2013. június 27.) *How Google Glass Is Changing Medical Education,* letöltés dátuma: 2013. december 12., forrás: Forbes: http://www.forbes.com/sites/johnnosta/2013/06/27/google-glass-teach-me-medicine-how-glass-is-helping-change-medical-education/

[14] Google, (2013. december 12.) *Google Glass Tech Spec*. letöltés dátuma: 2013. december 13., forrás: Google Glass FAQ: https://sites.google.com/site/glasscomms/faqs

[15] Candid Wueest, (2013. július 18.) *Google Glass Still Vulnerable to WIFI Hijacking Despite QR Photobombing Patch*. letöltés dátuma: 2013. december 13., forrás: Symantec: http://www.symantec.com/connect/blogs/google-glass-still-vulnerable-wifi-hijacking-despite-qr-photobombing-patch

[16] Mutualing, (2013. augusztus 19.) *Mutualing Unveils Google Glass for Public Safety,* letöltés dátuma: 2013. december 13., forrás: BusinessWire: http://www.businesswire.com/news/home/20130819005155/en/Mutualink-Unveils-Google-Glass-Public-Safety

[17] Claire Cain Miller, (2013. június 19.) *Privacy Officials Worldwide Press Google About Glass,* letöltés dátuma: 2013. december 13., forrás: The New York Times Technology Blog: http://bits.blogs.nytimes.com/2013/06/19/privacy-officials-worldwide-press-google-about-glass/

[18] Nemzeti Adatvédelmi és Információszabadság Hatóság, (2013. szeptember 11.) *NAIH munkatársai elsők között próbálták ki a Google Glass-t,* letöltés dátuma: 2013. december 13., forrás: NAIH weboldal: http://www.naih.hu/files/GoogleGlass_koezlemeny_2013_09_11.pdf

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Gáspár Szabolcs
szabolcs.gaspar@gmail.com

ELÜLSŐ KERESZTSZALAG SÉRÜLÉS ELŐFORDULÁSA A MAGYAR HONVÉDSÉG ÁLLOMÁNYÁN BELÜL ÉS REKONSTRUKCIÓS TAKTIKÁK A HONVÉDKÓRHÁZBAN

Absztrakt

Az elülső keresztszalag sérülés civil és katonai vonatkozásban egyaránt az egyik leggyakoribb térdízületi sérülés fajta. A Magyar Honvédség állományában előforduló keresztszalag sérültek jelentős része a Honvédkórházban kerül rekonstrukciós ellátásra. A szerző célul tűzte ki, hogy felmérje a Magyar Honvédség Honvédkórházában egy meghatározott időszakban (68 hónap) elülső keresztszalag sérüléssel operált betegállományt, különös tekintettel a Magyar Honvédség katonáira. Vizsgálatait retrospektíven, a rendelkezésre álló egészségügyi adatok alapján végezte. Megvizsgálja, hogy az „akcelerált ellátás" alkalmazásra kerül-e, kihasználva a Honvédkórház adta páratlan diagnosztikus, sebészi és rehabilitációs lehetőségeket, mely katonák esetében elősegíti a gyorsabb és hatékonyabb kezelést és ezáltal a mielőbbi szolgálathoz való visszatérés lehetőségét.

The anterior cruciate ligament (ACL) injury is the most common type among knee injuries both in civil and in military enviroment. Among servicemen suffering ACL injury reconstructions usually performed in the Military Hospital. The author's aims to explore the patient's records operated with ACL reconstruction in Military Hospital of a specified period (68 months) in particular to the Hungarian Defense Forces servicemen. Investigations has been made retrospectively based on the available medical records. The author ivestigates whether the "accelerated procedure" has been applied in the Military Hospital with the possibility of taking advantage of unique diagnostic, surcigal and rehabilitation opportunities offered by the Hospital that promote access to the swift return for military service.

Kulcsszavak: *elülső keresztszalag sérülés, elülső keresztszalag pótlás, Magyar Honvédség állománya, akcelerált ellátás ~ ACL injury, ACL reconstruction, Hungarian Defence Forces servicemen, accelerated procedures*

„A katona biológiai szempontból azon megterhelések idején van a legnagyobb veszélyben, amikor élettani kompenzáló mechanizmusait maximálisan igénybe veszi. Csak úgy felelhet meg a harctéri igénybevétel szélsőségeinek, ha megterhelését teljesítőképességéhez igazítjuk, vagyis parancsnoka elvárásai figyelembe veszik mozgósítható tartalékait is."[1]

BEVEZETŐ

Az elülső keresztszalag szakadása az egyik leggyakoribb elváltozás térdízületi sérülés esetén. Katonai szolgálat közben szerzett elülső keresztszalag sérülések műtéti kezelést igényelnek és az ezt követő több hónapos komplex rehabilitációt. Évente közel 100 elülső keresztszalag pótlást végzünk osztályunkon, melynek hozzávetőleg 20 %-a katona sérült.

A Magyar Honvédségen belül a fizikai alkalmasság-vizsgálat teljesítmény tesztjeinek sikeres végrehajtásához elengedhetetlen az elülső keresztszalag megléte, illetve annak jó funkciója. Az alkalmazott modern műtét technikai eljárások mellett is a képzett katonai állomány minimum ½ éves időszakra alkalmatlanná válik missziós, illetve fokozott fizikai terheléssel járó tevékenység elvégzésére. Nem beszélve arról az időszakról, míg a katona a definitív ellátáshoz jut.

Nemzetközi tanulmányok is bizonyítják, hogy az elülső keresztszalag sérülés nem ritka katonáknál. [2,3] Leggyakrabban sporttevékenység közben szenvednek el ilyen sérülést, mely a későbbiekben jelentősen befolyásolja fizikai teljesítőképességüket és katonai alkalmasságukat. [4] Több tanulmány foglalkozik a katonák akcelerált ellátásának kérdésével és biomarkerek kutatásával, melyek alkalmasak lehetnek előrevetíteni a későbbiekben bekövetkezhető elülső keresztszalag sérülést. [5,6]

Magyarországon eddig nem született olyan tanulmány, mely felmérte volna, hogy a Magyar Honvédségen belül milyen gyakran, milyen okból fordul elő elülső keresztszalag sérülés és a sérültek az ellátást követően milyen arányban képesek visszatérni eredeti beosztásunkba, illetve ellátni korábbi feladataikat. Továbbá nincs egységes szemlélet a műtétet követő rehabilitációban a mielőbbi gyógyulás és katonai készenlét elérése érdekében. A tanulmány készítésével ezen hiányosságok kiküszöbölésére teszek kísérletet. Véleményem szerint rendkívül fontos, hogy a MH Honvédkórháza adta páratlan lehetőségek kihasználásával felgyorsítsuk az elülső keresztszalag sérülést szenvedett katonák ellátását, rehabilitációját. Célszerű lenne létrehozni az „akcelerált ellátás" fogalmát, és ilyen esetekben egy egységes logikai vezérfonal mentén elkészített szakmai algoritmus használata mellett végezni ezen katona sérültek ellátását.

AZ ELÜLSŐ KERESZTSZALAG SÉRÜLÉS

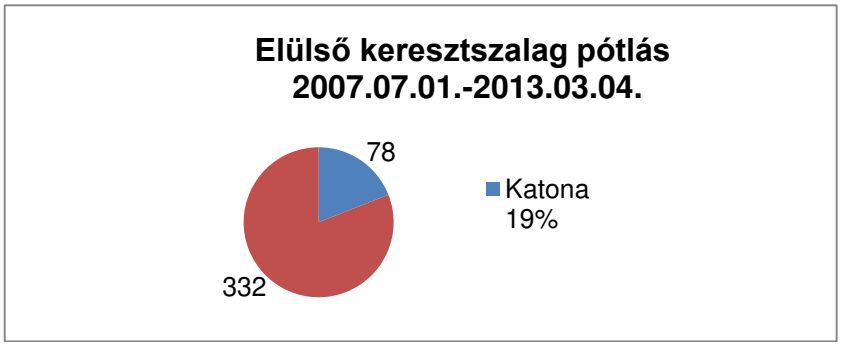
„Az elülső keresztszalag, a ligamentum cruciatum anterius (ACL), szakadása súlyos térdsérülés, melynek következtében a térdízület instabilitása mellett számos egyéb korai és késői következmény is kialakul. Az instabil térdben a sérülést követően megindul az ízületi porcfelszín károsodása, degeneratív elváltozása és emellett a megváltozott ízületi kinematika következtében az egyéb képletek sérülésének a kockázata is megnő. Ezért a műtéti beavatkozás, vagyis az elülső keresztszalag pótlásának a célja nemcsak a térdízület stabilitásának helyreállítása, hanem a degeneratív folyamatok kialakulásának megelőzése és az egyéb társsérülések prevenciója is." [7]

ANYAG ÉS MÓDSZER

Megvizsgáltam a 2007.07.01. és a 2013.03.04. közötti időszakban a Magyar Honvédség Honvédkórház Baleseti Sebészeti Osztályán ellátott elülső keresztszalag sérülést szenvedett és műtétileg kezelt betegeket. Az időpont választása a Honvédkórház Baleseti Sebészeti Osztályán bevezetett, akkoriban az osztály számára új műtéti technikának számító, a comb két hajlító izmának inas részét, úgynevezett hamstring inakat felhasználó beavatkozás bevezetési idejére esik. Ezen műtéti technika előnyeit – amely miatt bevezetése és gyakorlatban történő elsajátítása mellett döntöttünk – a műtéti ellátási lehetőségek részben kívánom részletesen kifejteni.

A vizsgálat retrospektíven, a rendelkezésre álló egészségügyi adatok felhasználásával készült.

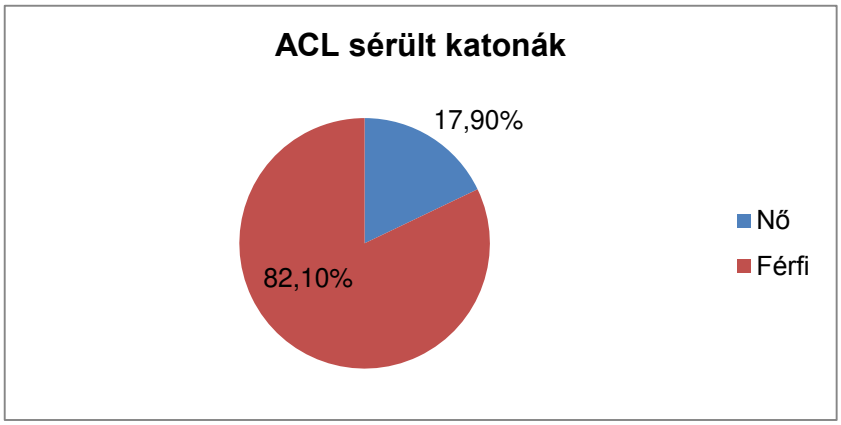
Ezen időszakban 410 elülső keresztszalag pótló műtétet végeztünk. Az ellátásra került betegek közül 78 volt a Magyar Honvédség aktív hivatásos vagy szerződéses katonája. (1. ábra).



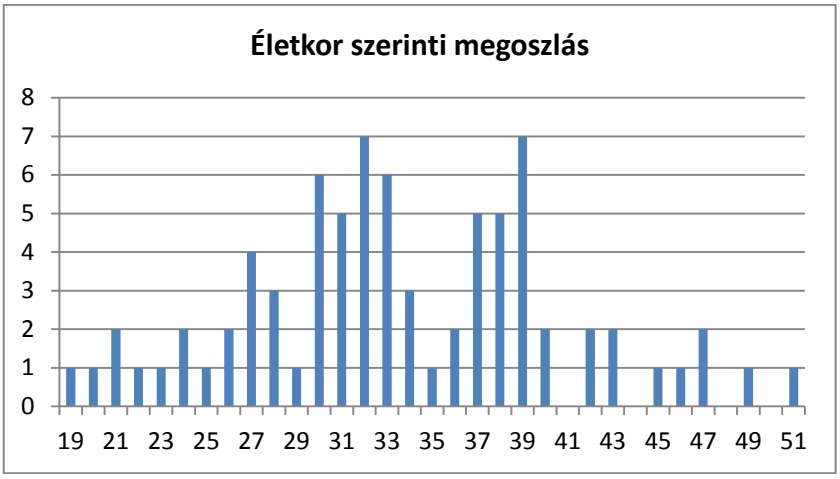
1. ábra. (Forrás: szerző)

Az ábra jól prezentálja, hogy a Honvédkórházban a katona sérültek mellett kiterjedt civil ellátás is folyik, mely elengedhetetlen a szakmai készültség fenntartásában. Évekre lebontva látható, hogy osztályunkon folyamatosan növekszik az elülső keresztszalag pótló műtétek száma, mely a modern ízületi tükröző (arthroscopos) eszközök bevezetése és a biodegradábilis implantátumok elérhetősége valamint az összehangolt agresszív rehabilitációs kezelés elterjedése váltott ki.

A 78 katona sérült 17,9 % nő volt. (2. ábra) Átlag életkoruk 33,6 év volt (19-51 év között). (3. ábra)



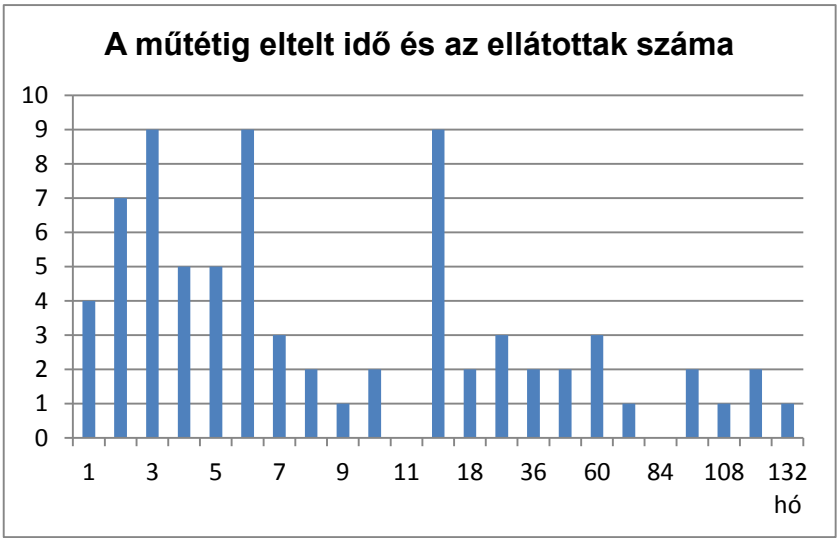
2. ábra. (Forrás: szerző)



3. ábra. (Forrás: szerző)

Jól látható az életkor szerinti görbén, hogy a műtéten átesett betegek túlnyomó többsége a 30-as éveik közepén járó katonákból került ki. A sérültek 62 %-a sportolás közben szenvedte el sérülését, mely megegyezik a nemzetközi szakirodalomban található hasonló adatokkal. [2, 4] Szembetűnő, hogy a sérült katonák 14 %-a missziós szolgálat alatt, vagy magyarországi szolgálatteljesítés közben szenvedte el sérülését. Az elvégzett 410 beavatkozás 94,8 %-a a hamstring inakkal végzett elülső keresztszalag pótlás, míg csupán 5,2 %-a volt a korábban „gold standard"-ként számon tartott csont-ín-csont (BTB) oltvánnyal végzett rekonstrukció. A katona sérültekre vetítve 89,8 % hamstring inas pótlás, míg 10,2 % BTB oltványos pótlás. Ez a szignifikáns különbség az osztály által 2007-ben bevezetett újfajta rögzítési technikának köszönhető, melynek következtében priméren elülső keresztszalag pótlás azóta szinte kizárólag hamstring inakkal végzünk. BTB oltványos és a comb feszítő izomcsoportjának inas végét (úgynevezett quadriceps ín) felhasználó pótlásokat általában revíziós műtétek kapcsán végzünk.

A rendelkezésre álló adatokból 75 katona sérültnél tudtunk a sérüléstől eltelt időre vonatkozóan adatokat nyerni. A sérültek átlagosan a sérülést követő 21,92 hónap múlva (1-132 hó) kerültek ellátásra. (4. ábra)



4. ábra. (Forrás: szerző)

Jól látható, hogy nem történt azonnali műtéti beavatkozás. Korai halasztott műtét (a sérüléstől számított 1-2 hónap) elvégzésére is csak 11 esetben adódott példa. Az átlagos ellátási idő 5,67 hónapra (1-12 hónap) csökken, ha a számításból kihagyjuk az 1 évnél régebben sérülteket, akiket nem lehet akut sérülteknek nevezni.

Álláspontunk szerint, amennyiben azonnali műtéti ellátás nem jön szóba, késői halaszott műtét (a sérüléstől számított 8-12 hét) elvégzését preferáljuk. Ebben az esetben az ízületben kialakult vérömleny már felszívódik és a sérültnek alkalma nyílik műtét előtti, az arra való felkészülést elősegítő gyógytornán való részvételre. Tapasztalataink alapján ezen betegcsoport jelentős részének korai rehabilitációja gyorsabb mint azon társaiké akik hasonló felkészítésen nem vettek részt.

Jelen vizsgálat nem terjedt ki arra, hogy a sérüléstől eltelt idő mennyire befolyásolja a rehabilitációt, illetve a visszatérést a katonai szolgálatba. Az időfaktort, mint a sebészi tapasztalataim alapján igen fontos tényezőt, egy későbbi tanulmányban kívánom pontosan analizálni és feldolgozni.

A betegek a műtétet követően 8 napot töltenek kórházi kezeléssel. Ezen időszak alatt megkezdjük korai rehabilitációs kezelésüket, mely passzív térdmozgató gépes kezelésből és irányított gyógytornából áll. A betegek a műtétet követő 8. nap varratszedés után kerülnek emisszióra 120 nap egészségügyi szabadság javaslattal, melyet a Felülvizsgálati Bizottság (FÜV) hagy jóvá. További rehabilitációs kezelésükre javaslatot kapnak, melyet azonban nem ellenőrzünk. Ezen kezelés a katona belátására, akaratára van bízva. Kontroll vizsgálatra a műtétet követő 6. és 12. héten kerül sor. A fenti gyakorlat nem teszi lehetővé az egységes kezelési algoritmus alkalmazását és a tudományos feldolgozáshoz nélkülözhetetlen hosszú távú után-követést.

MŰTÉTI ELLÁTÁSI LEHETŐSÉGEK

A világon leggyakrabban két metódus szerint végeznek elülső keresztszalag pótlást. A régebben „arany standard”-nak nevezett csont-ín-csont (BTB) oltvánnyal végzett pótlás mellett az úgynevezett hamstring inakkal (HT) végzett pótlás vált gyakorivá. Utóbbi esetben ugyanis az átültetett oltvány ínsejtjeinek (tendocyták) jelentős része élő marad, szemben a BTB plasztikánál, ahol az oltvány nagy részében az ínsejtek elhalnak. [8] Kisebb az adó helyen létrejött morbiditási probléma és a műtétet követő ízületen belüli szálagos összekapaszkodás (arthrofibrózis). Ezen oltvány nagyobb rotációs stabilitást biztosít egy előbbihez képest és a 4 köteges hamstring inas pótlás erősebb, mint a hasonló vastagságú BTB oltvány.

A Honvédkórház Baleseti Sebészetének gyakorlatában a 2007-es évtől kezdve fokozatosan átálltunk a BTB plasztikáról a HT oltványokkal végzett elülső keresztszalag pótlásra. Mindezt annak tükrében vezettük be, hogy a egyre elterjedtebbé vált a világon az agresszív rehabilitációs szemlélet a betegek műtét utáni kezelésében. Ezen szemlétet megvalósításához nélkülözhetetlen a betegek korai mobilizációja és az operált végtag lehetőség szerinti minél korábbi terhelhetősége. A koncepció egybevág osztályunk elveivel, melyek szerint elősegítsük a katona sérültek mielőbbi szolgálatba való visszaállítását és fizikai terhelhetőségét.

A műtét során az oltványokat többféleképpen tudjuk rögzíteni a combcsontban és a sípcsontban. Választásunk olyan, az emberi szervezetben annak enzimei hatására fokozatosan felszívódó, úgynevezett biodegradális anyagokra esett, melyek segítségével a korai terhelést jól toleráló, az oltvány stabilitását biztosító rögzítést vagyunk képesek elérni. Ezen rögzítés alkalmassá teszi a betegek korai agresszív rehabilitációját az oltvány lazulásának veszélye nélkül. Betegeink a 2. műtéti napon, külső rögzítők nélkül, teljes terhelés mellett használhatják operált végtagjaikat. A rögzítés mellett szól, hogy az oltványt a csont ízülethez közeli részéhez (úgynevezett notch közeli részhez) képes rögzíteni, mely csökkenti a későbbiekben előfordulható csatorna szélesedési tünetet, mely az oltvány meglazulásához vezethet. [9]

EREDMÉNYEK

Az elvégzett vizsgálatokkal megállapítottam, hogy a Honvédkórház Baleseti Sebészeti Osztályán elvégzett elülső keresztszalag pótló műtétek 19 %-ban operáltunk a Magyar Honvédség hivatásos vagy szerződéses állományához tartozó katona sérültet. Nemi eloszlásban a katona sérültek 82,1 % volt férfi, illetve a műtét időpontjában az ellátottak átlagéletkora 33,6 év volt, mely adatok korrelálnak a nemzetközi szakirodalomban fellelhető hasonló vizsgálati adatokkal. A sérülést követően átlagosan 21,92 hónappal kerültek ellátásra a betegek. A vizsgálat időszak alatt az elülső keresztszalag sérülést szenvedett katonák 10,2%-nál végeztünk BTB plasztikát, még többségüknél 89,8 %-ban hamstring inakkal pótoltuk szakadt elülső keresztszalagjukat.

Jelen vizsgálattal fényt derítettem arra a jelentős problémára, hogy jelenleg nincs egységes, az kor követelményeinek megfelelő „akcelerált ellátási" módszer a katona sérültek ellátásában. Rehabilitációs kezelésük ajánlások alapján, nem pedig vezetett, evidenciákkal alátámasztott útmutató alapján történik.

ÖSSZEFOGLALÁS

Megállapítottam, hogy a Magyar Honvédség Honvédkórházában ellátott betegek a kor színvonalának messzemenőkig megfelelő műtéti kezelésben részesülnek. A korai agresszív rehabilitációt a műtétet követő napon megkezdjük. A betegek kórházi tartózkodásuk alatt naponta aktív és passzív fizioterápiás kezelésben részesülnek. Azonban nincs egységes konszenzus a betegek ellátásának időpontjában és a kórházból történő emissziót követően.

A klinikai gyakorlat szerint az elülső keresztszalag szakadást szenvedett sérülteket vagy azonnali, vagy halasztott (8-12 héttel a sérülést követően) műtéti ellátásban részesítjük. Katona sérülteknél kifejezetten előnyös és hatékony lenne az azonnali műtéti ellátás és a szervezett, a műtétet követő legalább 6 hétig tartó rehabilitáció. Ezzel időt nyernénk, hiszen az elülső keresztszalag sérült katona képtelen feladata ellátására a definitív műtéti ellátásig, vagy nagymértékben növekszik további sérülések lehetősége, ízületi kopás kialakulása, amennyiben instabil térdét terhelve látja el feladatát. Halasztott ellátás esetén továbbá igen költséges a kivizsgálás időtartamára és a végleges ellátás bekövetkeztéig a katona egészségügyi szabadságon való tartása, esetleges fizikai-, alaki- és terep foglalkozások alóli felmentése.

Véleményem szerint elengedhetetlen ezen betegek egységes logikai vezérfonal mentén történő kezelése. A későbbiekben kívánom kidolgozni a szakmai ellátás egységesített beteg-útjait és a Honvédkórház adta rehabilitációs lehetőségek (Aktív Mozgásszervi Rehabilitációs Osztály MH EK Honvédkórház III. számú telephely, HÉMORI) kihasználását, melyet „akcelerált ellátás" néven kívánok bevezetni.

Felhasznált irodalom

[1] Kóródi Gyula: A digitális katona személyi védelem a honvédorvos szemszögéből Hadmérnök 2006:(Különszám) pp. 1-7. (2006)

[2] Owens BD, Mountcastle SB, Dunn WR, DeBerardino TM, Taylor DC: Incidence of anterior cruciate ligament injury among active duty U.S. military servicemen and servicewomen, Mil Med. 2007 Jan;172 (1):90-1

[3] Tamara D Lauder, Susan P Baker, Gordon S Smith, Andrew E Lincoln: Sports and physical training injury hospitalizations in the Army, Am. J. Prev. Med. 2000, 18:118-28

[4] Tengku Muzaffar Tengku Md Shihabudin, Shahrulazua Ahmad, Musa Kasmin, Masdiamin Mohamad Nor, Muhamad Fuad Daud, Mohammad Amiruddin Hamdan: The Activity Leading to ACL Injury and the ability to Resume Duty following Reconstructive Surgery in Malaysian Military Patients, Med J. Malaysia 2003 Vol 68 No 2:115-18

[5] Howes J, Wood A M, Bell D J, Wrigley S, Angus C: Fast track surgery for anterior cruciate ligament reconstruction in military patients in Scotland Br J Sports Med 2011; 45:A15 doi:10.1136/bjsports-2011-090606.47

[6] Svoboda SJ, Owens BD, Harvey T, et al: The association between serum biomarkers of cartilage turnover and subsequent anterior cruciate ligament rupture. Presented at the American Orthopaedic Society for Sports Medicine Annual Meeting 2012. July 12-15. Baltimore.

[7] Pavlik Attila: Az elülső keresztszalag pótlásánál alkalmazott press-fit rögzítés PhD értekezés 2005, Semmelweis Egyetem Doktori Iskola

[8] Johnson LL: The outcome of a free autogenous semitendinosus tendon graft in human anterior cruciate reconstructive surgery: a histological study. Arthroscopy. 1993;9(2):131-42.

[9] Fauno P, Kaalund S: Tunnel Widening After Hamstring Anterior Cruciate Ligament Reconstruction Is Influenced by the Type of Graft Fixation Used: A Prospective Randomized Study Arthroscopy: The Journal of Arthroscopic & Related Surgery Volume 21, Issue 11, November 2005, Pages 1337–1341

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Hronyecz Erika
hronyecz.erika@uni-nke.hu

AZ EURÓPAI UNIÓ VÉDELMI IPARÁNAK HELYZETE ÉS KIHÍVÁSAI NAPJAINKBAN

Absztrakt

A védelmi ipar jelenlegi helyzetének elemzése és a jövőbeni szerepének jelentősége napjainkban az egyik leggyakrabban tárgyalt témakör az Európai Unióban. A stratégiai fontossággal bíró iparágat érintő – a gazdasági válságból adódó – drasztikusan csökkenő költségvetési ráfordítások egyre inkább arra ösztönzik a tagállamokat, hogy most még erősebben és hatékonyabban fogjanak össze a közös biztonság- és védelempolitika keretén belül. A nemzetközi válságkezeléshez és békefenntartáshoz a tagországok katonai képességeinek és erőforrásaiknak optimális összehangolására, a védelmi szektor együttműködésének elmélyítésére van szükség, mivel az unió államainak a kritikus technológiák és képességek kifejlesztésére és fenntartására a jövőben külön-külön nem lesz kapacitásuk.

One of the most frequently discussed topic in the European Union is the analysis of the current situation and the future role of the defense industry. As the result of the economic crises the member states are increasingly encouraged to collaborate more strongly and more effectively on the fields of common security and defense policy especially focusing on the drastically decreased budget expenditures. For the international crisis management and peacekeeping missions it is required to optimize coordination in military capabilities and to deepen the military sector cooperation, because the member states won't have enough separated capacities to develop and maintain the critical technologies and capabilities in the future.

Kulcsszavak: *Európai Unió, védelmi ipar, biztonság- és védelempolitika, versenyképesség, együttműködés, költségvetés, kihívás ~ European Union, defence industry, security and defence policy, competitiveness, cooperation, budget, challenge*

BEVEZETÉS

Az Európai Unió szervezeti és nemzetközi szinten is kiemelkedő szerepet szán a béke és a biztonság megteremtésére, fenntartására, védelmére. Az EU közös biztonság- és védelempolitikájára (KBVP) jellemző, hogy alapvetően a tagállamok kormányközi együttműködésére épül, amely együttműködést meglehetősen nehezíti, hogy leginkább ezen a területen ragaszkodnak a tagországok nemzeti szuverenitásukhoz, többek között ezért sem tekinthető ez a hagyományos értelemben vett közösségi politikának. Az európai védelmi együttműködés hatékonyabbá tétele hosszú évtizedek óta a transzatlanti kapcsolatok egyik legvitatottabb kérdéskörét képezi. [1]

A 2013-as évben az Európai Unión belül a védelmi ipar és a közös biztonság- és védelempolitika témaköre kiemelt szereppel bírt. Az egész éves aktív munka zárófejezete az Európai Tanács 2013. december 19-20. között megtartott ülése volt, ahol a Tanács megvizsgálta és megvitatta az Európai Bizottság, az Európai Külügyi Szolgálat1 és az Európai Védelmi Ügynökség által előterjesztett közleményeket, jelentéseket és javaslatokat a védelmi és biztonsági ágazatra vonatkozólag. Annyi bizonyos, hogy a közös európai biztonság- és védelempolitika és egy ehhez szervesen kapcsolódó stabil és anyagilag, technológiailag innovatív védelmi ipar megvalósulása nagy megmérettetést jelent az Európai Unió számára.

AZ EURÓPAI VÉDELMI IPAR JELLEMZŐI, HELYZETE ÉS KIHÍVÁSAI NAPJAINKBAN

A védelmi ipar az Európai Unió ágazati politikái közül az ipari és kutatási politika részét képezi. Alapját és kereteit az Európai Unió működéséről szóló szerződés 173. és 352. cikke határozza meg. A 173. cikk az Európai Unió iparpolitikájának jogalapját alkotja, míg a 352. cikk azon esetek szabályzására szolgál, amikor az európai uniós alapszerződések nem rendelkeznek konkrétan a valamelyik uniós célkitűzés eléréséhez szükséges fellépésről. A reális alapokon nyugvó és eredményes közös biztonság- és védelempolitika, a hadiipari tevékenységek uniós szintű összehangolása, illetve a védelmi ipar versenyképesebbé tétele már a 2000-es évek elejétől a Közösség legfőbb célkitűzéseinek egyike. Ezen célok hathatós és gyorsabb megvalósítása érdekében korábbi kezdeményezések eredményeképpen 2004-ben létrehozták az Európai Védelmi Ügynökséget (EVÜ)[2]. A szervezet jogi és intézményi keretet biztosít a tagországok védelmi területen való együttműködéséhez.

Fő feladatai és funkciói:

- a védelmi képességek fejlesztése a válságkezelés területén;
- az európai fegyverkezési együttműködés előmozdítása és megerősítése;
- a DTIB3, az európai védelem ipari és technológiai alapjainak megerősítése, és egy nemzetközi szinten versenyképes európai védelmieszköz-piac létrehozása;
- az európai védelmi kutatás és technológia hatékonyságának megerősítése. [2]

Dánia kivételével az Unió minden tagállama része a brüsszeli székhelyű EVÜ-nek, amely az Európa Tanács irányítása és politikai felügyelete alá tartozik. Nemzetközi szinten a jelenlegi trendeket figyelve és vizsgálva megállapítható, hogy a védelmi ipar egy olyan stratégiai iparág, mely magában foglalja a hagyományos értelemben vett hadiipart, a belbiztonságot és a

[1] EKSZ – hivatalosan 2011. január óta működik az EU legújabb külpolitikai szerveként. Olyan szolgáltatást nyújt az Uniónak, mely lehetőséget ad kapcsolatépítésre, információgyűjtésre, emellett biztosítja az EU külpolitikai érdekeinek közvetlen érvényesítését. Az EKSZ közvetlenül a kül- és biztonságpolitikai főképviselő vezetése alatt működik, függetlenül az Európai Tanácstól és az Európai Bizottságtól.

[2] 2004. július 12. European Defence Agency (EDA)

[3] Defence Technology Industrial Base

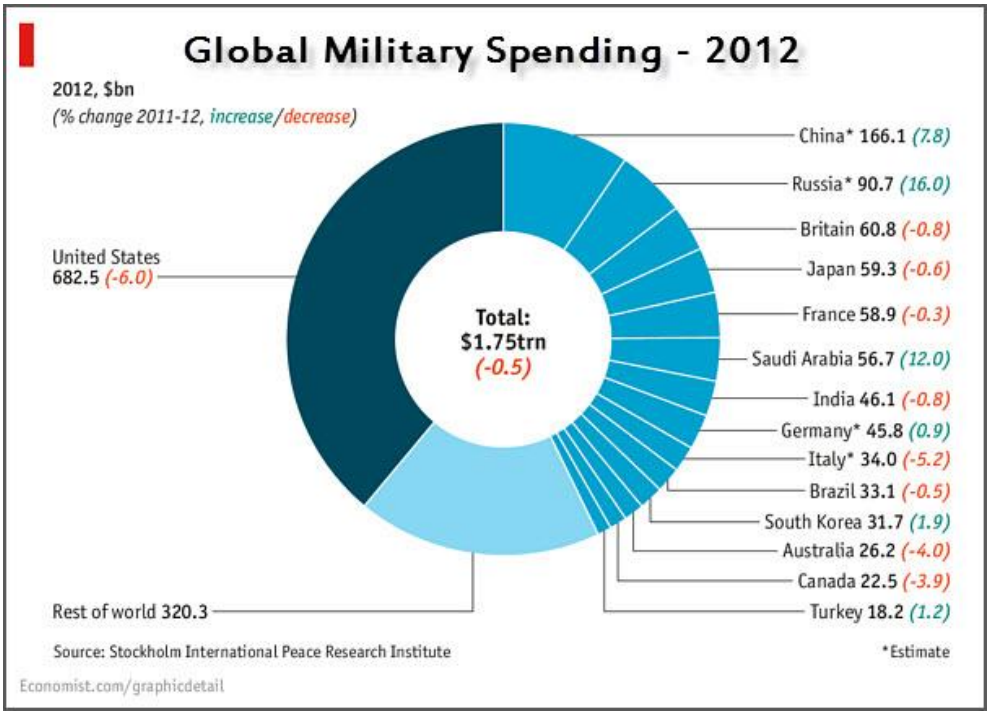
fejlődőben lévő biztonsági ipart, a repülőgép- és űripart, a terrorelhárítást, a kiber védelmet és a katasztrófavédelmet egyaránt. [3]

A védelmi ipar a többi iparághoz képest több területen specifikusabb vonásokkal rendelkezik. A termékek kifejlesztése jelentős időt vesz igénybe, a rendszerek működőképességét hosszú éveken, sokszor több évtizeden keresztül fenn kell tartani, a kutatások és fejlesztések jelentős és egyre nagyobb költségekkel járnak, a már értékesítésre bocsátható termékek kereskedelmi forgalma pedig erősen függ a tagországok kormányaitól. A hatalmas műszaki és tudományos felkészültség, a már monumentális méreteket öltő tőkeigény miatt napjainkban már a világhatalmak sem kívánnak kizárólag teljes körűen önellátó hadiiparra berendezkedni.

A védelmi piac – többek között a védelmi ipar jellemzőiből kifolyólag – a hagyományos értelemben vett piac tulajdonságaitól eltérő sajátosságokkal bír. Szinte kizárólag állami kereslet jellemzi, a gyártóknak és értékesítőknek termékeikkel szigorú exportellenőrzéseknek, komoly nemzeti és nemzetközi szabályoknak, szigorú proliferációval kapcsolatos kötelezettségeknek kell eleget tenniük. A fent említett okok által beszűkült keretek miatt így meglehetősen korlátozott a kínálat.

Az európai védelmi ipar költségvetését a 2000-es évek második felétől az erőteljes megszorítások jellemezték. 2005 és 2013 között reálértékben mintegy 20 százalékkal csökkentek a védelmi kiadások. [4] Bár az Európai Unió tagállamai ez idő alatt is határozottan törekedtek a közös biztonság- és védelempolitikára, számos nyilatkozat és megállapodás ellenére érzékelhető volt az egységes politikai akarat és a társadalmi támogatottság hiánya a kontinens szintű geopolitikai helyzet megerősítésére, és ez a státusz jellemző napjainkban is. [5] A Közösség tagországainak társadalmaiból hiányzik a hagyományos értelemben vett ellenségkép, nem érzik magukat katonai vonatkozásban támadástól fenyegetve. A nagyméretű, globális háborúk kialakulásának veszélye elhanyagolható, ugyanakkor fel kell készülni a kisebb méretű konfliktusok kialakulására, amely komoly következményekkel járhat az adott országra nézve. [6] A politikai erőfeszítések emiatt Unió-szerte inkább a gazdasági és társadalmi témákat érintő kérdésekre helyezik a hangsúlyt. A 2008-as gazdasági válság még mélyebb pontra taszította a hadiiparra, annak fejlesztésére irányuló összeghatárok szintjét, ami többek között azért is aggasztó, mert amíg kontinensünkön az elmúlt években folyamatosan faragták a korszerűsítésre és újításokra szánt költségeket, addig Kínában, Indiában, Brazíliában és Oroszországban a lehetőségeikhez mérten szisztematikusan növelték azokat. Tisztán politikai szempontból nézve teljesen logikusnak tűnik, hogy adott országban az állami kiadások szükségszerű csökkentése esetén azon területeken fogják vissza a költekezést, amelyek legkevésbé vannak kihatással az állampolgárok mindennapi életére, nem vagy csak minimálisan érintik érzékenyen a társadalmat.

Az Európai Unióban a védelmi költségvetések redukálása szinte valamennyi tagállamban jelentős forráscsökkentéssel járt, a kutatás területén és a technológiai innovációs programok tekintetében visszaesés következett be. A gazdasági és pénzügyi válság hatására a védelmi kiadásokra szánt összegek mértéke már egész Európa-szerte jellemzően csökkenő tendenciát mutatnak. Az európai védelmi ipari vállaltok többsége úgy reagál a recesszióra, hogy kihelyezi a gyártási folyamatokat a harmadik világ országaiba, ahol - ugyan a technológiák és a szellemi tulajdonjogok átadása árán - gazdaságosabban tudja előállítani termékeit.



1. ábra. Globális katonai kiadások – 2012. Százalékos növekedés/csökkenés dollár milliárdban mérve [7]

Problémát jelent többek között az is, hogy az európai védelmi ipar belső piaca meglehetősen széttagolt. Különböző nemzeti fogyasztói bázisok vannak, így a széttöredezettség miatt a kereslet és a kínálat összhangja nem jöhet létre. Ezen felül a fejlettebb országok nagyobb mértékben tudnak részt venni és hozzájárulni a hadiipari termékeket érintő kutatásokhoz és fejlesztésekhez, az ezen folyamatok végeredményeként megvalósított termékek, eszközök gyártásához és értékesítéséhez. Jelenleg az Egyesült Királyság, Franciaország, Németország, Olaszország, Lengyelország, Svédország és Spanyolország az a hét tagállam, melyek jóval erősebb védelmi ipari technológiai bázissal rendelkeznek a többi tagállamhoz képest. Ebből kifolyólag a kisebb országok, mint például Magyarország is, nem tudják egyenlő arányban kivenni részüket és pozícióba helyezni magukat, kiszorulnak olyan társulásokból és együttműködésekből, melyek meghatározó szereppel bírnak az Európai Unión belül a védelmi és biztonsági ágazatban. Az egyik ilyen kardinális nemzetközi intézmény az OCCAR[4]kormányközi szervezet, melynek feladata, hogy saját tagországi keretein belül elősegítse és kezelje az együttműködési fegyverkezési programokat, és azokat teljes életciklusukon keresztül végigkísérje. [8]

A védelmi piacra jellemző diverzifikáció komoly gátakat szab a kis- és középvállalkozásoknak is, mely többek között abban nyilvánul meg, hogy sok esetben nem rendelkeznek elegendő információval az üzleti lehetőségeket illetően, nehezen tudják értékesíteni termékeiket, a védelmi beszerzésekhez való hozzáférésük pedig meglehetősen sok akadályba ütközik az egységes szabványok és tanúsítások hiányának köszönhetően.

[4] Organisation for Joint Armament Cooperation, (Franciául: Organisation conjointe de coopération en matière d'armement ; OCCAR) Közös Fegyverkezési Együttműködési Szervezet, melyet 1996-ban alapított négy ország – Franciaország, Németország, Olaszország és az Egyesült Királyság – védelmi minisztere, majd 2003-ban és 2005-ben Belgium és Spanyolország is csatlakozott a társuláshoz.

CÉLKITŰZÉSEK ÉS ELKÉPZELÉSEK A JÖVŐRE VONATKOZÓAN

A biztonságot és védelmet illetően a közös cél e tekintetben egy erős, egy irányba tartó Európa, melynek alapja azonban a hiteles és hatékony közös védelemi és biztonságpolitikai együttműködés. José Manuel Barroso, az Európai Bizottság elnöke állítja: *„Közös védelmi politika nélkül fellépésünknek nincs elegendő súlya a világ színpadán. A közös védelmi politika megszilárdításához pedig meg kell erősítenünk védelmi és biztonsági ágazatunkat. A rendelkezésünkre álló erőforrások szűkösek: az együttműködés kulcsfontosságú, célkitűzéseinket és erőforrásainkat pedig úgy kell alakítanunk, illetve kiaknáznunk, hogy elkerüljük a különböző programokba fektetett energiák felesleges megkettőzését. Itt az ideje, hogy összefogjunk, és ezáltal még többet tegyünk; itt az ideje, hogy elkötelezzük magunkat a szorosabb védelmi együttműködés mellett, és megvalósítsuk azt."* [9]

Egy hitelesen és produktívan működő közös biztonság- és védelempolitikához szilárd európai védelmi ipari és technológiai bázisra van szükség és ennek megvalósítása érdekében szükségszerű lenne, hogy az erre irányuló törekvések és tevékenységek összessége elsőbbséget élvezzen az Európai Unió stratégiájában. Catherine Ashton, az Unió külügyi és biztonságpolitikai főképviselője és egyben az Európai Bizottság alelnöke a következőket mondta: *„Az EU fontos feladatának tartja, hogy a biztonság őreként lépjen fel szomszédságában és szerte a világon, hogy megvédje érdekeit és hozzájáruljon a nemzetközi béke és biztonság megteremtéséhez. Ahhoz, hogy ezt megtehessük, megfelelő kapacitásokra van szükségünk, melyek létrehozásának és fenntartásának előfeltétele a szilárd ipari bázis. Ez a munkahelyteremtéshez, a növekedéshez és az innovációhoz is fontos."* [10] Az EU-ban egy egységes védelmi piac kialakulása többek között azt eredményezné, hogy az európai hadiipar jóval kedvezőbb helyzetbe kerülne. Ennek persze egyik alapvető feltétele lenne, hogy a nemzeti piacok napjainkra jellemző magas szintű szétforgácsolódása csökkenő tendenciát tanúsítson.

Ha Európa erős és stabil biztonsági és védelmi ágazatot kíván kialakítani és fenntartani, ahhoz a tagállamoknak bővíteni kellene a közös kutatási programokat, törekedniük kellene az átfedések elkerülésére és mindezek mellett hangsúlyt kellene fektetni a védelmi költségvetéseik összehangolására is. A megkettőzések kiküszöbölésére és az ebből adódó felesleges költségek és anyagi források felemésztésének elkerülésére többek között elfogadható az a szemlélet, hogy minden olyan tagállam, mely a védelmi ipari termelésben részt vesz, lehetőleg arra az adott termék, technológia fejlesztésére, gyártására és előállítására szakosodjon, amelyiket adottságaihoz és lehetőségeihez mérten a legszakszerűbb és egyben a leghatékonyabb módon tud előállítani. [11]

A kutatás és fejlesztés területén kiterjedtebb összefogásra és koordinálásra lenne szükség, érdemes lenne ezt a szférát egyfajta rendszerbe foglalni. Célszerű lenne kiaknázni a jelentősebb védelmi cégek és egyetemek közötti együttműködést, melynek erősítése mindkét fél számára mérhető szellemi, technológiai és anyagi előnyökkel járna. Szükségszerű lenne a K+F tevékenységek mind mennyiségi mind pedig minőségi fokozása az ezzel járó financiális eszközök biztosítása révén. A kutatási és fejlesztési tevékenységeket, azok lehetőségét a termelő és szolgáltató üzemekben is ajánlott volna kialakítani, mivel a kizárólag erre szakosodott intézményekben az általában véve nagy volumenű kutatások mellett már nincs se idő sem pedig kapacitás a részletek feltárására és vizsgálatára a kutató állomány leterheltsége miatt. A polgári és a katonai kutatások közötti szinergiák is kiemelkedő fontossággal bírhatnak. A két kutatási terület közötti együttműködést érdemes lenne szorosabbá tenni és fokozottan igénybe venni. Ezen kívül fel kellene mérni, hogy a polgári kutatások eredményeit hogyan tudná a védelmi ipar hasznosítani. A fent megfogalmazottak által hatékonyabban ki/fel lehetne használni a kettős hatású (polgári és katonai) lehetőségeket, serkentve ezáltal is a gazdasági növekedést és új munkahelyek teremtését. Komoly előrelépést jelentene a vállaltokat – főleg a kis- és középvállalatok rétegét – illetően, ha bizonyos területeken egységes szabványosítással

és tanúsítással bírna az iparág. Egy versenyképes védelmi piac létrejöttéhez nagymértékben hozzájárulna továbbá a fegyverkezési programokban való együttműködések elősegítése, az interoperabilitás[5] biztosítása, mely az európai tagállamoknak a közös műveletek során optimális kapacitás-felhasználást nyújthatna.

A védelmi ipar – gazdasági és technológiai összetevőiből kifolyólag – fontos részét képezi Európa ipari versenyképességének. Az európai hadiipar megerősödése nemcsak a védelmi szféra területén lenne mérhető, hanem a polgári lakosság körében is érzékelhető változásokat idézne elő. Az iparági átszervezés kedvezne a vállalkozások – különösen a kis- és középvállalkozások – fejlődésének, új munkahelyek teremtésével járna. Az új termékek és eszközök, új gyártási módok bevezetése pedig új piacok megnyitásának, illetve a belső piac fellendülésének lehetőségét vonná maga után.

ÖSSZEFOGLALÁS

Az Európai Unió védelmi képességeinek megőrzésének és fejlesztésének nélkülözhetetlen alapja egy egységes, stabil, hosszútávon fenntartható, versenyképes védelmi technológiai és ipari bázis. Ehhez viszont mindenképpen szükséges egy széthúzásoktól és szélsőségektől mentes, egy irányba tartó, meghatározott működési elvekkel és keretekkel bíró közös biztonság- és védelempolitika, melynek az európai szintű összehangolása, mielőbbi megvalósítása a globális viszonyokat és állapotok tekintetve is sürgető erővel bír. A hihetetlen mértékű fejlődést tanúsító Kína, az erejét ismét visszanyerni igyekvő Oroszország és a szintén fokozódó emelkedés útjára lépő India komoly gazdasági és politikai kihívásokat jelentenek az EU-nak. A Közösség közös fegyverbeszerzésre és egységesítésre való törekvéseit nagyban nehezíti az a tényállás, hogy az tagországokban különböző törvényi, rendeleti és szabályozási rendszerek és elvek érvényesülnek, melyeket nem ajánlott figyelmen kívül hagyni, feladni vagy megváltoztatni, hiszen ezáltal nemzeti érdekek sérülhetnek. Többek között ebből kifolyólag is egy igen lassú folyamat elébe nézünk az egységes európai uniós KBVP-t illetően. Vitathatatlan tény továbbá az is, hogy az iparágat érintő problémák és kihívások java részének forrása financiális eredetű. A pénzügyi manőverezések lehetősége kiváltképp a 2008-ban kirobbant gazdasági válság következtében minden egyes költségvetési megszorítással évről évre egyre szűkül. Az Európai Unió kormányaira nagy feladat hárul annak tekintetében, hogy megtalálják az egyensúlyt a kiadások prioritását illetően, és a védelmi és biztonsági igényeknek maximálisan eleget téve megfelelő anyagi, szellemi és technológiai ráfordítások árán létre tudják hozni a célul kitűzött erős és egységes európai biztonság- és védelempolitikát. A tét, hogy az Európai Unió saját erejét, lehetőségeit és a nemzetközösség adta előnyöket kihasználva képes legyen garantálni saját biztonságát.

Felhasznált irodalom

[1] Németh József Lajos: A transzatlanti kapcsolatok néhány vitás kérdése biztonságpolitikai megközelítésben, Zrínyi Miklós Nemzetvédelmi Egyetem, Hadtudományi Doktori Iskola, PhD értekezés, 2007, p.17, 29, 42, 58.

[2] EUR-Lex – Hozzáférés az európai joghoz. 2004/551/KKBP : A Tanács 2004/551/KKBP együttes fellépése (2004. július 12.) az Európai Védelmi Ügynökség létrehozásáról, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004E0551:HU:NOT, (a letöltés ideje: 2014. február 13.)

[5] együttműködő képesség

[3] A Magyar Védelmiipari Szövetség helyzetértékelése, http://www.vedelmiipar.hu/index.php/hirek/hatteranyagok/56-helyzetertekeles, (a letöltés ideje: 2014. február 13.)

[4] Andre Frontini: A decemberi EU-csúcs és az európai hadiipar, Napi Gazdaság 2013. december 16., http://www.epc.eu/documents/uploads/pub_4024_ngazvide0161212.pdf, (a letöltés ideje: 2014. február 13.)

[5] Fregan Beatrix, Fábián Éva: The special relationship for european integration; Kommunikáció 2010; ZMNE 2010., p. 67. http://hhk.uni-nke.hu/downloads/kiadvanyok/konf2010.pdf, (a letöltés ideje: 2014. február 14.)

[6] Farkas Tibor: Válságkezelés, válságreagáló műveletek; Hadtudományi Szemle 2008/1., pp.:1-6. http://uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2008/2008_1/2008_1_hm_farkas_tibor_1_6.pdf, (a letöltés ideje: 2014. február 14.)

[7] Globális katonai kiadások 2012-ben, www.jobs-not-wars.org/global-military-spending-2012-chart/, (a letöltés ideje: 2014. február 15.)

[8] Szegedi László: A magyar védelmi ipar helyzete és várható fejlesztési feladatai - nemzetközi tapasztalatok figyelembevételével – az Európai Unióhoz való csatlakozás tükrében. Integrációs és fejlesztési munkacsoport. Biztonsági és Védelempolitikai témacsoport, 2002. pp .: 1-32.

[9] Úton a versenyképesebb és hatékonyabb európai védelmi és biztonsági ágazat felé, Európai Bizottság sajtóközlemény, Brüsszel, 2013. július 24., http://europa.eu/rapid/press-release_IP-13-734_hu.htm, (a letöltés ideje: 2014. február 14.)

[10] Úton a versenyképesebb és hatékonyabb európai védelmi és biztonsági ágazat felé, Európai Bizottság sajtóközlemény, Brüsszel, 2013. július 24. , http://europa.eu/rapid/press-release_IP-13-734_hu.htm, (a letöltés ideje: 2014. február 14.)

[11] A Külügyi Bizottság jelentése az európai védelmi technológiai és ipari bázisról (2013/2125(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0358+0+DOC+XML+V0//HU, (a letöltés ideje: 2014. február 14.)

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Székely Zoltán
szekely.zoltan@uni-nke.hu

HABEAS CORPUS MACHINIMA AVAGY ELFOGHAT-E ENGEM EGY ROBOT?

Absztrakt

A rendvédelmi tevékenység során a leggyakrabb alapjogot korlátozó intézkedés a személyes szabadság korlátozása, azaz az elfogás és előállítás. A technika fejlődésével elérhető közelségbe került, hogy a közeli jövőben ezt az intézkedést emberek helyett illetve mellett robotok hajtsák végre. Kérdés, hogy ez egyáltalán jogilag és műszakilag lehetséges-e, azaz a következő évtizedekben átvehetik-e robotok a rendőrjárőrök szerepét. A tanulmány ezt a kérdéskört járja körbe egy célzott alapkutatás egyik első lépcsőjeként. A teljes kutatás a robotizált megoldások hon- és rendvédelmi alkalmazási lehetőségeiről és annak társadalmi, jogi és műszaki feltételeiről, fenntarthatóságának biztosításáról szól. A jogi helyzetet e mű csak az intézkedéshez közvetlenül kapcsolódó, felhatalmazást tartalmazó közjogi jogág szempontjából elemzi, a munkajogi, polgári jogi, büntetőjogi ágak szerinti elemzést további munkák fogják tartalmazni, akárcsak a technikai megvalósítás feltételeinek lebontását. A végkövetkeztetéseket a tanulmány 7. fejezete tételesen összegzi.

Arrest and apprehension are the most regular law enforcement actions considering fundamental rights. In the near future, development of technical means puts the use of robots for the abovementioned action within reach. In the next few decades, the use of „robocops" must be discussed and decided, both legally and technically. This study addresses this topic as a first stage of a targeted research programme. The full research is aimed at the chance of using robots for national defence and law enforcement in a sustainable, possible, publicly and legally acceptable way. Regarding the legal frame, the current study is focusing on the public administration branch of law, the other branches as Labour Law, Civil Law and Penal Law will be analyzed in this scope with followingly published studies in the near future, just as details of conditions on technical execution. The final, 7th part of this work summarizes the conclusions of the study.

Kulcsszavak: *robot, rendőr, habeas corpus machinima, mesterséges intelligencia, robotzsaru ~ robot, police, habeas corpus machinima, artificial intelligence, robocop*

BEVEZETÉS

A rendőrségi által leggyakrabban alkalmazott alapjogot korlátozó intézkedések nem mások, mint az elfogás és az előállítás,[1] melyeket a továbbiakban az egyszerűség kedvéért e tanulmányban együtt elfogásként nevezünk. A Magyar Rendőrség által közzétett statisztikák alapján, Magyarországon ez átlagosan naponta kb. 350 embert érint.[2] Ezen kívül szintén alkalmazhatja a fent meghatározott elfogás intézkedést a nemzetbiztonsági szolgálatok, a büntetés-végrehajtás, a Nemzeti Adó- és Vámhivatal illetve az Országgyűlési Őrség hivatásos állománya, sőt még a személy- és vagyonőrök is. Tekintettel arra, hogy a személyes szabadság minden embert megillető, csak megfelelő jogállami garanciák érvényesülése esetén korlátozható alapjog, abszolút nem mindegy mikor, hogyan és ki által történik csorbítása.[3] Lehetséges-e, hogy a közeli jövőben robotok – a törvény felhatalmazása alapján - embereket fogjanak el? E kérdés egyre inkább aktuális. A robotika ugyanis elérte a fejlődés azon fokát, hogy már bizonyosnak tűnik: a következő évszázadban a robotok a társadalom mindennapjainak részeivé, életviszonyaink szereplőivé, ebből eredően jogrendszerünk elemeivé válnak. E szerepüket a hadtudomány már felismerte és bizonyos országokban – elsősorban az Amerikai Egyesült Államokban – legalább fél évtizede publikált eredményekkel is rendelkező kutatások folynak a robotok honvédelmi (katonai) felhasználásának lehetőségeiről.[4] Eközben rendvédelmi felhasználásuk irányába csak a közelmúltban indultak kutatások, ráadásul elsősorban a katasztrófavédelem területén.[5] Lehetséges rendőri szerepük meghatározására azonban csak a sci-fi irodalomban születtek elképzelések,[6] holott időszerű és szükséges a terület tudományos feldolgozása is. E tanulmányban az annak alcímében feltett kérdésre adom meg a választ, egy célzott alapkutatás egyik első eredményeként. A teljes alapkutatás arra a kérdésre keresi a választ, hogy melyek azok a honvédelmi és rendvédelmi tevékenységek során alkalmazható, robotizált megoldások, amelyeknek az élőerők megóvása és a hatékonyság növelése érdekében történő felhasználása társadalmilag elfogadott és hosszú távon is fenntartható. A kutatási tervben ezen írás tárgyául szolgáló témát két kérdés fedi le. Az egyik, hogy nehezebb-e egy robotot elfogadni a honvédelem és a rendvédelem eszközeként, a közhatalom érvényesítőjeként, mint egy embert? A másik, hogy milyen jogi szabályozási változtatások szükségesek a robotok honvédelmi és rendvédelmi felhasználásához? Természetesen erre a két kérdésre ez az egy tanulmány nem tud választ adni, ugyanis jelen munka nem dolgozza fel sem a hadijog sem a közjog teljes területét, pusztán a rendvédelem egy részére koncentrál. Kiegészítésképpen kitér ugyanakkor a technikai megvalósítás sarokpontjaira, a műszaki és a jogi megoldások fő szinergiáira, de elsősorban a tanulmány tárgyával kapcsolatban.

JOGELMÉLETI ÁTTEKINTÉS

A kérdés jogrendszerben történő elhelyezéséhez elengedhetetlen egy rövid és tömör jogelméleti áttekintés. A jog eredeti rendeltetése az adott közösség szempontjából hasznos életviszonyok megóvása (továbbá újabban keletkeztetése), egyben a káros életviszonyok visszaszorítása, ellehetetlenítése. Ahogy az életviszonyok változnak úgy a jogviszonyoknak és az azokat tartalmazó jogszabályoknak is változniuk kell. A jognak az élet egyes területeihez kapcsolódó, gyakran az adott életviszonyok jellegéhez igazodó részét nevezzük jogágnak.[7] Azokat a jogágakat, amelyek az önálló államot elérő szintű közösségek államként történő létezését, a közösség egyes tagjainak államhoz való viszonyát, az államnak az őt alkotó személyek feletti hatalmi jogosítványait ölelik fel, együttesen közjognak nevezzük.[8] Az egyszerűség kedvéért a közjog és a magánjog jogtörténelmi síkon folyamatosan mozgó határvonalát nem ismertetjük, a vegyes jogágakat pedig többségi jellemzőik szerint soroltuk be, a nagyfokú disztinkciónak a jelen kérdésben nincs relevanciája. A közjognak az egyik jogága a közigazgatási jog, ami –

nagyon leegyszerűsítve - a közösség életének állami szempontból releváns, elsősorban – de nem feltétlenül kizárólagosan (!) - a közérdeket szem előtt tartó igazgatását fedi. Ennek egy mellékága a rendészet jogterülete, melynek funkciója a közösség működésének szabályozása, az optimális és fenntartható működést biztosító rend kialakítása. A rendészeten belül foglalja el a helyét a rendvédelem tevékenysége, a közigazgatás ultima ratiója, feladata a kialakult rend védelme, a megbomlott rend helyreállítása, akár az erőszak monopóliumának szükséges és arányos alkalmazása árán is.[9] A rendvédelmi tevékenységhez kapcsolódó egyik jogosítvány, hogy a tevékenység végzésére feljogosított személyek egy másik személyt elfoghatnak, azaz személyes szabadságában akár erőszak alkalmazásával is korlátozhatják, illetve őt egy meghatározott hatóság (bíróság, ügyészség stb.) elé állíthatják, adott területtől vagy személytől távol tarthatják, kényszergyógykezelésnek vagy vérvételnek vethetik alá és még sorolhatnánk milyen más, törvényben meghatározott magatartásra kényszeríthetik. Természetesen ezt csak akkor tehetik meg, ha a törvényi feltételek fennállnak. Azonban most nem azt a kérdést boncoljuk, mikor és hogyan kerülhet erre sor. A kérdésünk az, hogy ki illetve pontosabban ki vagy mi teheti ezt meg, azaz hogyan alakul az alanya ennek a jognak? A személyes szabadság alapjog. Alapjogot csak törvény, más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával lehet korlátozni.[10] Az alapjogokra vonatkozó rendelkezéseiben az Alaptörvény a korlátozás alanyára, tehát a korlátozás alkalmazására jogosultra nem tér ki, egyetlen kivételt a bűncselekmény gyanújával gyanúsított és őrizetbe vett személlyel szemben tesz, ahol előírja, hogy akit ilyen okból vettek őrizetbe, azt a lehető legrövidebb időn belül bíróság elé kell állítani vagy szabadon kell bocsátani, tehát megnevezi a bíróságot, mint az eljárásra jogosult szervet. Az elfogás esetére az Alaptörvény nem határozza meg az intézkedés alkalmazására jogosultak körét. Ez azért fontos, mert ezáltal bármely törvénynek lehetősége van annak szabályozására anélkül, hogy az Alaptörvénybe ütközés tilalmát megsértené.[11] A jelenlegi törvényi szabályozás az elfogás és előállítás intézkedést például a rendőri szervek[12] tekintetében a rendőr alkalmazhatja, ami egyértelműen a rendőrség hivatásos állományába tartozó személyeket takarja.[13] Ugyanez a helyzet a nemzetbiztonsági szolgálatok,[14] a Nemzeti Adó- és Vámhivatal,[15] illetve az Országgyűlési Őrség[16] hivatásos állománya esetében. A magánbiztonsági szférában szintén maguk a személy- és vagyonőrök jogosultak az elkövető elfogására.[17] Az Alaptörvény szerint tehát a lehetőség Magyarországon megvan arra, hogy az elfogásra feljogosítsunk egy önállóan intézkedő robotot, azonban e lehetőség biztosítása érdekében törvénymódosításra van szükség. Jelenleg elfogás intézkedést a hatályos magyar törvény alapján robot önállóan nem alkalmazhatna. A robotot a rendőrség az elfogás során legfeljebb eszközként alkalmazhatja, tehát a robot a szintén jelen lévő hivatalos személy elfogás intézkedésének sikerét biztosíthatja, akárcsak a bilincs vagy a szolgálati kutya.[18] Utóbbi lehetőség, az eszközként történő alkalmazás, furcsamód a jelen törvényi szabályozás esetén csak akkor állna rendelkezésünkre, ha a robotot nem a rendőrség üzemeltetné, a külső eszközök igénybevételi jogosultságát megállapító rendelkezés ugyanis nem tartalmaz taxatív felsorolást az igénybe vehető eszközökről, míg a rendőrség saját eszközeinek alkalmazhatóságát szabályozó rendelkezés igen.[19] Nyilvánvalóan ezt a kérdést is érdemes törvénymódosítás útján rendezni. A rendvédelmi tevékenységet kifejtő egyéb szervezetek esetében szintén találunk törvényi példát eszköznek elfogásra történő alkalmazására, például a szolgálati kutya vagy elfogó háló elfogásra alkalmazásra tekintetében.[20] Persze számos esetben felmerült már a kérdés, hogyan engedhető meg egy eszköznek vagy berendezésnek, hogy egy ember személyes szabadságát korlátozza?

A SZEMAFOR-PÉLDA

Miután tisztáztuk a jogi alapkérdést, a fent kérdést ezen egyszerű példával szeretném tisztázni. Sokak számára elképzelhetetlennek tűnhet ugyanis az, hogy az ő személyes szabadságukat egy „berendezés" korlátozza, illetve hogyan lehet erre egy gépet feljogosítani. Pedig ha kissé visszanyúlunk a rendvédelemtől a tágabb rendészet irányába, máris találhatunk egy nagyon egyszerű kiindulási alapot a probléma megoldására. Valójában ugyanis az alapproblémát már majdnem több mint másfél évszázada megoldotta az élet. Londonban 1868-ban üzembe helyezték az első közlekedési lámpát, az elektromos közlekedési lámpa 1912-es szabadalmaztatása óta pedig külön kísérletek nélkül is elfogadható tény, hogy az emberek döntő többsége elfogadja személyes szabadságának lámpa általi korlátozását, magyarán szólva, ha piros, akkor megáll és csak a zöld jelzésen halad át. Ugyanez a helyzet a parkolókba vezető sorompókkal, vasúti biztonsági berendezések jelzőivel vagy a repülőtéri biztonsági kapukkal. A közlekedési lámpák vezérlését először 1963-ban bízták számítógépre a kanadai Torontóban. Azóta már minden nagyvárosban egy program és általa vezérelt berendezések határozzák meg, ki mikor és meddig ácsorog az autójával – vagy éppen gyalog - a kereszteződésben. E tanulmány szempontjából érdekes színfolt, hogy a dél-afrikai angolban a közlekedési lámpát robotnak hívják. Azonban a személyes szabadságnak a közlekedés biztonsága, ezáltal az élet és testi épség valamint a vagyon védelme érdekében történő korlátozásának az alanya nem a berendezés, de nem is a központi vezérlő egység, azok ugyanis csak közvetítik a döntést, amit az állam közlekedésrendészeti hatáskörében eljáró forgalomirányító hatóság hoz a jogszabályok szerint. Az állam az, aki a közlekedést jogszabályokkal szabályozza és ez a szabályozás mondja ki, hogy ha a jelzés tilos (piros) akkor az állam, a köz érdekében, megtiltja az áthaladás, ekképpen korlátozza a személyes szabadságot. Megállapíthatjuk tehát, hogy bármilyen gép vagy berendezés korlátozhatja a személyes szabadságot oly módon, hogy erre vonatkozó, törvényben meghatározott állami elhatározást érvényesít. Itt el is jutottunk a következő kérdésig, nevezetesen hogy mi a különbség egy robot és egy közlekedési lámpa között, azaz itt az ideje a robot definiálásának.

A ROBOT DEFINÍCIÓJA

Maga a robot kifejezés a „munka" szó szláv megfelelőjéből ered és a világirodalomban először egy szépirodalmi műben, egy Karel Čapek által írt, R.U.R. című drámában tűnt fel, 1920-ban.[21] A műben a tömeggyártásból kikerülő, modern rabszolgaként használt, ám gondolkodásra képes robotok fellázadnak az emberiség ellen és kipusztítják azt. Ezen alkotás benyomásai az elmúlt évszázadban meghatározták a robotokhoz való társadalmi és irodalmi illetve filmművészeti hozzáállást, gondoljunk csak Frank Herbertnek a Dűne című sci-fi regénysorozatára,[22] a Terminátor és a Mátrix sorozatfilmekre és így tovább. Persze az elmúlt évezredek során a tudomány már hozzáedződött, hogy legújabb vívmányait félelemmel vegyes gyanakvás övezi, művelői pedig megszokták, hogy csak az egzakt magyarázatoknak higgyenek. Ezért e rövid kitérő után vázolom, a kutatás szempontjából mit is értünk robot alatt.

Ehhez először le kell szögezni, hogy a robotnak jelenleg számos definíciója létezik. Az első kísérlet a definíció egységesítésére 1990-ben történt, amikor a VDI[23] 2860 számú irányelve[24] úgy határozta meg az ipari robotot, mint: *„[Az ipari robot] univerzálisan állítható többtengelyű mozgó automata, melynek mozgás-egymásutánisága (utak és szögek) szabadon – mechanikus beavatkozás nélkül programozható és adott esetben szenzorral vezetett, megfogóval, szerszámmal vagy más gyártóeszközzel felszerelhető, anyagkezelési és technológiai feladatra felhasználható."[25]* E definíció értelmezéséhez azonban tisztáznunk kell az automata fogalmát is. *„Automatán egy olyan absztrakt rendszert kell érteni, mely egy diszkrétnek képzelt időskála időpillanataiban érkezett ingerek hatására ezen időpillanatokban*

válasszal reagál, miközben belső állapotát megadott szabályok szerint változtatja a külső ingerek hatására. Az ingerekre adott válasz függ mind az ingerektől mind pedig a pillanatnyi belső állapottól. Ebben az értelemben tehát nemcsak a gépek, hanem bármiféle élő vagy élettelen objektumok tekinthetők automatának, ha ezen séma szerint vizsgáljuk őket, azaz ilyenfajta működést tulajdonítunk nekik."[26] Az automata fogalma nem csak azért fontos, mert nélküle az ipari robot fogalma nem értelmezhető.

Röviden visszakanyarodva a jogelmélethez, a jogi norma hármas szerkezeti jellege (diszpozíció-hipotézis-szankció)[27] gyakran olyan helyzetet teremt – különösen a kógens szabályok terén – ahol a jogalkalmazó ember is kvázi automataként működik. Ha a jogszabály által absztrakt módon megfogalmazott élethelyzet, mint feltétel előáll, az általa cselekvésre kötelezett jogalkalmazónak nincsen más választása, a meghatározott intézkedést kell végrehajtania. Ez fokozottan igaz, ha az intézkedés valamely alapjog korlátozásával jár, hiszen azokat csak törvényes feltételek fennállása esetén, szigorú eljárásrend szerint szabad korlátozni. Így például az elfogás során, ahol a törvény szerinti esetekben azt, akire a feltételek igazak, bizonyos esetekben el kell fogni, mérlegelés nélkül.[28] Pont ezért ez a legmegfelelőbb jogi helyzet az alapkérdés vizsgálatára.

A robot definiálására visszatérve, az ipari robot fenti fogalma mellett több, általánosabb meghatározás is létezik. *Az egyik szerint a robot egy elektromechanikai szerkezet, amely előzetes programozás alapján képes különböző feladatok végrehajtására.[29]* Ezt a fogalmat mindenképp szükséges kiegészíteni annyival, hogy előzetes programozás alatt a felhasználói (újra) programozhatóságot és az önálló tanulási képességet biztosító megoldásokat is érteni kell. Jelen tanulmányban például nem tekintjük robotnak azokat a manipulátorokat és drónokat, amelyek előreprogramozás (pl. betanítás) vagy távirányítás révén vezérelnek, azon egyszerű oknál fogva, hogy a tanulmány témájául szóló dilemma esetükben nem áll fenn, ugyanis a döntéseket az operátor hozza meg helyettük illetve csak egy előre programozott mozgássort végeznek, alternatíva nélkül.

A fenti fogalomnál részletesebb, a VDI ipari robotfogalmánál azonban általánosabb az ISO[30] 8373:2012 számú szabványban található robotfogalom: *Két vagy több tengelyen mozgó programozható, önálló, mozgató mechanizmus, amely környezetében meghatározott feladatokat végez.[31]* Általánossága ellenére e fogalom eléggé lényegre törő ahhoz, hogy a jövőben a robot egységes, tudományosan elfogadott fogalmává váljon, ugyanakkor a tanulmány során mégis a sokkal bonyolultabb és hivatalos magyar szövegével nehezen megjegyezhető, ám jogi erővel bíró fogalmat kell használnunk. Ez pedig nem más, mint az Európai Unió által a kettős felhasználású termékek kivitelének korlátozására kiadott rendeletében szereplő meghatározás. Mentségére legyen mondva, az ISO szabvány kiadása előtt került megszövegezésre. A definiáláson felül terjedelmes körülírást is tartalmaz, nyilvánvalóan azzal a szándékkal, nehogy a tiltó szabály megkerülésével ekvivalens technológia kerüljön kivitelre, ennek eredménye azonban egy terjedelmes, nehezen értelmezhető fogalom lett. Mindenek ellenére eddig ez az egyetlen robotfogalom, amely az Európai Unióban, így hazánkban is jogi erővel bír, ráadásul nemzeti törvényekkel szemben is elsőbbséget élvez. Íme:

„Robot: olyan manipulációs mechanizmus, amely lehet folyamatos működésű vagy pontról pontra mozgatható manipulációs mechanizmus, és szenzorokat is alkalmazhat, és rendelkezik az alábbi jellemzők mindegyikével:

1. többfunkciós;
2. képes anyagok, részegységek, szerszámok és különleges eszközök beállítására vagy orientálására, háromdimenziós térben történő változtatható mozgások révén;
3. három vagy több zárt vagy nyitott hurkos szervoeszközt foglal magában, amelyek léptető motorokat is tartalmazhatnak; és

4. a "felhasználó által programozható" tanít/visszajátszik módszerrel vagy elektronikus számítógéppel, amely lehet programozható logikai kontroller, azaz mechanikai beavatkozás nélküli.
5. N.B.: A fenti meghatározás nem foglalja magában az alábbi eszközöket:
    a) Olyan manipulációs mechanizmusok, amelyeket csak kézzel vagy távoperátorral lehet irányítani.
    b) Állandó sorozatú manipulációs mechanizmusok, amelyek mechanikusan rögzített programozott mozgások szerint működő automatizált mozgó eszközök. A programot mechanikusan korlátozzák a rögzített, de állítható ütközők, pl. csapok vagy bütykök. A mozgások sorrendje és a pályák vagy szögek megválasztása mechanikai, elektronikus vagy elektromos úton nem változtatható, illetve nem is cserélhető.
    c) Mechanikai vezérlésű, változtatható sorrendű manipulációs mechanizmusok, amelyek a mechanikusan rögzített programozott mozgások szerint működő automatikus mozgó eszközök. A programot mechanikusan korlátozzák a rögzített, de állítható ütközők, pl. csapok vagy bütykök. A mozgások sorozata és a pályák vagy szögek megválasztása a rögzített programsémán belül változtatható. A programséma változtatása vagy módosítása (pl. a csapok átállítása vagy a bütykök cseréje) egy vagy több mozgási tengelyen csak mechanikai műveletek révén történik.
    d) Nem szervo vezérlésű, sorrend manipulációs mechanizmusok, amelyek mechanikusan rögzített, programozott mozgások szerint működő automatizált mozgó eszközök. A program változtatható, de a folyamat csak a mechanikusan rögzített elektromos bináris eszközről vagy állítható ütközőkről kapott bináris jel hatására halad tovább.
    e) Descartes-féle koordináta manipulátor rendszerként definiált rakodódaruk, amelyeket függőleges elhelyezett tároló rekeszek integrált részeként alakítottak ki, és e rekeszek tartalmának tárolás és kirakodás céljából történő elérésére szolgálnak."[32]

A fenti definíciókból az a következtetés vonható le, hogy a robot nagyságrendekkel összetettebb, mint egy közlekedési lámpa, ugyanakkor az emberi (jogi) elhatározás végrehajtása szempontjából alanyként attól semmiben sem különbözik, ugyanolyan eszköze annak, pusztán több és összetettebb feladatok megoldására is képessé tehető. Ebből adódik az is, hogy egy olyan roboton, amely képes egy elfogás végrehajtására olyan eszközt értünk, amely az elfogással adódó összes munkát, a kényszerítéstől a szállításon át az adminisztrációig, képes elvégezni. Itt következik az újabb kérdés, ami egyszerűségében maga a bonyodalom: Lehetséges ez?

TECHNIKAI MEGVALÓSÍTÁS

Egy rendőrhatósági jogkörrel felhatalmazott robottól elvárhatjuk, hogy legalábbis elérje egy emberi jogalkalmazó képességeit, képes legyen önálló eljárásra, a megfigyelés, azonosítás, interakció, kényszerítés nagy hatásfokú végrehajtására. A robot helyes működéséhez így szükséges nagy mennyiségű és részletességű, különböző spektrumokban üzemelő műszer, az azok által biztosított adatok analizálására alkalmas feldolgozóegység, az analizált adatok alapján a gyanúsnak minősített, körözött, vagy éppen jogsértő viselkedést folytató személyek környezettől való elkülönítése, adatbázis alapján azonosítása, a helyes eljárás kiválasztása és sikeres végrehajtása.

Habár a teljes funkcionalitással rendelkező, tökéletes robotrendőr jelenleg távoli jövőnek tűnhet, a hozzá vezető lépések tisztán láthatóak. Az első feladat a humán jogalkalmazó számára

olyan technika biztosítása, melyet csupán hordozni és felügyelni kell. Amit már most is megtehetünk, hogy a járőröket kamerákkal, mikrofonokkal látjuk el, műszeres arzenáljukat infrás és lézeres eszközökkel egészítjük ki, az adatokat pedig valamely számítógépen, például okostelefonon rögzítjük, mely azonnal el is kezdi az elemzést és kiértékelést. Létező technika a digitális arc- és hangfelismerés, melyeket használva kellően finom műszerekkel akár nagy távolságból is lehetséges érdeklődésre számot tartó személyeket kiválasztani, a gyanúsnak tűnő vagy jogsértőként tetten ért személy teljes biometrikus azonosításához pedig alkalmazható ultrahangos ujjlenyomat-letapogató vagy például retinaszkenner. Az azonosítás terén jelentős mennyiségű tapasztalatot eredményeznek a világ legforgalmasabb repülőterein üzembe helyezett automata határátléptető rendszerek, melynek eredményeként a személyazonosítási technológiák napról napra pontosabbak.

Második feladat annak biztosítása, hogy a műszerek által szolgáltatott adatokat a helyszínen és valós időben, automatikusan kielemezzük, humán beavatkozás nélkül egyértelműen eldönthető legyen, folyamatban van-e jogsértés, szükséges-e közbeavatkozás, eljárás. Ehhez szükséges egy nagy teljesítményű, hordozható számítógép és azon futtatott szakértői rendszer, mesterséges intelligencia. A fennálló helyzet pontos elemzése és azonosítása után a kapcsolódó adatbázisból egyértelműen kiválasztható, milyen intézkedést kell foganatosítani. Ennél a pontnál a felszerelést hordozó hivatalos személy válláról már a mérlegelés és felelősség terhét is levettük, egyetlen megmaradt feladata nem más, mint részvétel az intézkedés szakszerű végrehajtásában.

Így harmadik és egyben utolsó feladatunk nem más, mint egy olyan robottest megalkotása és üzemeltetése, mely képes a műszereit és központi számítógépét hordozni, majd az automatizált döntés után az előírt kényszerítést végrehajtani.

A műszerezettség kérdése a legegyszerűbb, minden említett technika létezik, ezek napi alkalmazása egyszerűen azért nem történt még meg, mert a műszerek mérete, energiaszükséglete és ára még nem áll arányban szükségességükkel és hasznosságukkal, ám a technikai fejlődés és miniatürizáció megállíthatatlan, így kényszerűen el fogunk érkezni egy olyan határponthoz, amikor már egyszerűbb és olcsóbb egy ingzsebnyi eszközbe belezsúfolni egy jelenleg csúcstechnikás megfigyelő furgon tartalmát és így megspórolni akár egyetlen tanú beidézését.

Az alkalmas robottest megalkotásában ígéretes fejlesztések zajlanak, jelenleg a DARPA [33] versenyeztet különböző kutatócsapatokat, feladatuk egy titánból, acélból és alumíniumból alkotott, emberszerű robottest vezérlőszoftverének kifejlesztése.[34] Például az Atlas lépegető robot, felépítése alkalmassá teszi guggolásra, mászásra, lépcsőn futásra, ugrásra. A fejlesztés végén a robot alkalmas lesz radioaktív romok közül embereket menteni, ahonnan már csak egyetlen apró lépés egy ellenállást tanúsító bűnöző üldözése, földre kényszerítése és megbilincselése.

Legnehezebben kivitelezhető feladatunk tehát az, hogy miután megalkottuk az ideális robottestet, mely strapabíró, emberfeletti érzékszervekkel rendelkezik és mozgását hibátlan gyári szoftverek vezérlik, azaz idealizált robotrendőrünk fizikai valójában megfelel minden elvárásnak, ebből a szempontból sikeresen helyettesít, sőt lepipál minden humán rendőrt, megadjuk azt, ami ezt a testet uralja, az agyat, a központi számítógépet, a mesterséges intelligenciát, melyet a továbbiakban MI-nek nevezünk. Egy rendvédelmi pályát választó személy kiképzésben részesül, munkája során tapasztal, tanul és fejlődik, döntései során támaszkodik korábbi élményeire, tanulmányaira. Egy rendvédelmi feladatra szánt robot csak kevésben hasonlít, és nagyon sokban különbözik egy természetes személytől. Egy újonc robotból hiányzik 20 év élettapasztalat, erkölcs és morál, szokások és normák. Nincs intuíció, sejtés, asszociatív megértés, definiálni kell a magyarázatot magyarázó magyarázat minden apró elemét. Empátiás érzéke nulla, kognitív és predikciós képességei nem léteznek. Nincs esélye észrevenni, ha valaki hazudik, szimulál, tettet.

Ugyanakkor nagy szerencsénkre az újszülött robot problémáját elég egyszer elszenvedni. Helyzetfelismeréshez részben átemelhetőek a különböző biztonságtechnikai szoftverek, melyek képesek tárgyak, tüzek és füst azonosítására, elemzésére, ütközésgátló radarok, automata kapuk, forgalomirányító rendszerek szoftverfejlesztésében gyűjtött tapasztalatok és eredmények alapján objektummodellezéssel megalkotható egy részletes és kiterjedt fogalomtár, mely segítségével az MI nem csupán érzékeli, de nagymértékben érti is az őt körülvevő környezetet, nem csupán elszenvedője, de aktív formálója is lehet az eseményeknek. Az MI nem felejt, valaha megszerzett tudását képes bármikor, azonnal, hibátlanul előhívni. Amit egy robotnak sikeresen megtanítunk, azt a többi robot is azonnal és teljes mértékben elsajátítja egy központi adatbázison keresztül, ami hibát egy robot elkövet, azt a következő másodpercben már egyetlen másik sem fogja. Gyakorlatilag tehát egyetlen robotot kell megalkotnunk, kiképeznünk és letesztelnünk majd rendszeresen képeznünk ahhoz, hogy bármilyen mennyiségű robotot ugyanazzal a tudással lássunk el. Ez a multiplikációs képesség hihetetlen rugalmasságot és alkalmazkodási készséget képes biztosítani még egy olyan nagy szervezetnek is, mint a rendőrség.

A rendvédelmi MI és annak képzése leginkább úgy képzelhető el, hogy a való világot beláthatóan részletes és az érthetőséghez kellőképpen apró elemekre modellezzük le, számtalan példán keresztül megtanítjuk az MI-t kategorizálni, az ellenőrző kérdések során lelt ellentmondásokat figyelembe véve gondosan finomítjuk a modellt. Egy kérdéses szituáció pontos azonosításához priorizáljuk a bejövő paraméterek fontosságát, hatását, a különböző döntések kimeneteinek jóságát, heurisztikus mintaillesztéssel keressük a jelenlegihez leginkább hasonlító, az adatbázisban már szereplő esetet, attól különböző döntés esetén pedig új kategóriával bővítjük az adatbázist. Habár Gödel (első) nemteljességi tétele alapján nincs esélyünk tökéletes MI-t kinevelni,[35] nem készíthetjük fel minden, csak kellően sok esetre, hatékonysága minden egyes esettel javul, minden jogszabályi változásra azonnal és tökéletesen reagál, mindig és mindenki pontosan tudhatja, adott helyzetben mire számíthat a robot részéről. A robotot nem lehet megvesztegetni, provokálni, megfélemlíteni, lefegyverezni, zsarolni, nem megy szabadságra, nyugdíjba, nem fárad el, döntéseit nem befolyásolja szeszély, hangulat, megbízhatóságát nem szükséges megkérdőjelezni.

LEGFONTOSABB PROBLÉMÁK

Mint látható, sem a jogi alkalmazhatóság, sem a technikai megvalósítás nem lehetetlen, csupán idő és erőforrás ráfordításának kérdése. Ugyanakkor elkerülhetetlenül szükséges előre azonosítani azokat a buktatókat, amelyekre kiemelt figyelmet kell fordítani már a fejlesztés elején.

Elsőként le kell szögeznünk, hogy a robotnak tudnia kell ugyanazt, amit – ideális esetben – az elfogás során, minden rendőr biztosítani tud, azaz garantálni, hogy:

- a megfelelő személyt,
- csak a törvényes feltételek fennállása esetén,
- arányos erőt alkalmazva fogja el.

Persze – Gödel első nemteljességi tételére visszautalva – ennek száz százalékos biztosítása lehetetlen, de ugyanakkor ez a szám megközelíthető. A valódi kérdés az, képesek-e ezen a területen a robotok ugyanúgy vagy jobban teljesíteni, mint a rendőrök, nagyobb garanciát jelent-e a törvényes és tisztességes elbánásra, ha az elfogásban robotot is alkalmaznak. A kutatás során itt objektív célszámokat is képesek vagyunk meghatározni akkor, ha tudjuk, milyen arányban intézkednek „hibásan” a hús-vér rendőrök. Ehhez a Független Rendvédelmi Panasztestület egymást követő három évben készült beszámolóit dolgoztuk fel, azért választva ezt az időintervallumot, mert 2008 előtt még erőteljesen befolyásolták a mutatókat a 2006-os

események, a 2010 utáni ügyek pedig nincsenek mind lezárva, több ügyben még nincs jogerős bírósági döntés. A Független Rendészeti Panasztestület beszámolója szerint:

- 2008. évben elfogás és előállítás miatt 40 panasz érkezett, ebből 30 esetben megállapították az alapjogsértést.[36]
- 2009. évben elfogás és előállítás miatt 80 panasz érkezett, ebből 36 esetben történt alapjogsértés.[37]
- 2010. évben elfogás és előállítás miatt 201 panasz érkezett, 21 esetben állapították meg, hogy a panasz alapos.[38]

Ha figyelembe vesszük a napi átlagban 350 előállítást és csak ezt vetítjük az alapjogsérelmek arányára, akkor azt mondhatjuk, a rendőrök az intézkedéseik 99,98 százalékát megfelelően hajtják végre, azaz a fentebb felsorolt feltételek teljesülnek. Ez az a célszám, amit a robotoknak is stabilan nyújtaniuk kell, azzal együtt, hogy mivel szándékunk szerint a robotok minden intézkedést kép- és hangfelvétellel dokumentálnak majd, e téren a magasra becsült látencia minden bizonnyal csökkenni fog.

Egy ilyen eredményt csak megfelelő megoldások alkalmazásával lehet egy robotnál elérni, ilyenek például:

- A nagy biztonságú berendezéseknél alkalmazott megoldások (pl. szavaztatás) átvétele.
- Megfelelően hitelesített programozás.
- Szigorú minőségbiztosítási rendszer.
- Nagyfokú üzembiztonság (safety and security).
- Hatékony tanulási képesség.
- Ember-robot járőrpár.

A fentiek közül a legnagyobb kihívást az utolsó két pont jelenti. Hiszen az első négy pontban – elsősorban a vasúti és a légi közlekedés biztonsága területén – már számos eredmény született. Biztonsági berendezéseknél számos publikáció található úgy a logikai (programozási) [39] kérdésekre, mint a technikai megoldásokra [40] és gyakorlati tapasztalataikra [41] vonatkozóan. Minőségbiztosítási rendszer tekintetében természetesen kiindulási alap kell, hogy legyen az ISO 8373 és 10218 szabványok illetve az ISO 9000 szabványcsomag alkalmazása, azokon a területeken pedig ahol még nincsenek nemzeti szabványok, mint például a szoftver-minőségbiztosításnál, ott a kialakult szakmai szabályokat kell figyelembe venni,[42] illetve szükség esetén új szabványokat kidolgozni és benyújtani. Az üzembiztonság területén pedig szintén számos kötelező szabvány van érvényben [43] melyek alkalmazása alól csak indokolt esetben ajánlatos – ugyanakkor szükséges - felmenteni az elfogás végrehajtására szánt robotokat, illetve nagy valószínűséggel ezen a területen is néhány új szabvány kidolgozása is szükséges ahhoz, hogy az eszközök rendszerbe állíthatóak legyenek. Elérkeztünk a két utolsó ponthoz, amelyekről egyébként a technikai megvalósítás során már szót ejtettünk, hatékony tanulási képességhez és az ember-robot járőrpárhoz. Az MI tanulási képességeinek kialakítására vonatkozóan már viszonylag kiforrott elméleti alapok állnak rendelkezésre, melyek köszönhetően számos tanulási modellt ötvözhetünk, bár néhányakat, mint például az MI „kísérletezésén” alapuló megerősítéses tanulási módszert csak szigorú korlátok között szabad alkalmazni ezen a területen.[44] Sokkal komolyabb kihívás, egyben lehetőség az ember-robot járőrpár alkalmazása, mely során az a robot gyakorlatilag úgy viselkedik, mint egy elnyűhetetlen, beszélő szolgálati kutya, engedelmesen követi a járőrvezetőt (gazdát), kiterjeszti érzékelését és tudását, figyelmezteti, segíti és védelmezi, miközben folyamatosan tanul. Jelenleg egy robot elfogásra történő alkalmazását pontosan ebben a szerepkörben szándékozzuk megvalósítani, továbblépés szerintünk csak e lépcső elérése után lehetséges – amennyiben szükséges.

ÖSSZEGZÉS

A tanulmányban leírtakat összegezve tehát megállapítható:

- jelenleg robot önállóan elfogás intézkedést Magyarországon nem alkalmazhat, mert az elfogás intézkedések foganatosítására a rendvédelmi szervek hivatalos személyei jogosultak, de eszközként történő alkalmazását a rendőrségi törvény lehetővé teszi,
- a robotot önálló elfogás végrehajtására feljogosítani a robotot alkalmazó rendvédelmi szerv tevékenységét szabályozó törvényben kell, az Alaptörvényt módosítani nem szükséges,
- önmagában jogdogmatikai akadálya a robot elfogásra történő alkalmazásának nincs, már számos példa működik hazánkban és a világon arra, hogy személyes szabadságot korlátozó hatású tevékenységét valamely gép vagy berendezés fejtsen ki, akár emberi beavatkozás nélkül is,
- a technikai megvalósítás több lépcsőben lehetséges, elsőként segédeszközként, majd járőrtársként lesznek alkalmazhatóak a robotok, végül, ha szükséges, akkor az önálló intézkedési képesség is megvalósítható, szigorú biztonsági és minőségi követelmények mellett.

Felhasznált irodalom

[1] 1994. évi XXXIV. törvény a Rendőrségről (Rtv.) 33. § (1) bekezdés. Időbeli hatály: 2014. január 2. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=21269.208645 Letöltés ideje: 2014. január 2.

[2] http://www.police.hu/search/node/orsz%C3%A1gos%20%C3%B6sszes%C3%ADt%C5%91 Letöltés ideje: 2014. január 02.

[3] Magyarország Alaptörvénye (2011. április 25.), Szabadság és Felelősség fejezet, [római] IV. cikk. Időbeli hatály: 2013. december 18. Forrás: http://njt.hu/cgi_bin/njt_doc.cgi?docid=140968.248458 Letöltés ideje: 2013. december 18.

[4] Ellen M. Purdy: The Increasing Role of Robots in National Security. In: Defense AT&L, 2008. május-június, XLII. évf. (2008) 5-6. szám, p. 26-29., ISSN: 1547-5476

[5] http://www.darpa.mil/Our_Work/TTO/Programs/DARPA_Robotics_Challenge.aspx

[6] Isaac Asimov et al: Asimov teljes Alapítvány-Birodalom-Robot Univerzuma, I-XX. kötet, Szeged, 2003, Szukits Könyvkiadó, ISBN: 963-944-157-0. Fordította: Baranyi Gyula

[7] Jakab András: A szocializmus jogdogmatikai hagyatékának néhány eleméről. In: Iustum Acquum Salutare, III. évf. (2007) 1. szám, p. 189-214., ISSN: 1787-3223 (bár Jakab András következetesen alkalmatlannak tartja az életviszony, illetve a társadalmi viszony kifejezés alkalmazását a jogviszony definiálására, ugyanakkor tanulmányában – célszerűségi okból – e kifejezéseket használja a jogágak meghatározásakor)

[8] Búza László: A közjog és a magánjog fogalmi elhatárolásának kérdése. In: Az Erdélyi Múzeum Egyesület Jog- Közgazdaság- és Társadalomtudományi Szakosztályának Értekezései. I. évf. (1943), 2. szám, Kolozsvár, 1943. ISSN: -

[9] PARÁDI József et al. (szerk.): A magyar rendvédelem története. Budapest, 19962, Osiris. ISBN 963-047-958-3

[10] Magyarország Alaptörvénye (2011. április 25.) (a továbbiakban: Alaptörvény), I. és VI. [római 1-es és 4-es] cikk, a megismételt eljáráskor hatályos jogszabály: http://njt.hu/cgi_bin/njt_doc.cgi?docid=140968.205404, tanulmány elkészítésekor hatályos jogszabály: http://njt.hu/cgi_bin/njt_doc.cgi?docid=140968.248458 Letöltés ideje: 2013.11.17

[11] Alaptörvény T) cikk (3) bekezdés, 15. [arab 15-ös] cikk (4) bekezdés, 18. [arab 18-as] cikk (3) bekezdés

[12] Magyarországon a rendőrséget az általános rendőrségi feladatok ellátására létrehozott szerv, a belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerv, valamint a terrorizmust elhárító szerv alkotja. Rtv. 4. § (2) bekezdés.

[13] Idem. 1. sz. jegyzet

[14] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (Nbsz. tv.) 32. § Időbeli hatály: 2014. január 4. http://njt.hu/cgi_bin/njt_doc.cgi?docid=24361.254644 Letöltés ideje: 2014. január 4.

[15] 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról (Nav. tv.) 36. § (1) bekezdés g) pont. Időbeli hatály: 2014. január 4. http://njt.hu/cgi_bin/njt_doc.cgi?docid=132692.243562 Letöltés ideje: 2014. január 4.

[16] 2012. évi XXXVI. törvény az Országgyűlésről (Ogy. tv.) 139. § (1) bekezdés. Időbeli hatály: 2014. január 4. http://njt.hu/cgi_bin/njt_doc.cgi?docid=148174.253168 Letöltés ideje: 2014. január 4.

[17] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Szvr. tv.) 27. § Időbeli hatály: 2014. január 4. http://njt.hu/cgi_bin/njt_doc.cgi?docid=95492.245525 Letöltés ideje: 2014. január 4.

[18] Rtv. 26 .§ (1) bekezdés, 50. § (3) bekezdés b) pont, 51. §, 54. §,

[19] Vö. Rtv. 26. (1) bekezdés § és 49. §

[20] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről (Bv. tv.) 21. § (3) bekezdés b) pontja. Időbeli hatály: 2014. január 4. http://njt.hu/cgi_bin/njt_doc.cgi?docid=24246.245102 Letöltés ideje: 2014. január 4.

[21] Dobossy László: Karel Čapek. In: Irodalomtörténeti kiskönyvtár, Budapest, 1961, Gondolat Kvk., pp. 98. ISBN: -

[22] Frank Herbert – Kevin J. Anderson: A Butleri Dzsihad. In: A Dűne. Szeged, 2003, Szukits Könyvkiadó, p. 1-9., ISBN 963-497-007-9. Mohácsi Enikő fordítása.

[23] Verein Deutschen Ingenieure [Német Mérnökök Egyesülete]

[24] http://www.vdi.de/technik/richtlinien/richtliniendetails/?cHash=7516ede3ae00e37148abce98cc47426a&tx_wmdbvdirilisearch_pi1%5Bsuid%5D=90416

[25] Lásd. Pintér József: Ipari robotok. Előadás. 2010.

[26] Dömösi et al.: Formális nyelvek és automaták. Jegyzet. Nyíregyháza, 2011, Nyíregyházi Főiskola.

[27] Hans-Georg Gadamer: A jogi hermeneutika példaszerű jelentősége. In: Igazság és módszer, Budapest, 2003, Oziris, pp. 696, p. 361 – 379., ISBN: 978-963-389-213-8. Fordította: Bonyhád Gábor.

[28] Idem 1. sz. jegyzet.

[29] Az Oxford Dictionary angol értelmező kéziszótár „robot” fogalom-meghatározásának szerző általi fordítása. Eredetit lásd: „robot” - Oxford English Dictionary, Oxford, 2013, Oxford University Press. ISBN: 978-019-861-186-8, Online verzió. http://www.oxforddictionaries.com, Letöltés ideje: 2014. január 4.

[30] International Standardization Organisation [Nemzetközi Szabványosítási Szervezet]

[31] ISO 8373:2012 2.4 pont, a szerző fordítása.

[32] Az Európai Parlament és a Tanács 388/2012/EU rendelete (2012. április 19.) a kettős felhasználású termékek kivitelére, transzferjére, brókertevékenységére és tranzitjára vonatkozó közösségi ellenőrzési rendszer kialakításáról szóló 428/2009/EK tanácsi rendelet módosításáról, I. számú melléklet. Hivatalos Lap L 129, 16/05/2012 p. 0012 – 0280. Brüsszel, 2012, Európai Bizottság, ISSN 1977-0677. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:129:0012:01:HU:HTML Letöltés ideje: 2014. január 2.

[33] Defense Advanced Research Projects Agency [Fejlett Védelmi Kutatási Projektek Ügynöksége]

[34] http://www.theroboticschallenge.org

[35] „Minden ellentmondásmentes, a természetes számok elméletét tartalmazó, formális-axiomatikus elméletben megfogalmazható olyan mondat, mely se nem bizonyítható, se nem cáfolható.” Raymond Smullyan: Gödel nemteljességi tételei. In: A logika világa, Budapest, 1991, Typotex, pp. 150., ISBN 978-963-9548-98-5. Fordította: Csaba Ferenc

[36] A Független Rendészeti Panasztestület beszámolója a 2008. évi tapasztalatairól. Jelentés. Budapest, 2009, Független Rendészeti Panasztestület, 55-72. p. http://www.panasztestulet.hu/files/2008_tajekoztato.pdf Letöltés ideje: 2013.11.18

[37] A Független Rendészeti Panasztestület beszámolója a 2009. évi tapasztalatairól. Jelentés. Budapest, 2010, Független Rendészeti Panasztestület, 77-97. p. http://www.panasztestulet.hu/files/2009_tajekoztato.pdf Letöltés ideje: 2013.11.18

[38] A Független Rendészeti Panasztestület beszámolója a 2010. évi tapasztalatairól. Jelentés. Budapest, 2010, Független Rendészeti Panasztestület, 77-97. p. http://www.panasztestulet.hu/files/2009_tajekoztato.pdf Letöltés ideje: 2013.11.18

[39] Székely Béla: Biztosítóberendezési függőségek számítógépes tervezése. In: Vezetékek Világa – Magyar Vasúttechnikai Szemle. XV. évf. (2010) 1. szám, ISSN 1416-1656, p. 12-16.

[40] Makkay et al.: Robotrepülőgépek redundáns rendszerei. In: Repüléstudományi Közlemények. XXIV. évf. (2012) 2. szám, ISSN 1789-770X, p. 909-919.

[41] Walter Fuß: Electronisches Stw im Löstchberg-Basistunnel [Elektronikus biztosítóberendezés (Thales Elektra) a Lötschberg bázisalagútban]. In: Vezetékek Világa – Magyar Vasúttechnikai Szemle. XV. évf. (2010) 1. szám, ISSN 1416-1656, p. 17-20.

[42] Sziray-Benyó-Heckenast: Szoftver-minőségbiztosítás. Jegyzet. Győr, 2007, Széchenyi István Egyetem. pp. 132. Forrás: http://109.74.55.19/tananyag/tananyagok/Jegyzetek/Szoftver-minosegbiztositas.pdf, Letöltés ideje: 2014. január 12.

[43] Lásd: Nemzeti Foglalkoztatási Szolgálat Nemzeti Munkaügyi Hivatal 2012/58-01/Ú sz. Munkavédelmi Módszertani Útmutatója A Hatósági Gyakorlat Szempontjából Jelentőséggel Bíró, Munkavédelmi Szakterületet Érintő Szabványismeretekről és Követelményekről. Budapest, 2012, Nemzeti Foglalkoztatási Szolgálat, pp. 21. Forrás: http://www.mvkepviselo.hu/szabvanyok/2013/2012-58-01mnh.pdf, Letöltés ideje: 2014. január 12.

[44] Russel - Norvig: Artificial intelligence. A modern approach. [Mesterséges Intelligencia Modern Megközelítésben] Prentice Hall, Upper Saddle River, New Jersey, 07458, USA, 20032, Pearson Edication Inc. ISBN 013-790-395-2, Magyar fordítás: Édelkraut et al: Mesterséges Intelligencia Modern Megközelítésben, Budapest, 2005, Panem Könyvkiadó. Forrás: Mesterséges Intelligencia Elektronikus Almanach, http://project.mit.bme.hu/mi_almanach/books/aima/index Letöltés ideje: 2014. január 12.