HADMÉRNÖK

Katonai műszaki tudományok
on-line

XII. évf. 1. szám - 2017. március

A szerkesztőség / Editorial office:

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

Kiadó / Publisher :

Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
National University of Public Service; Faculty of Military Science and Officer Training

ISSN 1788-1919

Jelen számban megjelent írások szerzői / Authors of the Current Issue:

Benye János – Komárom-Esztergom Megyei Katasztrófavédelmi Igazgatóság, Pv. felügyelő

Dobor József Dr. – Nemzeti Közszolgálati Egyetem, KVI, adjunktus

Pátzay György Prof. Dr. – Nemzeti Közszolgálati Egyetem, KVI, egyetemi tanár

Kossa György – INTER TAN-KER Zrt.

Földesi Krisztina – Óbudai Egyetem, BDI doktorandusz

Kovács Tibor Dr. habil. – Óbudai Egyetem, BGK, egyetemi docens

Ganbadrakh Tsend-Ayush – Nemzeti Közszolgálati Egyetem, HDI doktorandusz

Gávay György – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz

Tóth Bence Dr. – Nemzeti Közszolgálati Egyetem, HHK, adjunktus

Gerevich János – Nemzeti Közszolgálati Egyetem, HDI doktorandusz

Hegedűs Hajnalka – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz

Hornyacsek Júlia Dr. – Nemzeti Közszolgálati Egyetem, KVKI, egyetemi docens

Jobbágy Szabolcs - Nemzeti Közszolgálati Egyetem, HDI doktorandusz

Kátai-Urbán Irina – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz

Kovács László Prof. Dr. – Nemzeti Közszolgálati Egyetem, HHK, egyetemi tanár

Kun István Dr. – Nemzeti Közszolgálati Egyetem ÁKK, főiskolai tanár

Kuti Rajmund Dr. – Széchenyi István Egyetem, egyetemi docens

Laposa Tamás – Nemzeti Közszolgálati Egyetem, KDI doktorandusz

Major Zsolt – Óbudai Egyetem, BDI doktorandusz

Molnár Dóra Dr. – Nemzeti Közszolgálati Egyetem, NETK, egyetemi docens

Mesics Zoltán – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz

Pántya Péter Dr. – Nemzeti Közszolgálati Egyetem, KVI, adjunktus

Puskás Béla – Óbudai Egyetem, BDI doktorandusz

Solymosi Máté – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz

Horváth Kristóf – OAH, Általános Nukleáris Főigazgató-helyettes

Vincze Árpád – OAH, Főosztályvezető

Vass Gyula – BM OKF, Szolgálat vezető

Szűcs Endre Dr. – Óbudai Egyetem, BGK, adjunktus

Szakali Miklós

Temesvári Zsolt Marcell – Óbudai Egyetem, BDI doktorandusz

Maros Dóra Dr. – Óbudai egyetem, KVK egyetemi docens

Jakus Attila

Tick Andrea Dr. – Budapesti Gazdasági Egyetem, KKK, egyetemi docens

TARTALOMJEGYZÉK

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

ATTITUDE CHANGE TOWARDS BIOMETRY BETWEEN 2006 AND 2016

A BIOMEMTRIÁVAL KAPCSOLATOS ATTITÜDVÁLTOZÁS 2006 ÉS 2016 KÖZÖTT

FÖLDESI Krisztina; KOVÁCS Tibor

(ORCID: 0000-0001-5867-9958); (ORCID: 0000-0001-7609-9287)

foldesik@fejer.police.hu; kovacs.tibor@bgk.uni-obuda.hu

Abstract

Utilisation of technical novelties is continuous within the police organisation to make the police work more reliable. An example of this is the personal identification based on fingerprints, which was first used in law enforcement. The ongoing development of biometry, the use of 21st century technical novelties in police activity would mean further support in making the police work more efficient and high-standard. The only question is: what methods and control mechanisms will society accept, and to what extent the police force itself will support and accept the general use of these methods and mechanisms. This work contains the analysis of two studies and multiple investigations aimed at answering this question.

Keywords: *safety and security, identification, personal identification, biometry, fingerprint, police*

Absztrakt

A rendőri munka megbízhatóbbá tételének érdekében a technikai újítások alkalmazása a rendőri szervezeten belül folyamatos. Ilyen például az ujjnyomat alapján történő személyazonosítás, amelynek elsőszámú felhasználási területe a rendészet volt. A biometria szakterületének további fejlődése, a XXI. századi technikai nóvumok felhasználása a rendőrségi területen további támogatást jelentene a rendőri munka hatékonyabbá, színvonalasabbá tételében. A kérdés csupán az, hogy milyen módszerek, és milyen ellenőrzési mechanizmusok alkalmazását fogadja el a társadalom, és maga a rendőri állomány milyen mértékben támogatja, fogadja el azok általános alkalmazását. E kérdés megválaszolására lefolytatott két kutatásés több vizsgálat, elemzés összegzését tartalmazza e munka.

Kulcsszavak: *biztonság, azonosítás, személyazonosítás, biometria, ujjnyomat, rendőrség*

A kézirat benyújtásának dátuma (Date of submission): 2017.02.14.
A kézirat elfogadásának dátuma (Date of acceptance): 2017.03.08.

INTRODUCTION

Biometric procedures gain more and more ground also in the modern, application oriented technical scene. This is the situation in both the private and the public security sector. To determine the utilisation practice and developmental directions of biometric devices, it is crucial to study what changes occurred in the societal acceptance. The significance of biometrics based personal identification has particularly grown in the second millennia. The COUNCIL REGULATION (EC) No 2252/2004 of the European Union (adopted in December 2004) orders the Member States to include biometric identification information into the concerned documents, after the adoption of common technical and security requirements. In its commission decision from 28 June 2006, the EU determined the common requirements of second generation passports containing digitalised fingerprints. Furthermore, the EU also determined a deadline for implementation: 36 months. The European Union supported the development also through financial means, Hungary received close to HUF1 billion for this cause, thus starting June 28 2009, all passports issued contain fingerprints as well. The borderless nature and fear inducing characteristic of International terrorism and crime play a role in this [1]. In the course of crime investigations, we face countless new threats, and methods of perpetration, which supersede the opportunities provided by traditional investigation techniques and security systems. And after 9/11, a whole new era of safety and security began. From that time on, biometric data has been claimed to be the only and categoric method for establishing public safety and security. It is regarding this topic we conducted our research in the 2006-2016 period.

COMPARATIVE STOCHASTIC ANALYSIS OF RESEARCH RESULTS FROM 2006 AND 2014 CONCERNING AVERSIONS TOWARDS BIOMETRIC IDENTIFICATION [4]

A frequent point in social sciences is that whether in a base population providing different samples, the value of a variable X is generally the same in the groups providing the samples. Because in such cases we are working with quantitative variables the value range of which only meets the criteria of ordinality. We get such a variable for example, if we ask the test subject to judge on a scale of 1 to 5, how much s/he supports the practical usage of a procedure. And according to some people's approach, the comparison of size levels in such a case using the average is ambiguous, and the results are questionable. It is this problem, to which the method of stochastic comparison provides a solution. Concerning a variable X, stochastic equality can be defined between two populations if $P(X1>X2)=P(X1<X2)$ is true, i.e. X1 and X2 from the two populations are the result of two observations chosen randomly, and independent from one another. Basic concepts here are stochastic equation (StE) and stochastic homogeneity (StH). Thus, through the generalisation of these, we can determine the stochastic compliance of more than two base populations.

In order to concretise these processes, we performed a comparison of the research projects completed in this field: both of them had been conducted at the University of Óbuda. The 2006 study was done at the predecessor in title, Budapest Technical College, Donát Bánki Faculty of Mechanical Engineering, Institute of Mechanical Structure and Security Technology, Security Technology Lab [2], and we personally conducted the 2014 study at the Doctoral School of Security Sciences [3], and involved security sciences majors as well as professional police officers.

Due to the societal background at the time of the 2006 research, the utilisation of biometric identification technology was considered relatively new. A largely incomplete legislative background, smaller technological repertoire, less practical experience in usage, but large installation and operation cost were to be expected in application. Based on the operation in

the professional field of the last 8 years, we can make statements of great significance concerning professional work as well. The 2006 research sample involved 59 people, which increased to 333 in 2014. To have the most nuanced conclusions possible and to get more solid results, we had created another control group composed of police officers beside the students, inevitable for the objective assessment of the situation. In the indicated period, 153 police officers from the Fejér County Police Department filled in the questionnaire (with the base population counting 924 police officers on duty). Student respondent count was 180.

Both researches presented a custom made questionnaire, which was filled in voluntarily and anonymously. In both instances, the questionnaire contained closed, attitude measuring questions to determine the sentiments in question.

To enhance the objectivity of the results and to clarify eventual cognitive dissonances, we integrated four questions requiring essay-like answers into the 2014 research. (60 students detailed their opinion on four questions of the questionnaire, with the help of which we gained accurate information on the value indicated in the attitude range).

One of the central topics of the studies was: which emotional and mental attitudes are triggered in users by the use of biometric systems?

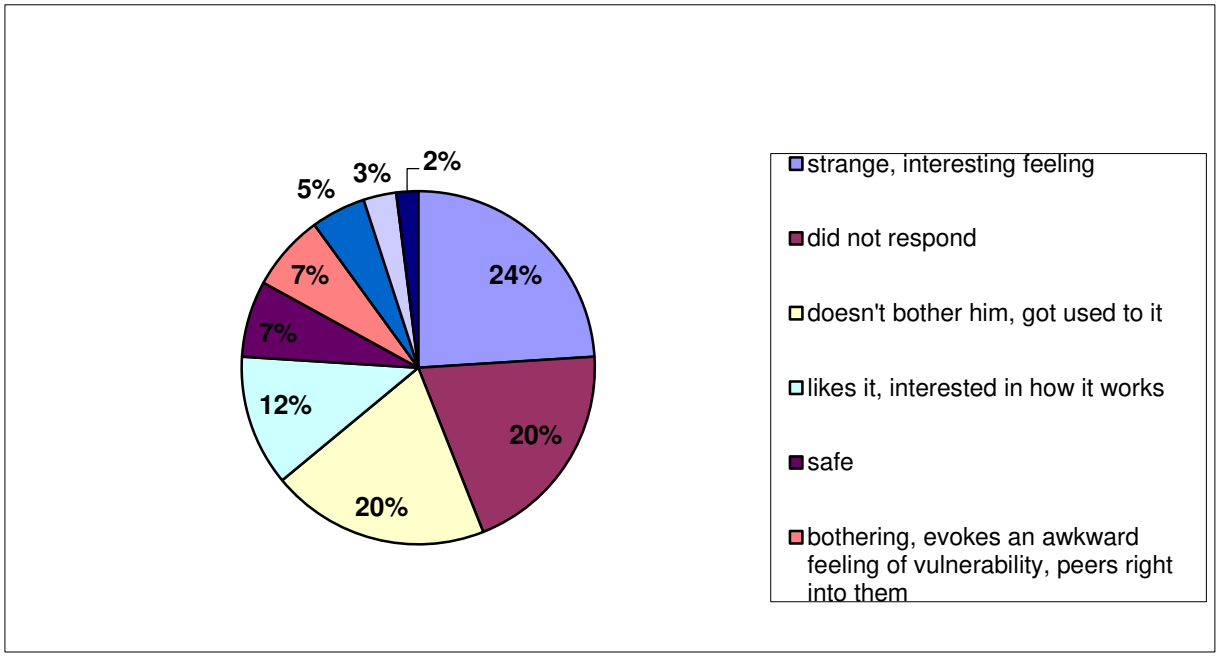


Figure 1 Emotional and Mental Attitudes Towards Access Control Systems (source: SUPLICZ, S. - FÜZI, B., 2006. [2])

According to the analysis of the 2006 source (**Figure 1**) 70% had a positive, accepting attitude, 20% did not answer, and 10% had a disapproving opinion due to bad feelings or slowness.

Relating to the usage of the biometric system, the results of the 2006 research showed 71% of all respondents stating that they fully trust the biometric system, and support its application (**Figure 2**).

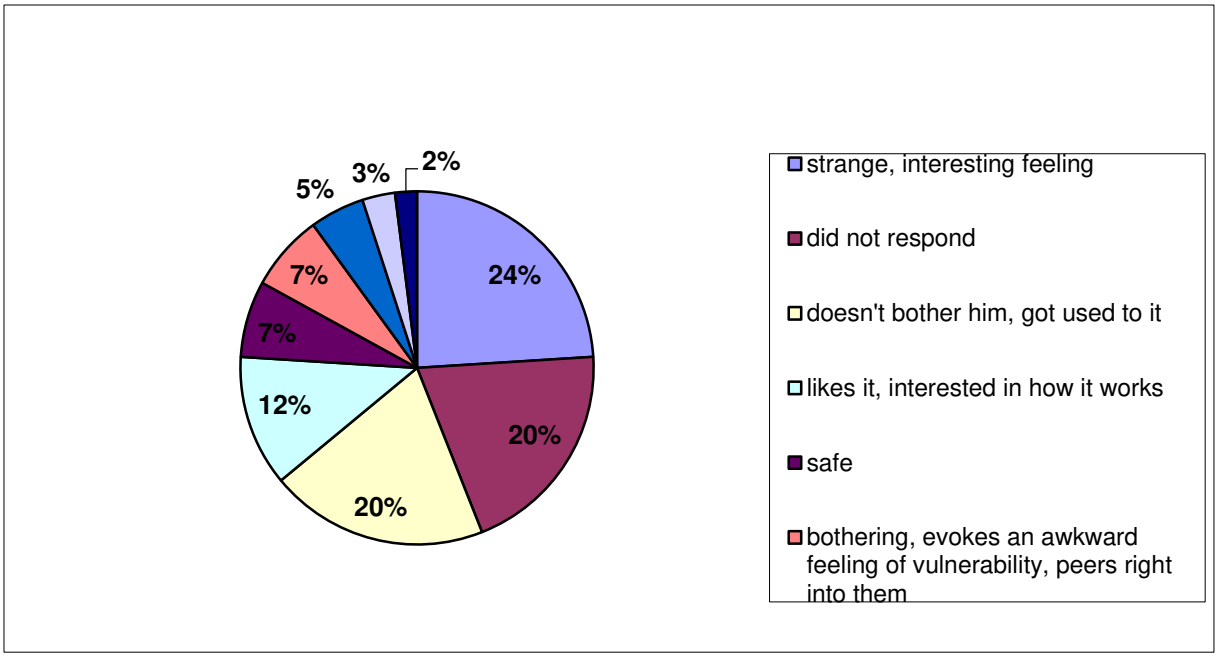


Figure 2 Attitude towards the use of the biometric identification system (source: SUPLICZ, S. - FÜZI, B., 2006. [2])

A significant conclusion is that only 2% out of the 7% being averse were expressly rejecting the system. The above results allude to the great popularity of the product, since even a lot of those gave an accepting answer, who were concerned about the system from a privacy protection or emotional point of view. All these could be considered as very good results concerning a new system used for the first time.

It was this question to which a point in the 2014 research intended to find an answer for, namely, to what extent do the respondents support the introduction of biometry based systems. Since the age composition of the police force shows 55% in the 18-35 range, it is important to weigh the opinion of this age group in a proper manner (**Figure 3**).

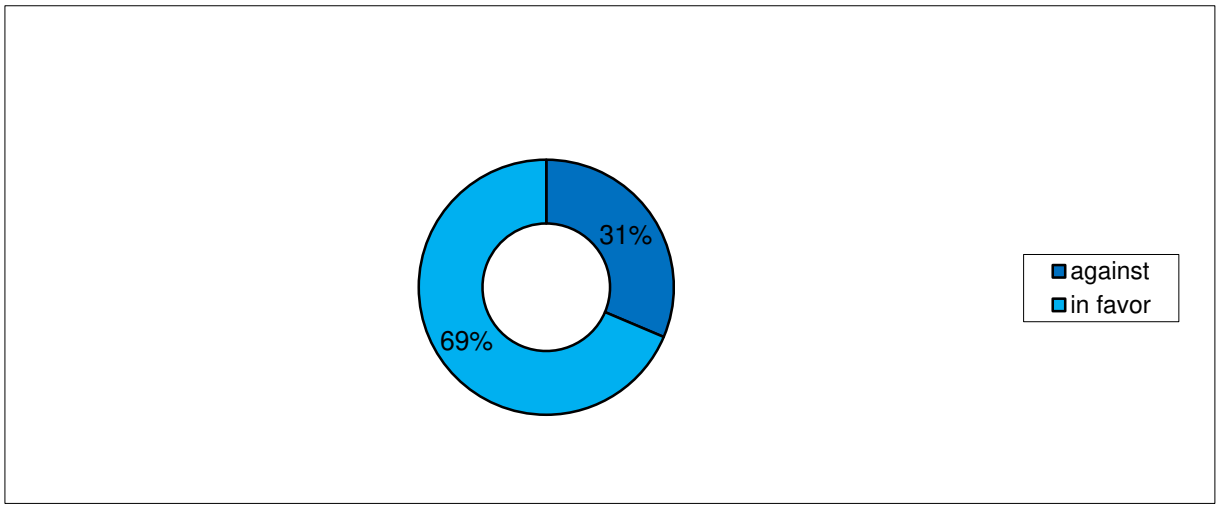


Figure 3 Attitude of police officers 18-35 years of age towards biometry.

It immediately became clear that not only did the 2006 results fail to become more positive and accepting in the eight years passed, but they turned fully rejective towards biometry considering that 31% of police officers is against the application of biometric identification procedures. This result is articulated even more by the fact that such high proportion of

rejection appears in a social group, where the application of certain components is job duty, and the eye-catching results of the efficient operation of these technologies are clearly visible.

The outcome of the survey conducted among university students unambiguously supports the above statement (**Figure 4**).

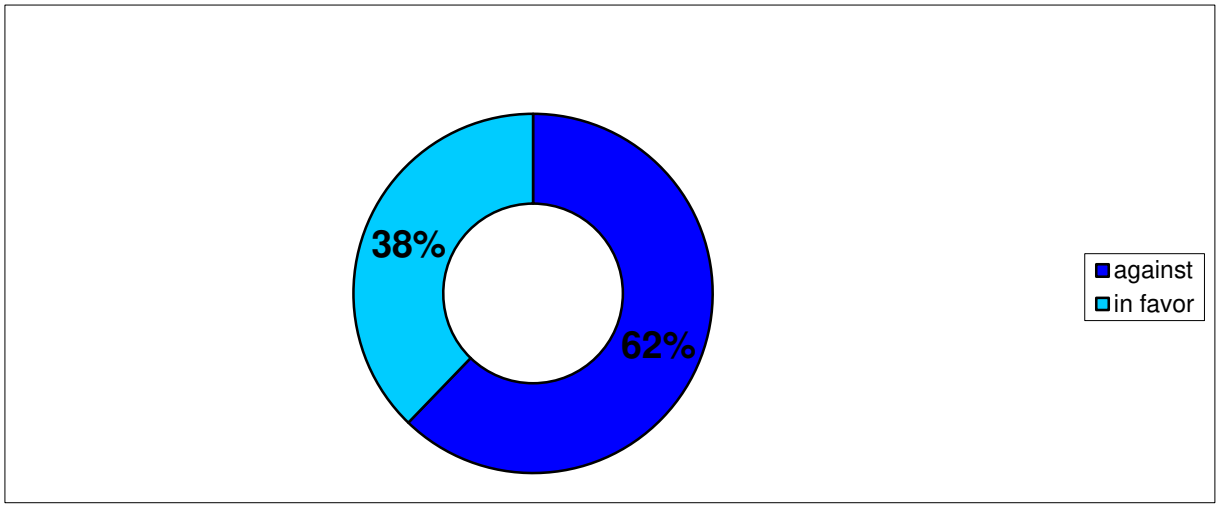


Figure 4 Attitude of university students towards general capture of biometric data.

Concerning the common aversion towards biometric device system, 62% of the respondents from university population unequivocally rejects these, and absolutely disagrees with the general scope, all-inclusive usage of these. Thus, it can be ascertained that the university population is in total rejection towards any kind of control, rule and checking.

Sixty of the students from the University of Óbuda, Donát Bánki Faculty of Mechanical Engineering and Security Technology left a detailed essay-like opinion concerning the statements 1 to 4 of the questionnaire (see further down). Formation of opinions was conducted in groups of six. Based on these, we received a more nuanced and, in a way, altered result concerning the above question.

They first examined the question of the universally required electronic fingerprint registry. From the ten groups formed, five groups supported it with conditions, and five groups categorically dismissed the possibility of a universal fingerprint registry. Then again, if we look at the detailed answers, we see that nine groups would not support the establishment of this. This fact seemed, as a matter of fact, to verify the statement that university students reject any manifestation of control on themselves, although the 69% measured in the questionnaires produced 90% here.

Analysing the justifications however, I ascertained that in many cases rejection appears for merely technical reasons. Since in their studies university students concern all forms of biometric identification in detail and thoroughly, they are also aware of the technical background of these. They also clearly see the incompleteness of the different procedures.

To the question of what level of knowledge do you have concerning biometry, I received answers from the professional police officers in the 2014 research refuting my hypothesis. Because I assumed that they possess far more knowledge than average people regarding biometry (**Figure 5**).

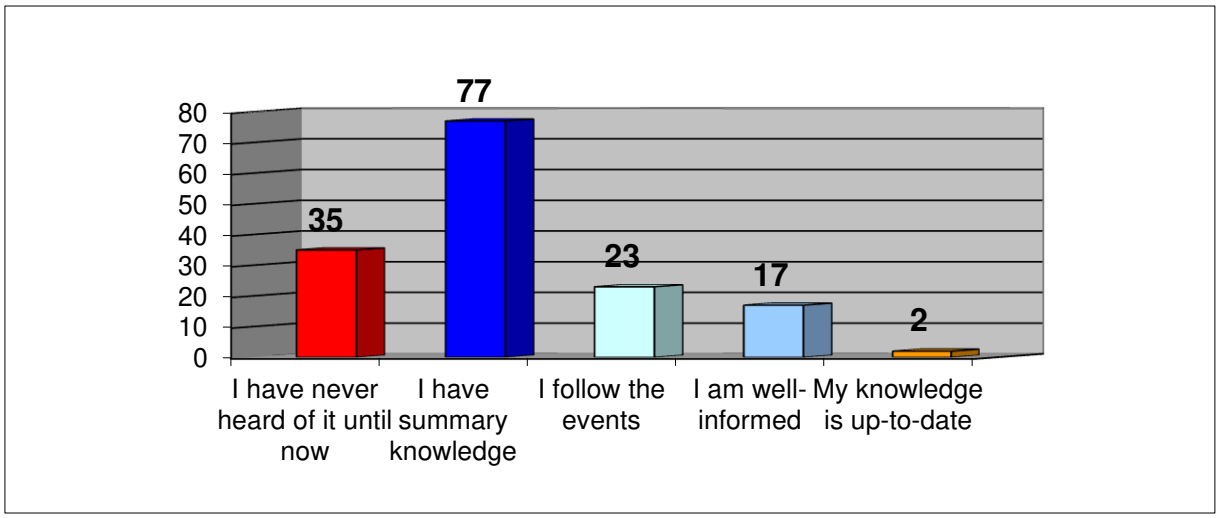


Figure 5 Knowledge level of the Fejér County Police Department police force regarding biometry.

23% of respondents did not even hear of biometry until now, and according to themselves do not have any knowledge concerning this discipline. The largest portion of police officers, 49% stated that they only have summary knowledge in this field. It is also a big problem that only 2% of the 153 respondents claimed to be well-informed in this topic. This fact is also thought-provoking because dactyloscopy, face recognition, and DNA-identification constitute an integral part of police force's basic education, and if the police force with an occupational duty to deal with biometry possesses such little knowledge in this field than the knowledge proportion amongst civilian population is even lower.

The knowledge level of university students involved in the 2014 research proved to be much higher (**Figure 6**).

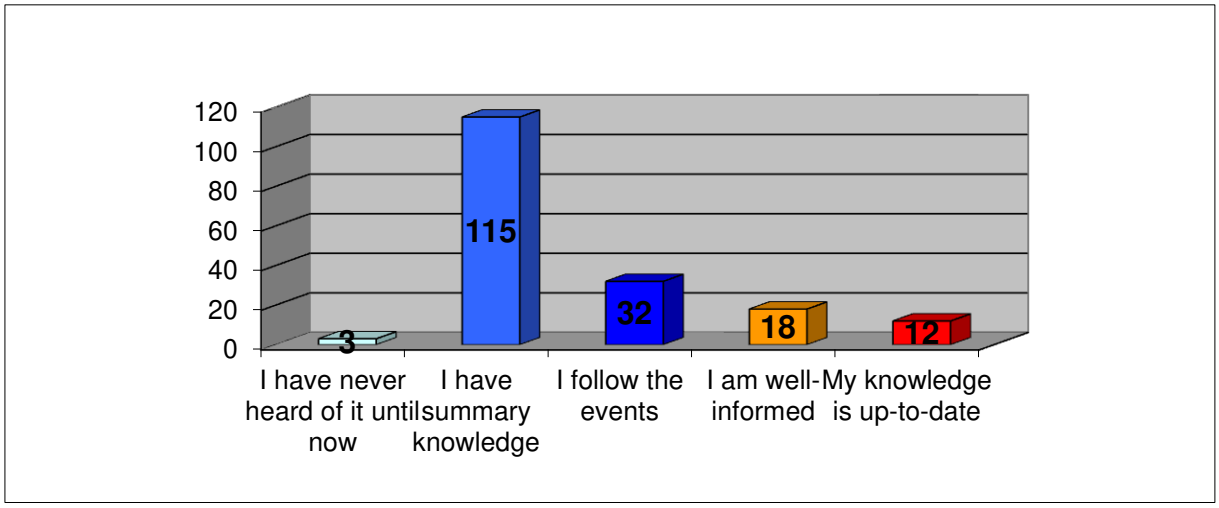


Figure 6: Prior knowledge of university students regarding biometry.

30% of respondents stated that not only are they well-informed and are following the events in the world of biometry, but their knowledge is up-to-date. This is understandable, since they are Security Technology majors. Then again, the remaining 70% of "specialists" having only summary knowledge is an unexpectedly high proportion.

Examining the 8 years passed between the two studies, based on the above, it can be ascertained that no progress was made in improving society's knowledge level regarding biometric identification. In 2006, 31% answered that they did not have any substantial

information on iris identification / biometric identification, the remaining 69% also only possessed filtered information, incomplete knowledge. In 2014, the proportion of those not able to even explain what biometry is was 23% among police officers, and 49% only had very minimal knowledge in this field. That is, 71% of police officers did not know anything about biometric identification. The 30% knowledge level of university population can also not be considered an advancement, with the other 70% producing only summary knowledge.

The low knowledge level of the population providing the samples also has a major effect on other issues relevant to this field, and on the development of attitudes towards these issues. Evidence to this is presented in the justifications provided by the university students; e.g. in the second essay point, which was focused on the willingness to support the recording of iris recognition data of new-borns after delivery. Basically, the groups unequivocally stated that they agree with the application of this biometric identification method. However, they only agreed considering its reliability. A face recognition system is capable of sending a signal based on the criminal records, if a person wanted or only monitored by the police enters the district. Practically, it is able to connect to population registry data, where beside our personal data, our digitalised photos are kept as well. Thus, anyone possessing such a professional system can monitor the chosen individual – who, of course, may or may not be a criminal –; i.e. where, when, with whom and why s/he goes, what habits, illnesses, phobia etc. s/he has. Therefore, the technology itself is capable to create anyone's personality profile, which is clearly prohibited by numerous international treaties and regulations (e.g. Council of Europe regulation [5]). This system using a face recognition software is already part of Hungarian reality [6]: The Ministry of Interior installs camera systems using face recognition software in a HUF12 billion project and the National Security Service (NSS). The media and journalists, together with multiple human rights organisations termed this initiative a “cheeky face recognition” and the term “Orwell-land” was used in connection with it [7]. In their opinion, 1984 of our nightmares seems to be coming true, the possibility of the almighty “Big Brother”, who sees all, who treats all ordinary people as subordinates, uses and exploits them according to its own interests.

Beside all of the above, we have to remark that a strong influence of the media was palpable in the case of students, namely the effect of numerous series on television portraying police investigation, and mustering techniques of securing evidence. Even in the population well-versed in this topic, these resulted in events of imagination. Regarding fingerprints, four groups remarked that they do not really support the universal capture of these because it is data easy to steel, and the fingerprint of an innocent person, or a fraction of it, can easily be placed in a crime scene, in order to have that person identified as the perpetrator.

The third statement concerned the establishment of a face recognition database, in order to monitor the movement of criminals in public places. Six groups elaborated in their opinion that they completely disagree with this proposal. The first and foremost reason for their decision was the unreliable nature of this method. Secondly, they argued that because this lack of reliability, a lot of false positive identifications would occur, through which honest people would be accused of crimes. There was a group that rejected the method referring to personal rights once again, since also people would be monitored, who only walk by the camera accidentally, and so their data could be manipulated.

THE QUESTIONNAIRE

Respondent's Sex: Male Female

Respondent's Age: below 18 18 – 35 years 36 – 55 years 56 and above

Respondent's Highest Degree: Primary School High School Higher Education

Please read the following statements, and using the grades below indicate how much you agree or disagree with them.

1	2	3	4	5
Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree

1.	**I support the expansion of electronic fingerprint registry to all men and women.**	**1**	**2**	**3**	**4**	**5**
2.	**I agree with collection and retention of iris recognition data of every child at birth by the police.**	**1**	**2**	**3**	**4**	**5**
3.	**I agree with the establishment of a face recognition-arrest warrant database, with the help of which monitoring of faces involved in crimes becomes possible.**	**1**	**2**	**3**	**4**	**5**
4.	**I agree with the police registering the DNA-sample, fingerprints and face recognition data of abusers (sexual abuse of children) and people committing deliberate homicide.**	**1**	**2**	**3**	**4**	**5**
5.	**I agree with the police registering further biometric data (DNA, iris, vein pattern, etc.) of any person committing any deliberate crime, on top of their fingerprints.**	**1**	**2**	**3**	**4**	**5**
6.	**I do not support the DNA-sample registration of every child at birth.**	**1**	**2**	**3**	**4**	**5**
7.	**I support the face recognition and police registration of people committing robbery and other crimes against property.**	**1**	**2**	**3**	**4**	**5**

EFFECT OF A SUCCESSFUL APPLICATION ON ACCEPTANCE

Beside theoretical education, the University of Óbuda, Donát Bánki Faculty of Mechanical Engineering and Security Technology puts great emphasis on armouring students with as much practical experience as possible. In this effort, a hybrid access control system (biometric ID and chip) was established on the Campus in Népszínház Street, and has been operated by the school for multiple years. Following technological developments, there are new components introduced to the system from time to time, complementing, or in some cases, replacing the former technology used.

The system was installed in 2010 with the purpose of providing access control based purely on biometrics. However, the fingerprint reader crashed after capturing 1,000 users, despite the fact that the manufacturer's device specifications indicated handling of 10,000 samples (the total number of users is around 4,500). After some thorough examinations, the professional leadership decided to limit the fingerprint-based access control to 400 people, and to meet further access control needs using chips.

In 2015, we decided to replace the fingerprint recognition device with the palm vein recognition (“vein scanner”) system used in the Groupama Arena, which by then had outgrown its minor initial flaws. The developer was also very keen on providing us with two

devices, because in the school building, there's a constant strain on the device, while in the stadium it is “floodlike”, and so, gathering information of day-to-day use becomes possible.

The device accepting 500 users quickly became popular, since it answered a lot quicker than the former fingerprint recognition device (the pass-through time practically became comparable with that of the chip method), it worked with low levels of false rejections (around 1%), and it is quite comfortable if one does not need to grope around or go back for the access card, etc.

In 2016, we purchased licenses for another 700 people, thus our biometric access control capacity rose to 1,200 users. Although, based on our continuous assessments, the false rejection rate increased slightly, but this could be traced to application error in practically all cases (mostly, it was wrong positioning of the palm on the detector). The popularity, feasibility, and ultimately, the acceptance of this biometric identification method is shown by the fact that we managed to fill the user limit on a strictly voluntary base in a matter of a few days.

SUMMARY

As a conclusion, we can state that there are still some questions left regarding the practical applicability of biometric identification systems. Numerous misbeliefs, legends and false notions are distorting people's opinion concerning this. It is unfortunate that public opinion is often based on incorrect information from the wrong source, as a consequence of which their perspective evolves in the wrong direction, and the results of the two studies have shown the aftermath of this fact in a palpable way by demonstrating that during the eight years passed, members of society had not received appropriate information concerning biometry. This resulted in knowledge deficiency and uncertainty, and ultimately, in aversion and fear towards the use of biometric devices.

The most important component in this aspect is the use of correct terminology, conveying accurate information, and public disclosure of newest technology, in order for the larger public to have an accurate and precise idea of the current technical opportunities an capabilities of biometric identification.

It can be ascertained as a basic fact, that today many have already heard about the concept of biometry, however, its set of tools, and potential uses remained unknown to them. Our finding that, according to themselves, 23% of the people serving in law enforcement never even heard of biometric devices renders this topic especially sensitive. Another 49% has only summary knowledge of biometry. Their knowledge is summary, incomplete, however, this knowledge evokes fear and distress. The ongoing specialisation, and perfectioning of biometric devices, and also the expansion of utilisation areas are not followed by the information need, and information processing of those concerned. They might very well know of certain new biometric devices, but they fail to comprehend the practical applicability of them. A particularly sensitive point of this system is the field of law enforcement, where personal identification based on biometric features would render the subjective element of performing personal identification for the purpose of law enforcement in a traditional way – based on anatomic features containing high probability of error – controlled.

The fact that more than one-fifth of police officers had not even heard of biometry questions also the efficacy of police’s basic training. Since an organic part of it is learning the elements, steps and basic concepts of dactyloscopy, face recognition and DNA-identification.

However, half knowledge in this topic serves only fear mongering and spreading hysteria, where in sci-fi like everyday life, the chosen ones hold biometry-based personal observation in their grasp, and play with individuals like with puppets.

In can be ascertained that individuals have a great need for safety and security, even if it means a minor curtailment of their freedom. In this regard, police officers have more

categorical, unambiguous opinion on biometric devices, which they see applicable in a more stringent manner and in a wider range than university students. In the end, also when taking all seven questions into consideration, it can be stated that the opinion and attitude of the police force is completely unequivocal, not influenced by the respondent's sex: all possible and already developed area and device of biometry is deployable and to be deployed in fighting crime, and the creation of public safety and security.

Based on our research and examinations, it could be confirmed that the need for safety and security is a relevant issue in all age categories, on all levels of education and both sexes. Then again, immense anomalies can be observed in the applicability of biometry. There is a consensus on the necessity of its application in registering and identifying criminals. Then again, the rejection observed in other cases, to a great extent, may be traced back to knowledge deficiencies. Thus, spreading more thorough and reliable information to a wider audience, and the precise, professional and all-encompassing creation of legal framework are primary tasks.

Tasks to improve the acceptance of biometric identification

Comparing the result of studies, examinations and analyses, it can be stated as a fact that the acceptance of technologies using biometric data was becoming worse in society up until the recent years. Being aware that the base population providing the sample is the user of these techniques, is familiar with them, and would be interested in a more successful application of theses in his/her everyday work, this result is even more significant. Then again, the 38-31% rejection rate compared to the 2% from 2006 makes it clear that the professional forums, practical work and information spreading in this field are not sufficient, misinformation and disinformation may occur, and forums conveying reliable, relevant information, technical specifications and innovations in a credible manner are completely missing. These forums – organized and working on a professional basis – will have a basic task split into four segments:

1. It is clearly necessary to immediately rectify and correct false information, which is entirely missing regarding this discipline.
2. The next element in public relation activities is making the outward communication of the discipline credible, professional and unified.
3. Missing harmonisation of law on an international level must be performed, subsequently, the legal framework of uncontrolled, excessively controlled or not properly controlled areas must be created and adopted.
4. Fourth, but indispensable task is to narrow the scope of the discipline, and to make it professional, in the course of which all “charlatans” doing unprofessional and technically insufficient work are done away with from the circle of professional teams installing biometric identification access control systems. This activity, of course, can only be done through elected professional bodies comprising credible individuals.

Independent from the criminal statistics, it is also a societal expectation and the need of people irrespective the type of settlement they live in, to be able to live their everyday life peacefully, free of crime, knowing that their children and they themselves are safe and secure. Also in the course of the European Union's law making and framework creating activity, public safety had been declared, and was worded in the Amsterdam Treaty adopted on 2 October 1997, and effective as of 1 May 1999. They defined creation of an area of “Freedom, Security and Justice” as the central objective (neither the Maastricht Treaty, nor the Amsterdam Treaty provided a definition for the area of freedom, security and justice).

The Fundamental Law of Hungary itself also enunciates this basic right [8]. Then again, it is important that we have a precise idea of the level of freedom society is willing to sacrifice in order to make everyday life more secure. Of course, we also have to be aware of the conclusions that biometric identification is not a "silver bullet", as many claimed it to be, e.g. in the fight against terrorism, or in crime prevention, but it surely needs to have a much more relevant role in creating public and private safety, in the implementation of which the largest responsibility falls on the professionals of this discipline.

BIBLIOGRAPHY

[1] http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/HU/index.htm; letöltve: 21 June 2012

[2] SUPLICZ, S. - FÜZI, B.: Study of Attitudes and Aversive Reactions Evoked by an Access Control System Using Iris Identification, a treatise, Budapest Technical College, Donát Bánki Faculty of Mechanical Engineering, Institute of Mechanical Structure and Security Technology, 2002

[3] FÖLDESI, K. - KOVÁCS, T.: Study of Aversions Towards Biometry among Police Officers and University Students, a treatise, University of Óbuda, Doctoral School of Security Sciences, 2014

[4] VARGHA, A.: Comparison of Independent Samples Through New Ranking Procedures http://www.ksh.hu/statszemle_archive/2002/2002_04/2002_04_328.pdf; downloaded: 01 December 2013

[5] Munkaanyag a biometriáról - Working document on biometrics Adopted on 1st August 2003 by ARTICLE 29 - Data Protection Working Party MARKT/10595/03/EN, WP 80 www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf

[6] http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/HU/index.htm; downloaded: 12 October 2014

[7] www.jozsefvaros.hu/hir/1965/kocsis_mate_a_biztonsag_mellett_tette_le_a_voksat/; downloaded: 02 October 2014

[8] Fundamental Law of Hungary, *Article IV* "(1) Everyone shall have the right to liberty and security of the person."

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

THE CONTROLLING ANALYSIS OF THE GOODS PROTECTION SESTEM IN AN OPERATING DEPARTMENT STORE

EGY MŰKÖDŐ ÁRUHÁZ ÁRUVÉDELMI RENDSZERÉNEK KONTROLLING VIZSGÁLATA

MAJOR Zsolt; KOVÁCS Tibor

(0000-0003-0123-6376); (0000-0001-7609-9287)

majorzsolt1976@gmail.com; kovacs.tibor@bgk.uni-obuda.hu

Abstract

Over the past ten years I have spent in this field, I have seen the application of several systems of property protection. Each and every security system should guarantee protection and security, including the maximization of the protection of property. In the majority of the case studies I experienced that the controlling aspect of the protection systems was wanting in one respect or another. However, controlling is an indispensable part of the protection plan. The protection of property project is a complex activity touching upon all segments of security. Controlling includes the description of mechanical and financial parameters and the framing of the temporal and financial parameters of the project realization. It is necessary to have a continuous feedback on operation once the project is devised and launched. The assessment of experiences based on feedback and the development of the controlling system is a never-ending process. We can never sit back and relax thinking that our system runs perfectly since the development of technology always calls for new challenges.

Keywords: *protection, goods, department, controlling system, theft*

Absztrakt

A szakmában eltöltött több mint tíz évem alatt sokféle vagyonvédelmi rendszer alkalmazásával találkoztam. A védelem és biztonság szavatolása, az értékek maximális biztosítása a feladata valamennyi biztonsági rendszernek. Az esettanulmányok döntő többségénél a védelmi rendszer kontrolling szemléletének hiányosságát tapasztaltam. A kontrolling kihagyhatatlan részét képezi a védelmi terv kialakításának.. A vagyonvédelmi projekt egy komplex, valamennyi biztonsággal kapcsolatos szegmenst érintő tevékenység. A kialakítása sajátságos és egyszeri tevékenység. A kontrolling tartalma a műszaki és a pénzügyi paraméterek leírása, a megvalósítás időbeli és financiális paramétereinek keretbe foglalása. Az összeállítást és elindítást követően szükségünk van a működésről egy folyamatos visszacsatolásra. A visszacsatolásokból eredő tapasztalatok leszűrése és a kontrolling rendszer fejlesztése egy soha véget nem érő folyamat. Soha nem dőlhetünk hátra megnyugtatóan, hogy tökéletes a rendszerünk, hiszen a technika fejlődésével újabb kihívások adódnak.

Kulcsszavak: *védelem, termékek, üzlet, kontrolling rendszer, lopás*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.31.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.02.

BEVEZETÉS

The purpose of goods protection with respect to the department store. The companies launch entreprises covering their activities in order to produce profit. Owners quantify their expectations and define the numbers necessary for the operation of their venture. In order that the business management live up to these numbers, the rules of economy have to be observed. Each and every forint invested has its place within the system and it has to come back within a given time frame. In the case of goods protection, it is rather difficult to accurately determine the time of return as not all items equipped with goods protection tools will be attempted to be stolen. If we knew which products would be stolen, it would be necessary to equip only those ones. With regard to this segment, controlling systems offer two solutions.

The design of department stores aims at the complete satisfaction of customer interest. Modern approaches profess the view that the goods should be placed as close to the customer's reach as possible. On the one hand, experiencing the physical parameters of the product generates trade. On the other hand, it facilitates the execution of harmful activities by those who enter the store without any intention of shopping. Unfortunately, my experience is that most Contractors regard it as a waste of money to acquire technical tools and devices ensuring goods protection, let alone to employ people controlling them. It is for this reason that I consider it important to keep the qualification level of the staff at the highest possible.

The protection system needs constant updating, and changes in technology have to be closely followed. Developments integrated into our existing system have to be based on the principles of controlling.

Several actors are affected by a positive outcome:

- Owners, business managers: profit and profitability
- Employees: higher salary, better work atmosphere
- Customers: although unconscious on their part, but a feeling a security will draw in more customers. The return shows not only in the inventory, but is has a positive effect related to trade in general as well.

FACTORS NEGATIVELY AFFECTING GOODS PROPERTY

Only a fraction of these negative events will actually be noticed. It is therefore of vital importance that these events be recorded in greater numbers, in accordance with what really happened. These pieces of information can be compared to a floating iceberg: it is through the accurate documentation of past events that we can analyze the quality of protection efficiently and change measures productively. These measures are crucial in the domain of both prevention and intervention. Employees have to be made aware of the importance of sharing detailed information related to department store happenings. The relevance of this point is twofold, qualitative and quantitative, both being essential.

- *Qualitative*: referring to the fact that the quality and usability of the information are determined by the informator's abilities.
- *Quantitative*: referring to the fact that information should be to our disposition in as great amount as possible; the broader the spectrum of experiences, the more effective the development.

MEASURING RISKS

What external and internal factors lead to the disappearance of the product.

Theft from the outside

The individual thief comes as a visitor and may actually buy something, but all their activities within the building are subjugated to the theft. The person executes the deed on their own.
Persons committing group theft come as visitors and may, in some cases, actually buy something. They divide the subtasks of the theft among one and another. Each person has a well-defined role: observer, distractor, preparator and supplier.
As the proverb says, a thief is born by occasion. It is always an opportunity that incites theft, the opportunity being the lack of security, about which I am going to write later on.

The thief who arrives as a regular client has previously selected the item that would make the object of theft. This person takes advantage of every single opportunity to reach the goal, and takes no interest in any other product. A significant number of black market actors acquire their stock using this strategy.

Theft from the inside

The employee seizes the opportunity and steals the product. When done individually, there is an increased probability of being caught. The employees form a group and do their deed together so as to decrease the risk of being caught – the group form facilitates the spotting of the right time and place.

Sources of danger generated by the product:

- the commercial behavior of the department store, flaws in sale;
- flaws in the retail trade appearance or in the packaging of the product;
- flaws in the professional competence of the sales contributors;
- intentional damage done by the employees and
- unintentional faults done by the employees.

Following the analysis of case studies drawn from practice, I have concluded that it is not possible to make a 100% estimation of the target areas, the volume, the time and the consequences of the near-future target events. At the same time, we can prepare for the harmful effects by solution plans and protection strategies.

The scope of RISK Management

It includes those areas where commands related to risk management enter into interaction with one and another.

Reception of goods: the arrival of products, the nature of work procedures: qualitative and quantitative controlling, entering the department store in the stock registry. The items can arrive directly from the manufacturer, from the central stock of the store or from another store. Installing goods protection devices of the goods not equipped with appropriate protection in the factory.

Internal logistics of the department store: transporting groups of goods to the right department, taking care of the packaging, checking goods protection devices.

Departments: placing into the selling area and in the trade system by taking commercial aspects into account.

Selling:

- Cash register zone, shopping through the cash register zone, traditional self-service.

- Handing out products, when the quantity or any other factor justifies selling though the reception gate. No goods can leave the area of the department store without control.
- The area in front of the department store, advertising activities: model products exposed in this area with the aim of increasing trade can be considered potential risk factors. The amount of source spent on protecting them is determined by the forensic status of the area.

The tools we have to reach our goals

What developments we wish to foster, which cost money and which cost energy and time.[1]

- A camera system available, the optimal setting of the department store area covered. The parameters of the cameras available. Taking the shelves into consideration.
- Goods protection devices available,
- Mechanical protection: devices that can prevent or burden theft even without electricity. Locks, chains, cabinets, display cases and combinations of these.
- Acousto-magnetic goods protection devices: devices using electro-magnetism that prevent or burden the theft of goods. The item is equipped with a device that signals at the detector gate.
- Goods protection safes;
- Secure spiders, special design for the appropriate placing on the packaging.
- Hardtags, goods protection tags put on the item, cannot be easily eliminated.
- Softtags, can be easily placed on the product, difficult to detect.

Elements of goods protection controlling

Factors that have a negative effect on the operation of goods protection controlling

Factors influencing human activities:

- queuing;
- the employees have to wait without any tasks to do;
- unnecessary work, empty time;
- errors;
- harmful effects not signaled in advance;
- inappropriate working conditions;
- erroneous communication.
- Elements necessary for a successful controlling:
- Declaring a joint will from the very beginning;
- The effect of management activities, directions, tasks and activities related to management. Mission (from where to where you want to get), value system, dominant atmosphere within the company, the internal working environment of the organization, decision-making.
- The management and its structure, principles, organizational structure, system of relations.
- Co-operation with partners;
- Managing human resources, determining staff size, distributing tasks, formation, development, determining levels of knowledge, operating a system of rewards.
- Process perspective, harmonizing resources related to shared activities, controlling processes, continuous development, monitoring, increasing efficiency and productivity.
- System perspective, identifying processes in interaction, learning about them, understanding them, integrating them into the system and controlling.

- Equipment system, determining tasks necessary for reaching the goals, execution, controlling.
- Principles of arrangement, planning, controlling, developing, maintaining.

The primary function of these devices is to ensure appropriate information for the management about the conditions of the environment and the internal processes, with the aim of planning and introducing the necessary interventions and defining appropriateness. The management is able to control the processes it has launched. The controlling leader's task is to ensure the set goals.[1]

Good protection controlling

- Specifying goods protection aims, minimizing expenses, maximizing security;
- Setting specific goods protection goals;
- Collection information relevant to goods protection, analyzing and interpreting it;
- Working out a function monitoring efficiency.

Tools for goods protection

- Measures: regulations controlling internal organizational processes, concerning individuals coming from the outside;
- Architectural design, plan of commercial arrangement;
- Goods protection system;
- Electronic goods protection devices;
- Mechanical goods protection devices.

The first figure demonstrate of the tools for goods protection

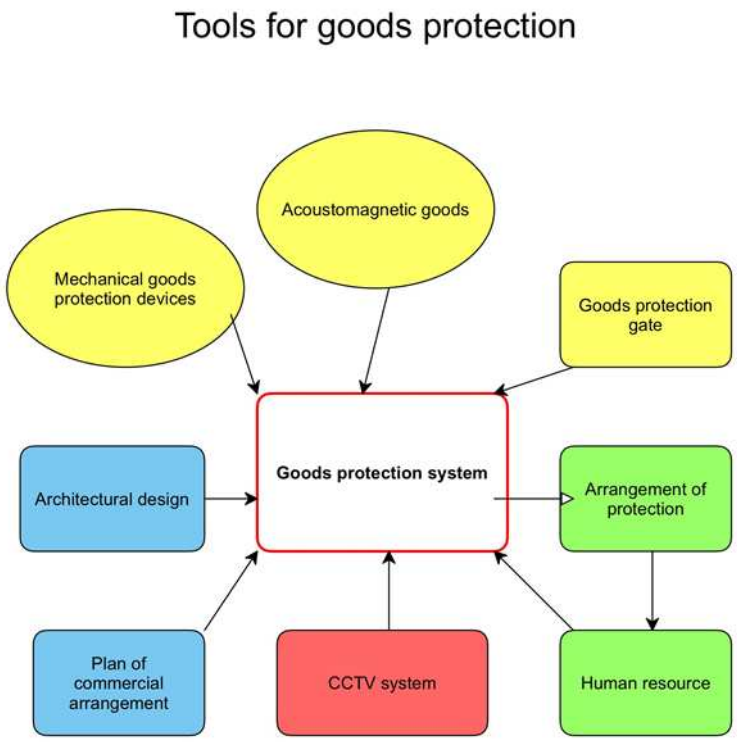


Fig.1: Tools for goods protection (edited by the author)

For a successful goods protection controlling [1]

- Introducing the indicator function which can predict harmful action in an early phase;
- Preventive effect to avoid the actual realization of the harmful action, creating a situation which can reduce its probability to the greatest degree possible;
- Flow of information, as quick and accurate as possible;
- A goal-oriented approach to processes, we always have to be aware of the purpose of each and every process;
- Setting aims in order to define future tasks with a view of reaching our clear goals.

Elements of the goods protection controlling system [2]

- Understanding the elements of goods protection
- Working out a goods protection plan
- Putting the plans in practice
- Measuring performance
- Comparing performance
- Assessing performance
- Development

The second figure demonstrate of the controlling goods protection

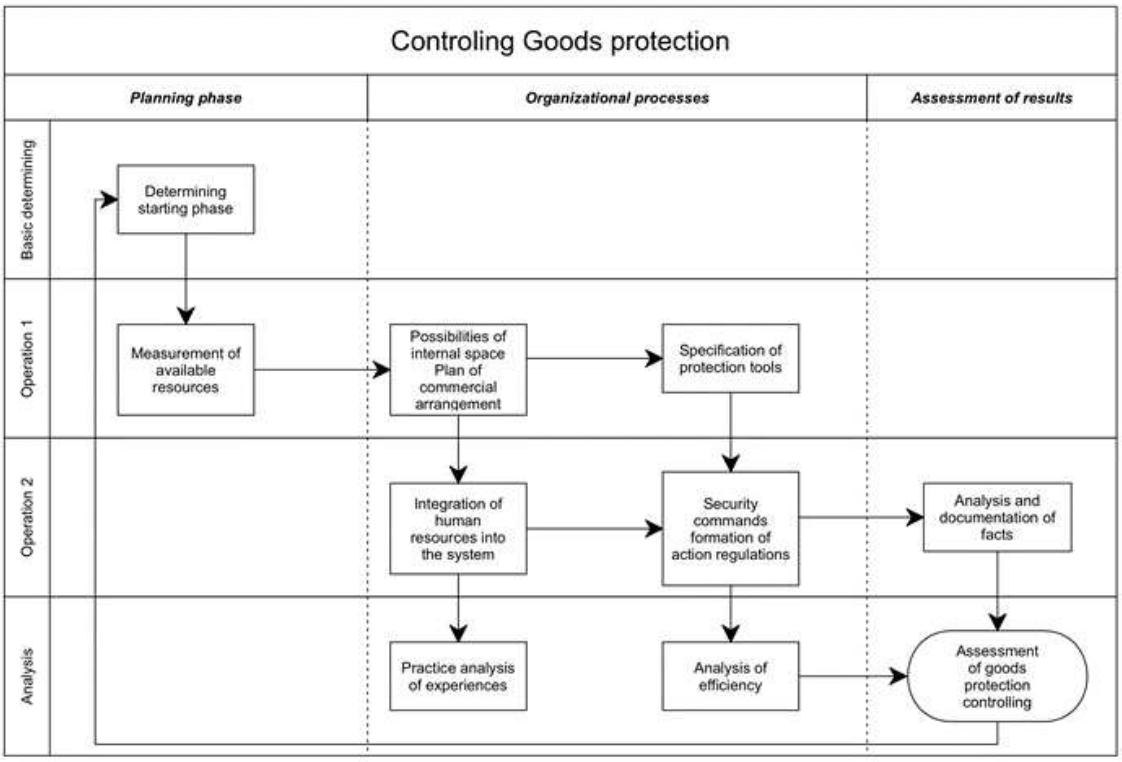


Fig.2: Controlling Goods protection (the author edited based on [2])

Structuration of goods protection controlling

- Dividing goods protection processes into parts
- Measuring the performance of each part
- Measuring and recording the starting point

- Setting the planned status
- Implementing assessment
- Determining developments, making new plans

The structuration of goods protection controlling demonstrated by 3 figure.

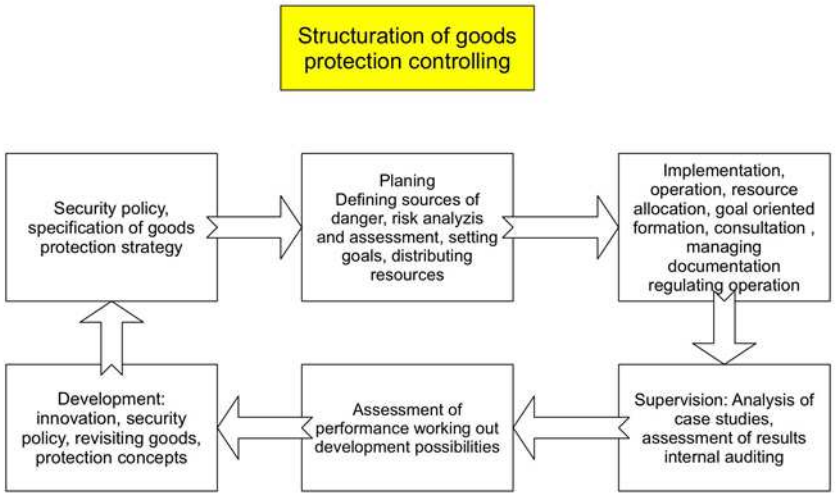


Fig.3: Structuration of goods protection controlling (edited by the author)

CONCLUSIONS

The ars poetica of protection strategies is the organization culture, a system integrating the shared presuppositions, values, convictions and beliefs accepted by the members of the organization. They are considered to be valid by the members, are observed and handed down to new members. They represent the model solutions to problems as well as the desirable mind-set and behavior.

Configure the protection system is essential for controlling. Successful controlling = the effective implementation of the relevant information available to us from highlighting data. The permanent information feedback is necessary for the objective data rating. This is the way for the easier and more efficient job

BIBLIOGRAPHY

[1] FRANCSOVICS, Anna: Controlling electronic publication; Óbuda Egyetem Keleti Károly Gazdasági Kar, Budapest, 2011.

[2] MCS Managment & Controlling Service Kft: Controlling a gyakorlatban; 2001

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

VÉDELMI TERVEZÉSI MODELLEK KIALAKULÁSA ÉS FEJLŐDÉSE

EVOLUTION AND DEVELPMENT OF DEFENCE PLANNING AND MODELLING

SZAKALI MIKLÓS; SZŰCS Endre

(ORCID ID); (ORCID ID)

mszakali@hotmail.com; szucs.endre@bgk.uni-obuda.hu

Absztrakt

A cikkben egy kevésbé közismert területtel a védelmi tervezéssel, annak kialakulásával és fejlődésével foglalkozunk. Röviden ismertetjük az általános értelemben vett stratégiai tervezés és a védelmi tervezésnek a kapcsolatát. Bemutatjuk a védelmi tervezés alapjai kidolgozásának szükségszerűségét és főbb körülményeit. Átfogó leírást nyújtunk a védelmi tervezés elméleti megközelítéseinek változásairól, fejlődéséről, valamint a jelenleg is alkalmazott védelmi tervezési modellek közül mutatjuk be a legjellemzőbbeket. Tekintettel a téma kiterjedt szakirodalmára, valamint a nemzetek és különböző szervezetek által alkalmazott modellek számos változatára a cikkben az általunk meghatározónak ítélt modelleket és összefüggéseket terveztük áttekinteni.

Kulcsszavak: *stratégiai tervezés, védelmi tervezés, tervezési modellek*

Abstract

In this article we intend to deal with a publicly less-known knowledge domain, namely defence planning introducing its evolution and further development. We will shortly present the connection between the generally recognized strategic planning and the more specific defence planning. Than we are touching upon the necessities and the main circumstances that made inevitable to lay down the bases of the defence planning domain. With displaying the most commonly used planning models this article will provide you with a comprehensive picture on the main stages of those theories and practical approaches that shaped defence planning and modelling.

Taking into consideration the extensive literature of this special field and the great variety of the models applied by nations and different organizations we agreed on selecting those models and correlations that were decisive in course of development.

Keywords: *strategic planning, defence planning, planning models*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.10.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.20.

BEVEZETÉS

A cikkben a védelmi tervezési modellek kidolgozásának kezdetével és fejlesztésük főbb állomásaival foglalkozunk, ugyanakkor fontosnak tartjuk bemutatni a védelmi tervezés, mint a védelmi ágazati szakpolitika stratégiai tervezésének helyét és szerepét a stratégiai tervezés általános rendszerében.

Feltehetjük a kérdést, hogy mi is a stratégiai tervezés és miért van erre szükség? Egészen leegyszerűsítve a válasz; a jelenünk és a jövőnk közti híd megtervezése, kidolgozása úgy, hogy azzal a jövőnket is formáljuk a saját értékeink és érdekeink figyelembevételével. Ennek alapján a stratégiai tervezés egy általános tevékenység, amelyet az egyén szintjétől a kormányzati, a nemzeti és a nemzetközi szervezetek szintjéig mindenhol gyakorolnak a jövő alakítása érdekében.

Ugyanakkor a stratégiai tervezés az érdekérvényesítés és a hatalom gyakorlásának eszköze is, amelyet a jövőbeli cél/célok meghatározása és elérése érdekében, folyamatos kontroll (felügyelet és beavatkozási lehetőség) fenntartása mellett gyakorol az erre felhatalmazott vezető/személy.

Egy stratégiai terv főleg a hosszú távú (10< év) stratégiai célok kijelöléséről szól, amellyel meghatározzák a jövőben elérni kívánt állapotot/helyzetet illetve az ehhez szükséges haladás irányát. A célok kijelölése természetesen tükrözi a hatalmi viszonyokat és érdekeket, amelyek a tervek végrehajtásához szükséges erőforrások biztosításában is megnyilvánulnak. A hatalmi viszonyok alatt ebben az esetben nem csak a politikai, hanem a gazdasági, tulajdonosi helyzeten és jogi felhatalmazáson alapuló hatalmat, döntési jogkört is értjük.

Stratégiai tervezést általában minden politikai, gazdasági és társadalmi tevékenységet folytató szervezet, vállalat, intézmény folytat, amely tudatosan tervezi a jövőjét és biztosítani akarja helyét és sikerességét hosszú távon is. Az állami és kormányzati szerveknek azonban a stratégiai tervezés nem csak egy lehetőség, hanem kötelezettség is, amelyet általában jogszabályok írnak elő. A választásokon nyert mandátum alapján a kormány joga és kötelessége a választók képviseletében a nemzet érdekeinek érvényesítése és fejlődésének biztosítása. Ennek érdekében minden hivatalban lévő kormány kidolgozza és működteti a stratégiai tervezés rendszerét, melynek keretében meghatározza az összkormányzati stratégia célkitűzéseit és prioritásait, valamint az azokat támogató ágazati stratégiák kidolgozásának és végrehajtásának rendjét. Ebből következően a védelmi ágazat felelős szakpolitikai szerve a védelmi minisztérium kidolgozza a védelmi ágazat stratégiai/hosszú távú tervét. A védelmi ágazat stratégiai tervezési folyamatát és eljárásrendjét nevezzük védelmi tervezésnek.

A védelmi tervezés egy bonyolult tevékenységi rendszer, amely magában foglalja a politikai, gazdasági, katonai, műszaki és egyéb szakterületek interakcióit a védelmi tervek megalapozása érdekében. Ezeket a folyamatokat még a tervezés területén jártas szakembernek is kihívás átlátni és irányítani, nem beszélve az állam döntéshozóiról, akik nem a tervezés szakemberei. Az illetékes döntéshozóknak viszont joguk és kötelességük meggyőződni az állami források célirányos felhasználásáról és arról, hogy a tervezés eredményeként valóban megjelennek a védelmi funkció gyakorlásához szükséges erők, eszközök és képességek.

Ezért szükséges a bonyolult tervezési folyamatokat modellek segítségével bemutatni és áttekinthetővé, érthetővé tenni a tervezési folyamaton kívüli, de a folyamatra hatást gyakorló szereplők részére is. A tervezési modellek tehát a folyamatok egyszerűsített ábrái, melyek a legfontosabb résztvevőket, tevékenységeket, alternatívákat, okmányokat és döntési pontokat tartalmazzák, azokat a fő elemeket, amelyek garantálják a kívánt célok elérését és az állami források felhasználásának átláthatóságát és elszámoltathatóságát.

PPBS alapú tervezés elterjedése

Az előző bekezdés alapján nyilvánvalóvá vált a PPBS jelentősége, mely legfőbb érdeme, hogy egy tervezési rendszerbe integrálta a védelemi képességeket meghatározó politikai, katonai és költségvetési tényezőket és ezek kölcsönhatásában biztosított keretet a védelmi tervek kidolgozására.

Természetesnek tekinthető, hogy a PPBS alapú tervezés népszerűvé vált nem csak a védelmi szektorban, de a polgári vállalatok körében is, és világszerte elterjedt. A régi NATO országok tapasztalataira alapozva az aspiráns és partner nemzetek részére is a PPBS alapú védelmi tervezés bevezetését javasolta a NATO.

Több nemzetközi szervezet Word Bank, International Monetary Fund, OECD ajánlásokat tett a kormányzati stratégiák és a központi költségvetés összehangolásával, valamint a források felhasználásának átláthatóságával bajlódó tagjai számára a PPBS alapú tervezés alkalmazására.

A védelmi tervezési modellek fejlődése

Az 1989-1990-es éveket követő poszt-bipoláris korszakban a potenciális fenyegetések és a kihívások sokrétűbbekké és nehezebben azonosíthatóakká váltak, s részben e miatt, részben pedig a biztonsági környezetre egyre inkább jellemző bizonytalanság következtében a védelmi tervezési rendszereknek rugalmasabbá és költségérzékenyebbé kellett válniuk. A meglévő PPBS eljárások alapvetéseinek figyelembevételével folyamatosan keresték a védelmi tervezés megújításának lehetőségét az új követelményeknek való megfelelés érdekében. Ezt a törekvést mutatja be a védelmi tervezés elméleti megközelítési lehetőségeinek [2] leírása:

1. *Fentről lefele történő tervezési (Top-down planning*) [3] *modellt* leggyakrabban az *alulról felfelé történő tervezéssel (Bottom-up planning)* kombinálva, ún. *ellenáramú tervezésként* alkalmazzák. Vagyis a felülről lefelé történő tervlebontás meghatározza a célokat és a főbb keretszámokat, az alsóbb szintek pedig a részleteket kibontva tovább terveznek. Az alulról felfelé történő tervezés viszont a legalsó szinten indul, s az egészre érvényes elvárások a folyamat végén alakulnak ki.Az ellenáramú tervezés lényege éppen az, hogy a sarokszámokat, elvárásokat, elveket, felülről kell meghatározni, az igényeket viszont – lehetőség szerint már ennek figyelembe vételével – alulról kell megfogalmazni. Ezután kerülhet sor az igények és lehetőségek ütköztetésére. Tekintettel arra, hogy az igények – a tapasztalatok szerint – minden esetben meghaladják a lehetőségeket, következhet a tervezési folyamat legnépszerűtlenebb feladata, a tervalkuk sorozata.
2. *Forráskorlátok közötti tervezés (Resource Constrained planning) modellje.* A védelmi tervezés e módszerének esetében a védelmi költségvetésben meghatározott források alapján igyekeznek kialakítani az életképes, fenntartható, de végső soron a rendelkezésre álló források által meghatározott képességeket. A tapasztalatok azt mutatják, hogy e tervezési módszer – a legnagyobb tervezési fegyelem mellett is – tartósan alulfinanszírozottá teszi a haderőket és zavarokat okozhat működésükben. Forráskorlátozott tervezés mellett igen nehéz megvalósítani nagyszabású és hosszú távú modernizációs terveket, mert az ezekre szánt források hosszú évekre elvonhatják a modernizáció lehetőségét a haderő más területeitől, mivel a forrás-korlátozott tervezés egyik legfontosabb jellegzetessége a fejlesztési projektek időintervallumának elnyúlása.
3. *Technológiai-optimizmus (Technology optimism) modell.* E tervezési módszer legfontosabb stratégiai célkitűzése a műveleti és stratégiai fölény fenntartása technológiai fejlesztéseken keresztül. A nyugati világ legfejlettebb államai – élükön az Egyesült Államokkal – évtizedeken keresztül ezt a módszert preferálták leginkább, s igen nagy sikerrel. A technológiai optimizmus kritikusai azonban arra

is felhívják a figyelmet, hogy a haditechnika megszerzése sokkal könnyebb, mint az intézmények és struktúrák kifejlesztése és működtetése, nem is beszélve arról, hogy az igen drágán kifejlesztett új technológia önmagában ritkán vezet el paradigmaváltáshoz. Az aszimmetrikus hadviselés szakértői pedig a technológiai optimizmus magas költségeit bírálják, rámutatva a modell költséghatékonyságának problémáira.

4. *Kockázatkerülő-tervezési (Risk Avoidance) modell. Ez a modell a konzervatív* tervezési modellek csoportjába tartozik, s elsősorban a már bizonyítottan bevált koncepciók és struktúrák kiterjesztésén és továbbvitelén nyugszik. E modell fő jellemzői közé tartozik a bázis alapú tervezés (amely az előző évi, valamint a tervévi változások számszerű hatásának beépítésével határozza meg a tervidőszak céljait), az inkrementális (fokozatosan növekvő) haladás és fejlesztés, a kockázatkerülés, a hagyományos tervezési elvek és szemlélet érvényesítése, a visszafogott változtatások, a relatíve kisebb, de biztos eredményekkel való megelégedés, és az innovatív kapacitások figyelmen kívül hagyása.
5. *Inkrementális-tervezési (Incremental planning) modell.* A meglévő képességek képezik a jövőbeni fejlesztések alapját, vagyis ezek fokozatos továbbfejlesztésén keresztül alakítják ki a kockázatkerülő tervezetési folyamatot. Nem az a cél tehát, hogy minden funkciót egyszerre fejlesszünk, hanem az, hogy fokozatosan és folyamatosan egy-egy újabb funkciócsoporttal gazdagodjon a rendszer. Az inkrementális megközelítési mód egy köztes megközelítés az ún. vízesésmodell[1] és az evolúciós (pl. kockázatkerülő) fejlesztési modellek között. A vízesésmodell megköveteli, hogy a megrendelő véglegesítse a követelményeket, mielőtt a tervezés elindulna, a tervezőtől pedig azt, hogy válasszon ki bizonyos tervezési stratégiákat a megvalósítás előtt. Az evolúciós megközelítésnél pedig megengedettek a követelményekkel és tervezésekkel kapcsolatos döntések elhagyása, ami pedig gyengén strukturált és nehezen megérthető rendszerekhez vezethet.
6. *Történelmi-tapasztalati (Historical extension) modell*. Hasonlón a kockázatkerülő és az inkrementális tervezési modellhez a történelmi tapasztalatok kiterjesztése is abból indul ki, hogy ami működött a múltban, az működni fog a jövőben is. E modell tehát a jövőbeni műveleti hatékonyságot történeti analógiák elemzésén, ezen elemzések eredményeinek a védelmi tervezési folyamatba való beépítésén keresztül kívánják biztosítani. Hívei a történeti tapasztalatokból kiindulva fejlesztik tovább a pozitív tényezőket és hagyják el a negatívakat. Alapvetően konzervatív tervezési modell, és viszonylag könnyen megszerezhető hozzá a társadalom és a közvélemény támogatása.
7. *Képességalapú-tervezési (Capability-based planning) modell*. A képességalapú tervezés alapja a lehetséges jövőbeni műveletek és feladatok funkcionális elemzése. A tervezés kimenete, illetve eredménye nem konkrét képességek és létszámszintek, hanem annak meghatározása, hogy milyen feladatokat kell tudnia ellátnia képességekre lefordítva a feladat végrehajtására rendelt erőnek. A képességleltár elkészültével és a képességhiányok meghatározását követően a képességteremtés megvalósíthatóságát lehetővé tevő legköltséghatékonyabb és termelékenyebb lehetséges tényleges eszközöket és egységcsomagokat határoznak meg. A

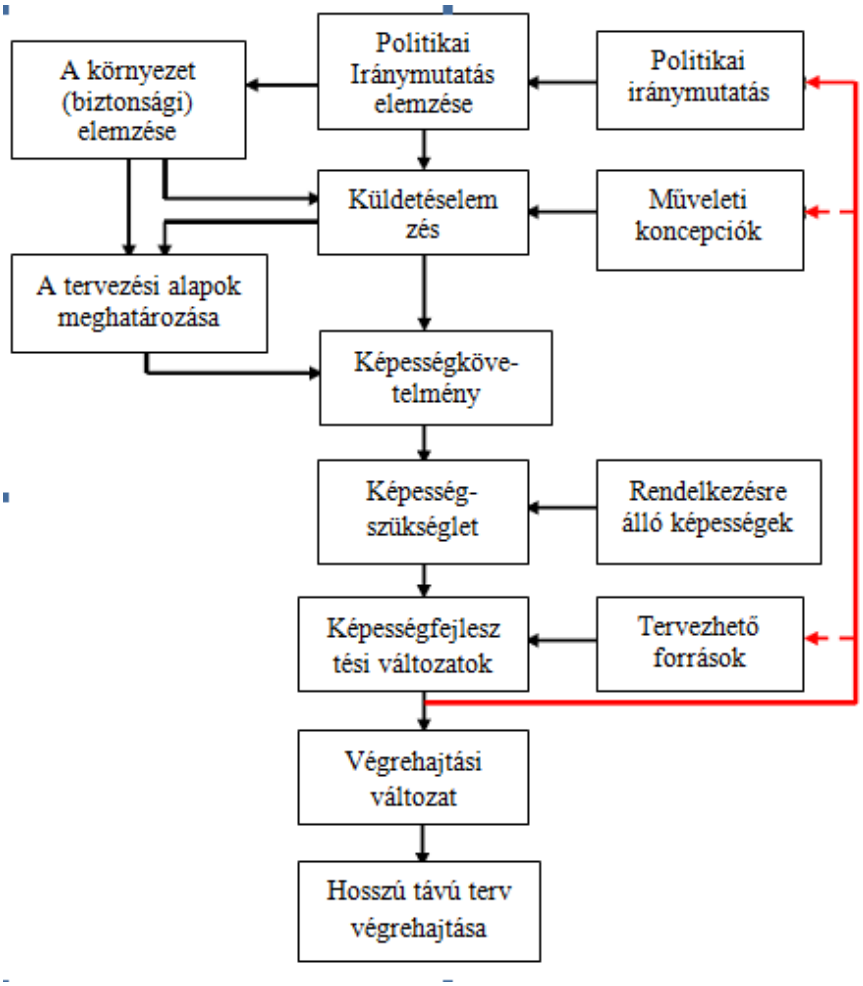
[1] Az ún. vízesés fejlesztési modell szakaszai: 1. problémadefiniálás, helyzetfelmérés, elemzés; 2. koncepciókészítés, megvalósíthatósági tanulmány, döntés, projektindítás; 3. rendszertervezés logikai szintje; 4. rendszertervezés fizikai szintje; 5. megvalósítás; 6. tesztelés; 7 rendszerbeállítás.

képességalapú tervezési modell a kétpólusú világrend bukását, s az egyetlen konkrét és beazonosítható ellenségkép megszűnését követően vált igen népszerű védelmi tervezési eljárássá.

8. *Forgatókönyv-alapú tervezési (Scenario-based planning) modell.* Ez a megközelítés lehetséges forgatókönyvekre vonatkozóan vetíti ki a haderő képességeinek fejlesztését. A szcenárió nem egy előrejelzés, ugyanakkor azonban nem is teljesen lehetetlen jövőbeli szituáció, leginkább egy hipotetikus szituációnak tekinthető. A forgatókönyvek kidolgozását megelőzi a kulcsproblémák és az elemzés kereteinek kijelölése, az elemzés/megközelítés helyességének vizsgálta, a releváns folyamatok és driverek, illetve a lehetséges környezeti és műveleti paraméterek azonosítása. Az eltéréseken alapuló szcenáriók kidolgozást követően a szcenáriókhoz szükséges terveket készítik el, majd a fejlemények és feltevések megfigyelésével zárul e tervezési modell folyamatköre.
9. *Fenyegetettség-alapú tervezési (Threat-based planning) modell.* A fenyegetés alapú tervezés a lehetséges ellenfelek meghatározásán és képességeik vizsgálatán alapul. A képességbeli követelmények legfontosabb viszonyítási alapja a potenciális ellenfél képességeinek a meghaladása, amelyben a minőségi és mennyisége megoldások egyaránt szerepelnek. A fenyegetettség alapú megközelítés abban különbözik a szcenárió alapú tervezéstől, hogy hiányzik belőle a humanitárius és más nem fenyegettség alapú szcenáriók vizsgálata és figyelembevétele.
10. A NATO tagállamok többsége tehát az egyik oldalon a védelmi költségvetések folyamatos stagnálásával, illetve szűkülésével, a másikon pedig a változó biztonsági környezet miatt a lehetséges NATO-missziók és feladatok egyre bővülő spektrumával voltak kénytelenek szembenézni. A fentiek következtében a NATO-tagállamokban a poszt-bipoláris korszakban előtérbe került a képesség-alapú (*Capability-based planning)* és a forgatókönyv-alapú tervezés (*Scenario-based planning)*. Néhány példa ezek változataira.

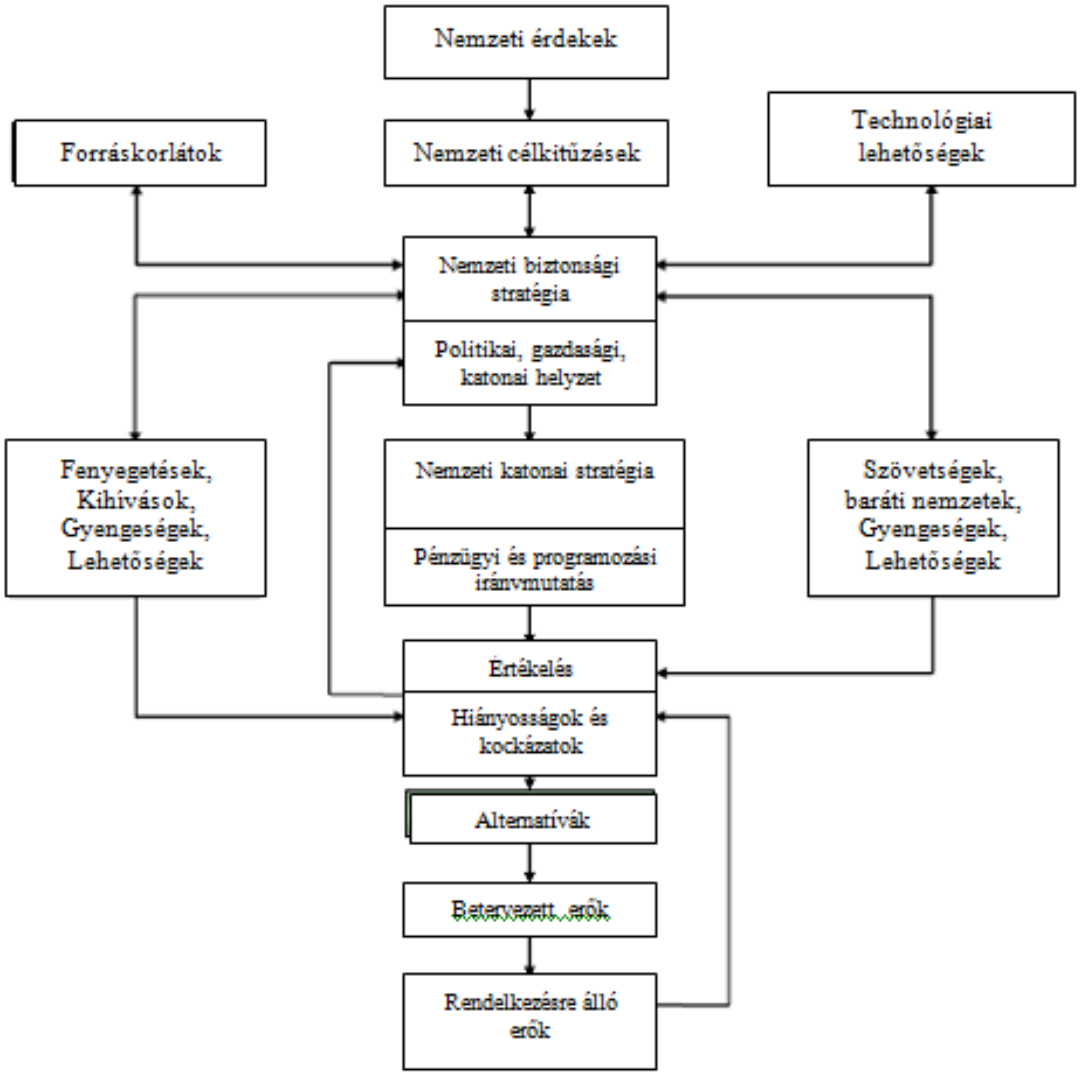
Dejan Stojkovic, Bjørn Robert Dahl által felállított általános tervezési modell [4] (1. ábra) megfelel a tervezési megközelítések több kritériumának, ezért javasolják a szerzők.

- fentről – lefelé történő megközelítést alkalmaz;
- auditálásra alkalmas nyomvonalat tartalmaz;
- lehetővé teszi a quantitative analysis (matematikai modellezésre épülő vizsgálat) elvégzését;
- a folyamatok, valamint a ki,- és bemeneti követelmények meghatározottak;
- átfogó próba folyamaton ment keresztül.



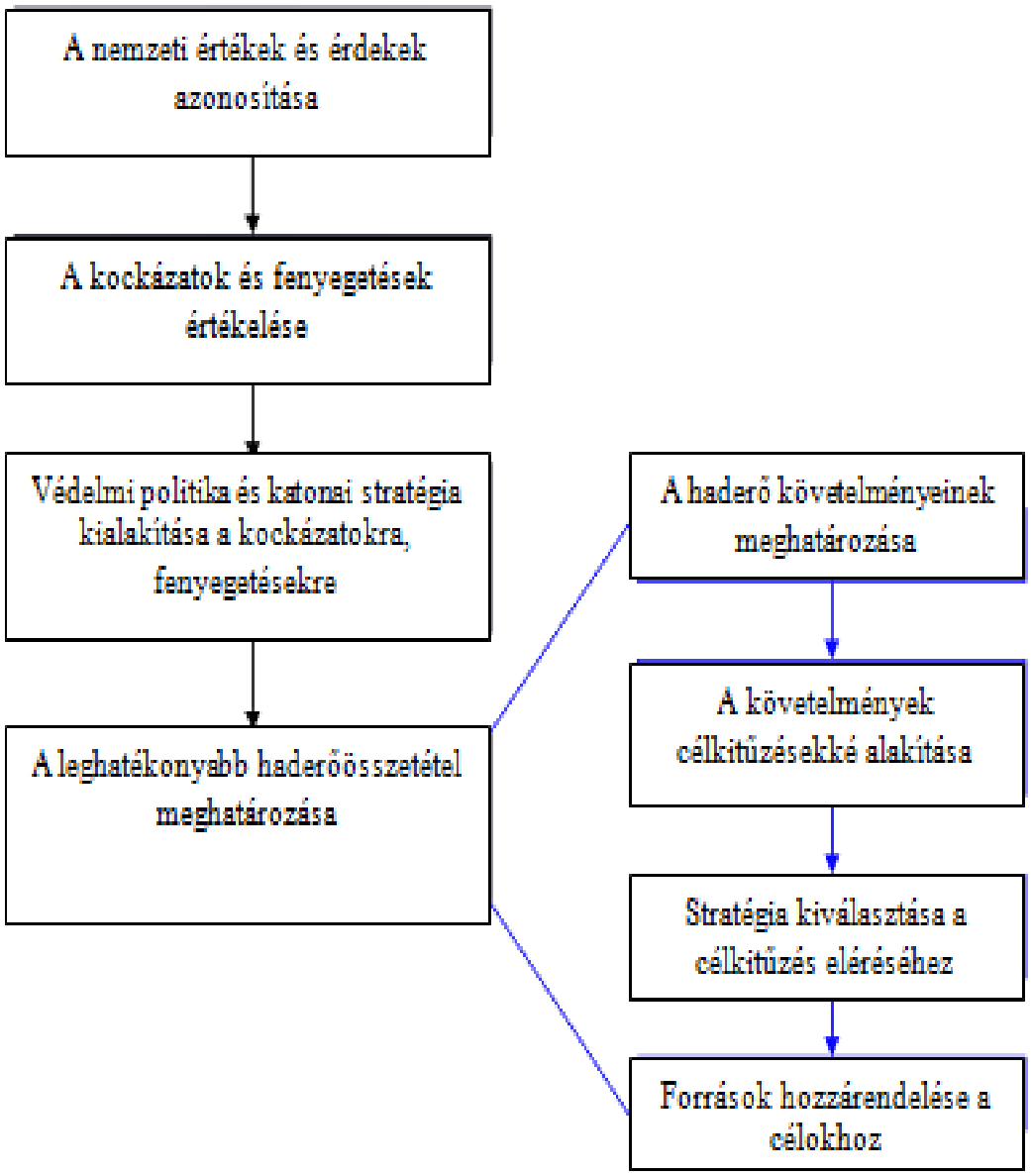
1. ábra Általánosan javasolt modell a védelmi tervezésre

Az általános modellhez nagyon hasonló az *USA Stratégiai és Haderő-tervezési kerete* [5] (2. ábra), amelyet Lloyd modellként is ismerünk.



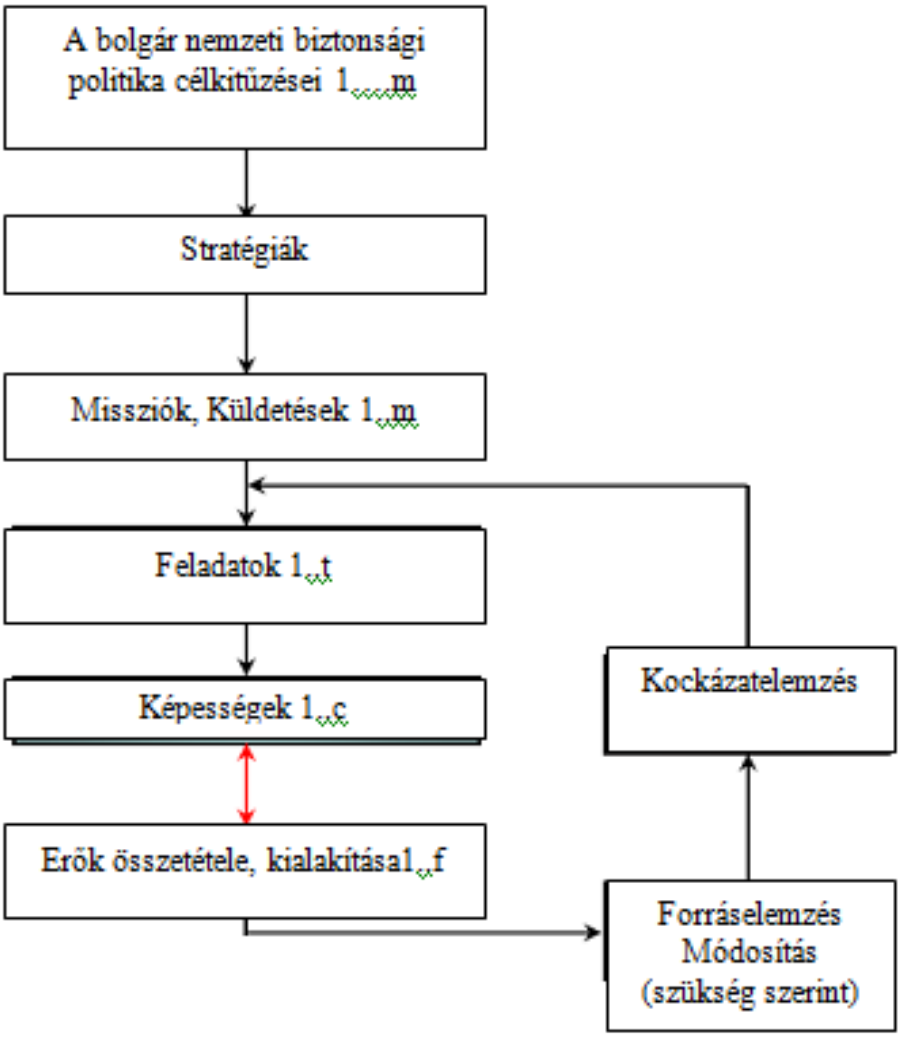
2. ábra Az USA stratégiai és haderő-tervezési kerete

Az *olasz* védelmi tervezési modell [6] (3. ábra) nem hasonlít a fenti két modellre, a képesség szó nem szerepel a modellben, ugyanakkor követi az általános modellt a nemzeti érdekek, védelmi irányelvek és a katonai stratégia összekapcsolásában. A katonai stratégia végrehajtására a megfelelő haderő-összetétel kialakítását tartja szükségesnek, amely így magában hordozza a képességek követelmények összetevőit, mint pl. fegyverzeti, humán erőforrás, struktúra. A modell előnye az egyszerűség és a könnyen áttekinthetőség.



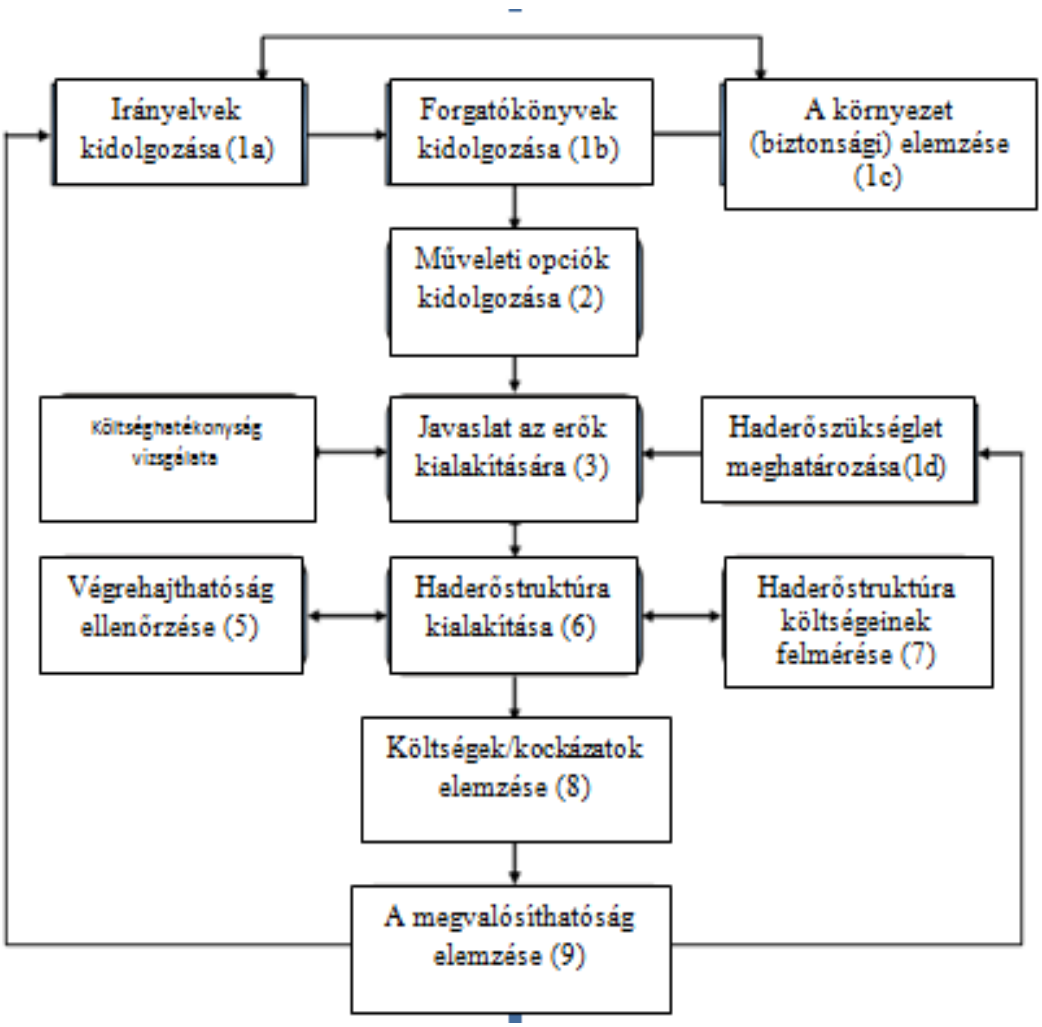
3. ábra Az olasz védelmi tervezési modell

A *bolgár* védelmi tervezési keretet [7] (4. ábra) az általános tervezési és az olasz tervezési modell kombinációjaként értékelhetjük. Esetükben részletesen kibontják a stratégiákhoz kapcsolódó küldetések rendszerét, majd a küldetésekhez kapcsolódó feladatrendszert. A feladatrendszer alapján határozzák meg a szükséges képességeket és a képességeket „előállító" haderő-összetételt. A tisztán szakmai alapú tervezés eredményéhez rendelik a forrásokat és forráshiány esetében a kockázatok elemzését követően visszatérnek a szakmai tervezési eljáráshoz a feladatrendszer ismételt elemzésével.



4. ábra A bolgár védelmi tervezési keret

Az eddig bemutatott, valamint egyéb nemzeti modellek alapján a NATO kidolgozta az ún. Legjobb-tapasztalatokon alapuló/Best Practice modellt [8] (5. ábra), melyet javasolt a tagországok és a partnerek figyelmébe a képesség-alapú tervezés megkönnyítése érdekében.



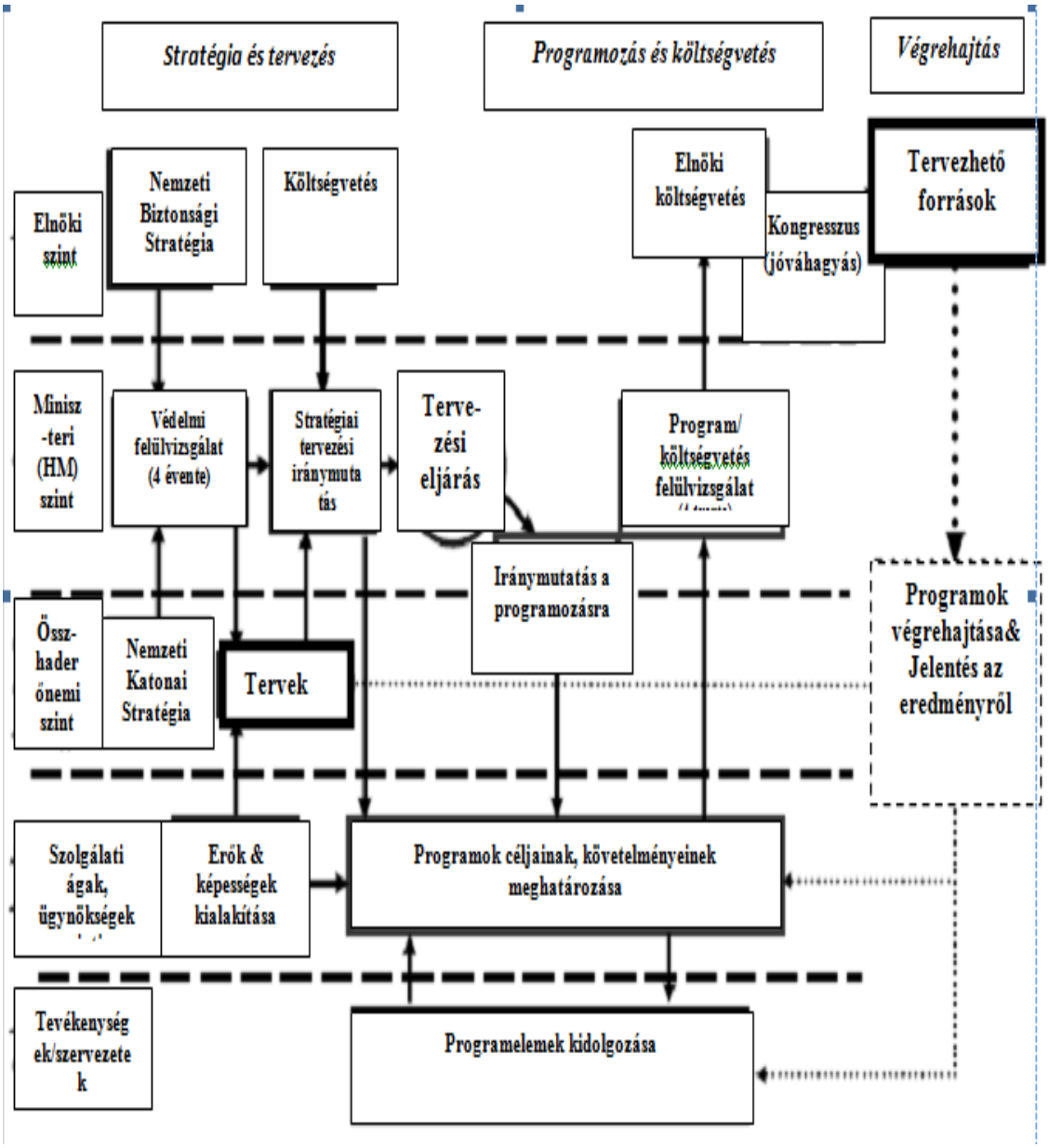
5. ábra NATO „Best Practice" modell

A PPBE (PLANNING-PROGRAMMING-BUDGETING-EXECUTION/ TERVEZÉSI-PROGRAMOZÁSI-KÖLTSÉGVETÉSI ÉS VÉGREHAJTÁSI) MODELL KIDOLGOZÁSA [9]

2004-ben az Aldridge csoport egy jelentésében az amerikai tervező PPBS-en alapuló rendszert túl bürokratikusnak, fiskális szemléletűnek és a rendszer kimeneti követelményeit becsléseken alapulóaknak találta. Megítélésük szerint a rendszer még a fenyegetettség alapú tervezés eszköze volt és nem támogatta az akkoriban előtérbe kerülő képesség-alapú tervezést.

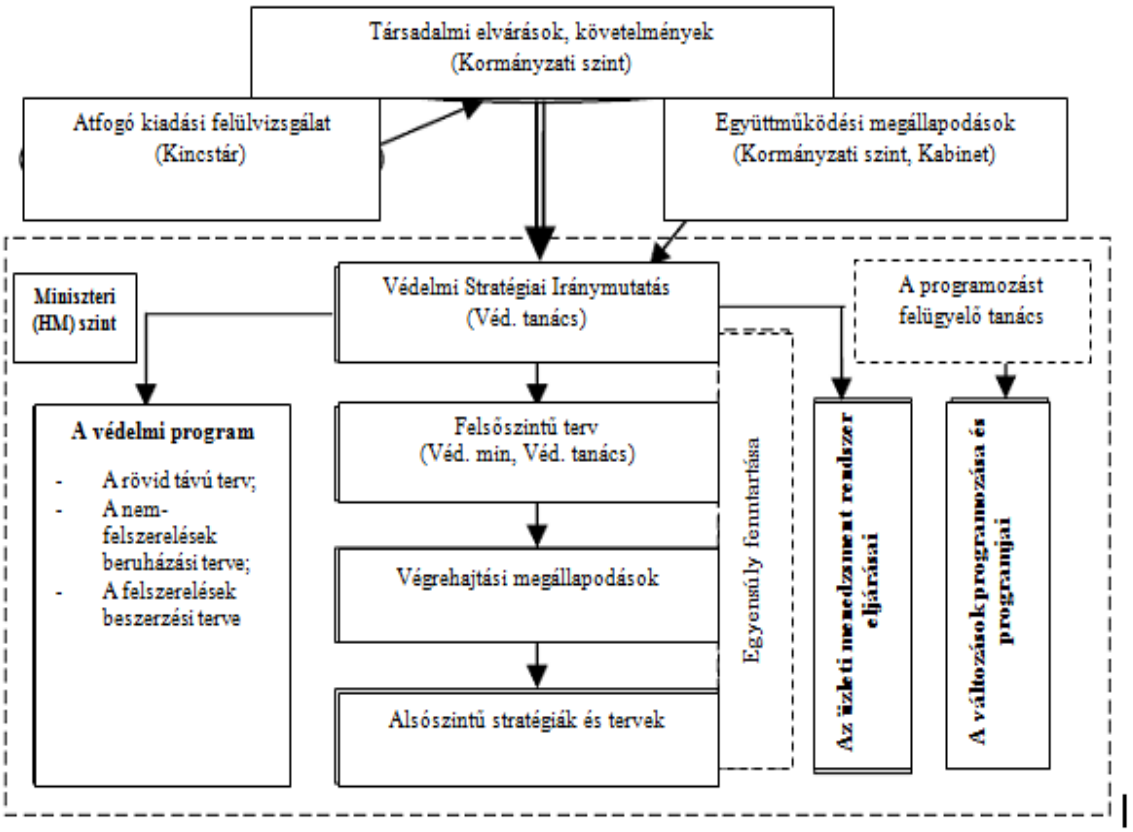
A PPBS átalakítása két fő elemen keresztül valósult meg:

1. a tervezési ciklust 2 évre növelték, hogy elég időt biztosítsanak az összhaderőnemi (joint) tervezéshez és csökkentették a szükségtelenül részletes éves programozást, amikor azt a biztonsági környezet, vagy a tervezési alapvetések változása nem indokolja.
2. beemeltek egy un. végrehajtási (Execution) fázist, - gyakorlatilag egy menedzsment modult – amely a tervek végrehajtását követi figyelemmel, így biztosítva az összhangot a tervezés és a tervek végrehajtása között. A menedzsment modul monitoring, elemző-értékelő tevékenységeken keresztül valósul meg. Összehasonlító elemzésekkel mérik a védelmi programok tervezett és az elért eredményeinek különbségét, megállapítják a források felhasználásának gazdaságosságát, valamint a fejlesztések hatékonyságát. Az Végrehajtási/Execution fázis bevezetését követően a tervező rendszer nevét PPBS-ről PPBE-re változtatták. Az alábbi ábrákon szintén azt figyelhetjük meg, hogy egyes nemzetek hogyan integrálták a menedzsment funkciót a védelmi tervezési folyamatukba.



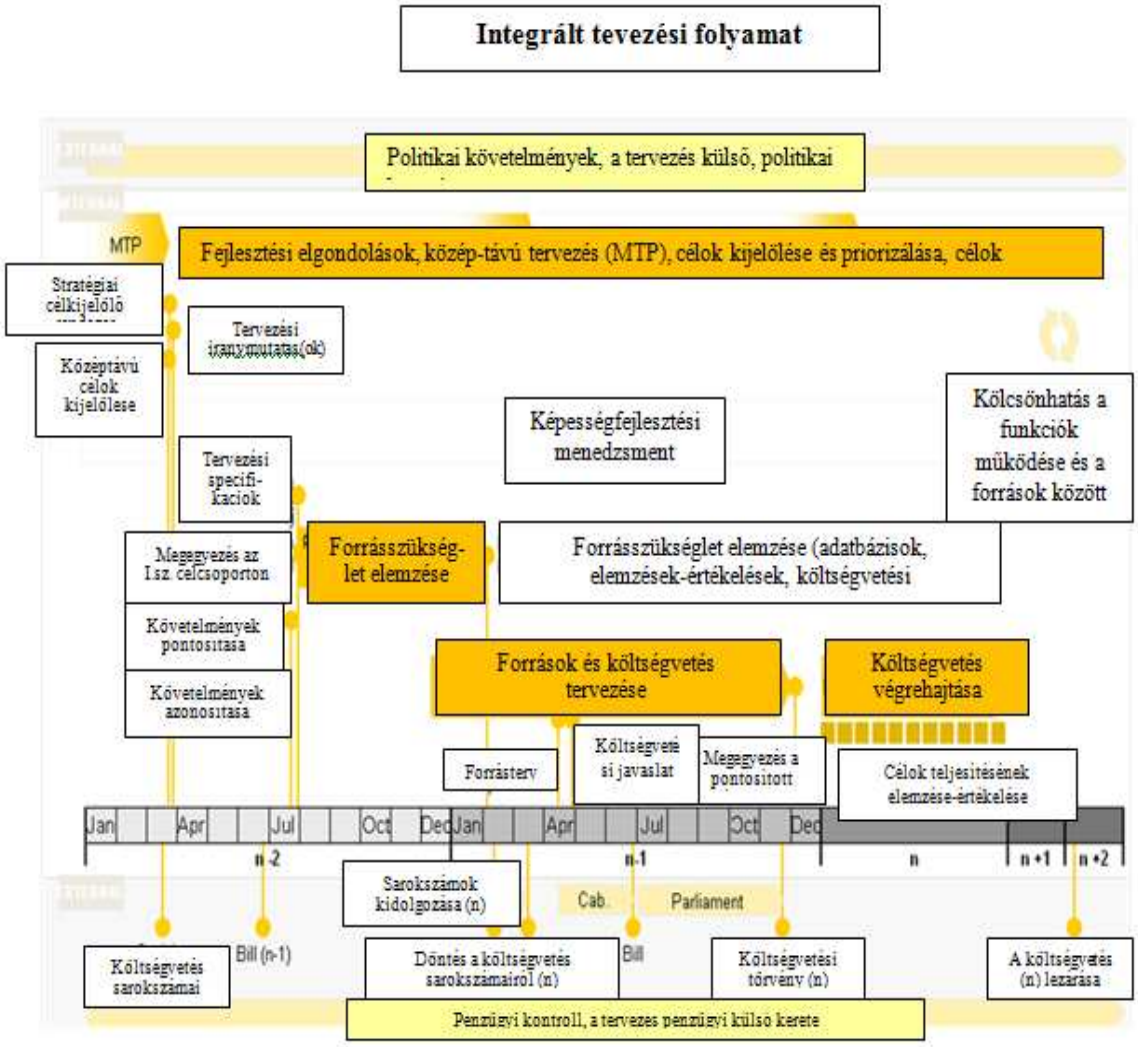
6. ábra Az USA PPBE modellje [9]

A brit tervezési modellen [10] (7. ábra) is megfigyelhető, hogy a hagyományos védelmi tervezési alaptevékenységek (a kormányzat politikai és forrás inputja, a védelmi program, a különböző stratégiák és tervek) mellett integrálták a folyamatba az üzleti menedzsment és rendszereljárások modulját. Jelentőségét mutatja, hogy a modul a védelmi minisztérium stratégiai vezetéséhez a Védelmi Tanácshoz van „bekötve". Így a legmagasabb vezetési szint által meghatározott feladatokat hajtja végre, valamint annak részére biztosít információt a rendszer tevékenységéről és az eredményekről.



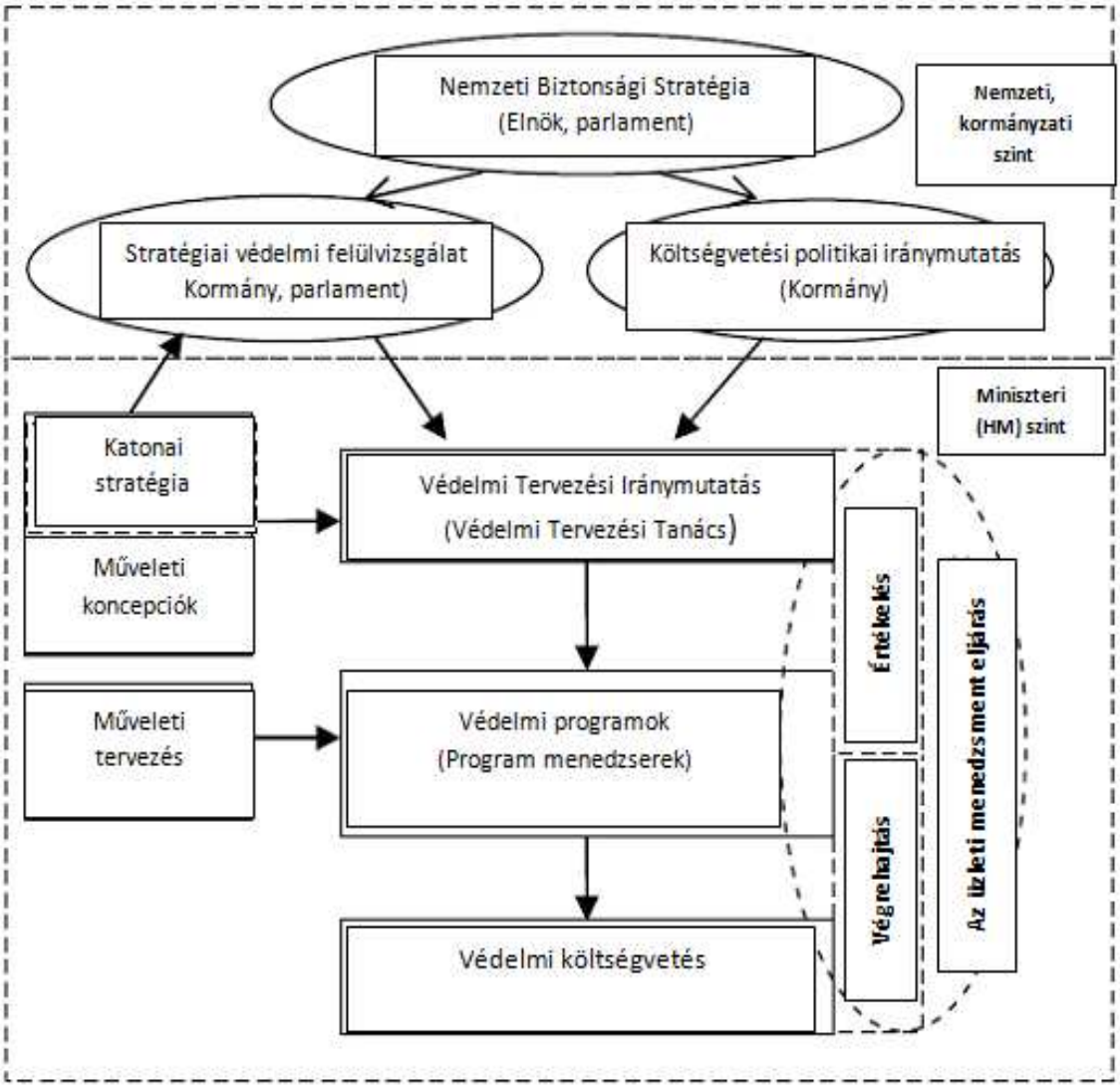
7. ábra Brit védelmi tervezési és üzleti menedzsment modell

A német Integrált Tervezési Folyamat [11] (Integrated Planning Process) (8. ábra) is a fenti PPBE rendszer adaptálásával került kialakításra. A rendszer jellegzetessége, hogy van egy külső keret (external framework) melyet felülről a politikai és koncepcionális követelmények, alulról pedig a pénzügyi kontroll tevékenység határol. A rendszer belső tartalmának újdonsága a képesség menedzsment (Capability management) bevezetése, amely átfogja az belső eljárásrendet és komlex módon figyelemmel kíséri és szabályozza és összehangolja mind a funkcionális, mind pedig a pénzügyi folyamatokat.



8. ábra A német Integrált Tervezési Folyamat

Mindezek figyelembevételével a NATO ismét kidolgozott egy általános modellt [12] (9. ábra) a védelmi tervezésre, amely magában foglalja a PPBS alapjait, a fentről-lefelé és a képesség-alapú tervezési megközelítéseket, valamint a menedzsment modul integrálását a tervezési folyamatba.



9. ábra A NATO által javasolt általános modell a védelmi tervezésre

KÖVETKEZTETÉSEK

A védelmi tervezés folyamatosan fejlődik a külső biztonsági környezet, valamint a belső politikai akarat és gazdasági lehetőségek változásait lekövetve. Ez a fejlődés töretlen lesz, amíg a biztonsági környezet kihívásaira a katonai válaszadás lehetősége reális opció marad.

Meghatározó jelentőségű és jelenleg is érvényes az a felismerés, hogy a védelmet döntő módon befolyásoló elemeket egy rendszeren (PPBS) belül kell kezelni.

A következő mérföldkőnek a képesség-alapú tervezésre való áttérést tekinthetjük, melynek alapja szintén a biztonsági környezet jelentős változása volt. Egy állandó nagymértékű fenyegetettség megszűnése, és több, térben elkülönülő kihívás egyidejű megjelenése tette szükségessé a tervezési filozófia módosítását, a menedzsment modul bevezetését.

Tovább segítették a védelmi tervezési rendszerek fejlődését az időközben végzett elméleti és gyakorlati tanulmányok és vizsgálatok, amelyek nagyon fontos részletekre és összefüggésekre világítottak rá. Azonban megállapíthatjuk, hogy nem lehet egyetlen elméleti, vagy gyakorlati modellt sem általános érvényűnek tekinteni a meglévő strukturális és funkcionális hasonlóságok ellenére sem. A modellek kialakítása nagymértékben függ egy nemzet geo-stratégiai helyzetétől, politikai és védelmi struktúráitól, intézményrendszerétől, valamint azok jogi felhatalmazásaitól.

Jelenleg a védelmi tervezés nemzeti alapokon folyik, a NATO, EU un. kollektív védelmi tervezése is a nemzetek terveire, képességeire épül. Ugyanakkor az európai szinten elhúzódóan alulfinanszírozott védelmi költségvetések és az egyre növekvő számú kihívások (orosz-ukrán konfliktus, ISIS, energiabiztonság, Ebola, terrorizmus, stb) figyelembevételével beláthatjuk, hogy előállhat olyan helyzet, amikor az egyes nemzetek önállóan már nem tudják kezelni a biztonsági kihívásokat.

Amennyiben az egyes európai nemzetek nem növelik jelentős mértékben (2% walesi döntés 2014-ben) a védelemre szánt forrásaikat és a kihívások száma és veszélyessége tovább nő, akkor elkerülhetetlenné válik a kollektív biztonsági, védelmi megoldások előtérbe helyezése. Azonban ezekhez a megoldásokhoz szükséges képességeket is a nemzeteknek kell létrehozniuk. Amennyiben erre nem képesek nemzeti alapon, úgy - véleményem szerint – egyedül a többnemzeti képességfejlesztés, biztosíthatja a szükséges védelmi képességeket, melyek létrehozásának az alapja a többnemzeti (a bilaterális, regionális, keretnemzeti kezdeményezés) alapú védelmi tervezés lehet.

Közös védelmi tervezési kezdeményezések már vannak, de valós előrelépésről még nem beszélhetünk. Természetesen ez nem könnyű folyamat, mert a nemzetek szuverenitásuk egy részének feladásaként értékelhetnek egy ilyen kezdeményezést.

FELHASZNÁLT IRODALOM

[1] TULKOFF, M. L., GORDON, C. V., DUBIN, R. D., HINKLE, W. P.: Project Leader Planning, Programming, and Budgeting System (PPBS)/Multi-year Programming" Institute for Defence Analyse, IDA Document D-4057 Log: H 10-000982, 2010 Sept, 25-26 o.

[2] TÁLAS P., VARGA G.: „A szövetséges államokban folyó védelmi tervezési tevékenység vizsgálata a NATO tervezési rendszerek tükrében" tanulmány az ÁROP-1.1.19-2012-2012-0001 kódjelű, „Hatásvizsgálatok és a kormányzati stratégiai irányítás rendszere egyes ágazati dokumentumainak elkészítése, valamint alkalmazási gyakorlatának támogatása a Honvédelmi Minisztériumban" elnevezésű projekt részeként készült. Budapest, 2013. 4-8. o.

[3] NATO Handbook on Long Term Defence Planning, RTO Technical Report 69, 2003 April, 4. o.

[4] STOJKOVIC, D., DAHL, B. R.: „Methodology for long term defence planning" Norwegian Defence Research Establishment (FFI), 28 February 2007. 16. o.

[5] LLOYD, R. M.: Strategy and Force Planning Framework, Strategy and Force Planning, Third Edition. Newport, RI: Naval War College, 2000. 3. o.

[6] STOJKOVIC, D., DAHL, B. R.: „Methodology for long term defence planning" Norwegian Defence Research Establishment (FFI), 28 February 2007. 39. o., Adapted according to: Risi, M.: Exchange of Information on Force Planning, (lecture), RACVIAC, Bestovje, Croatia 2001.

[7] STOJKOVIC, D., DAHL, B. R.: „Methodology for long term defence planning" Norwegian Defence Research Establishment (FFI), 28 February 2007, 40. o., Minchev, O., Ratchev, V., Lessenski, M.: Bulgaria for NATO - 2002, Institute for Regional and International Studies, Sofia, 2002. 257. o., Novick, D.: "The Origin and History of Program Budgeting." RAND Paper P-3427. Santa Monica, CA: RAND, 1966. NATO Handbook, 3. o.

[8] STOJKOVIC, D., DAHL, B. R.: „Methodology for long term defence planning" Norwegian Defence Research Establishment (FFI), 28 February 2007. 34. o.

[9] ZRNIĆ, B. Ph. D.: The New Trends in Defence Planning and Their Impact on the Defence Planning Systems in Transitional Countries, VOJNO DELO 1/2008. 33. o.

[10] ZRNIĆ, B. Ph. D.: The New Trends in Defence Planning and Their Impact on the Defence Planning Systems in Transitional Countries, VOJNO DELO 1/2008. 35. o.

[11] Német-magyar törzsmegbeszélés előadása, Budapest, 2013.

[12] ZRNIĆ, B. Ph. D.: The New Trends in Defence Planning and Their Impact on the Defence Planning Systems in Transitional Countries, VOJNO DELO 1/2008. 41. o.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

JÁRMŰVÉDELEMBEN ALKALMAZOTT FÉMES BALLISZTIKAI VÉDŐELEMEK ANYAGAI ÉS GEOMETRIÁI

MATERIALS AND GEOMETRY OF BALLISTIC ARMORS IN VEHICLE PROTECTION

GÁVAY György; TÓTH Bence

(ORCID: 0000-0003-0632-5650); (ORCID: 0000-0003-3958-187X)

gavay.gyorgy@uni-nke.hu; toth.bence@uni-nke.hu

Absztrakt

A lövedékek, repeszek elleni védőelemek illetve védőanyagok tulajdonságait tárgyalva fontos tisztázni az alapvető fogalmakat. A publikáció célja ezen túl feldolgozni és bemutatni a páncélozott járművek védőelemeinek fémes, homogén anyagait, és az egyszerűbb kialakítási formákat, az aktuális védőelem-vastagság változását a találati szög változásának függvényében.

Kulcsszavak: *ballisztikai védőelem, páncélátütés, döntött páncél, aktuális páncélvastagság*

Abstract

Before discussing the properties of armor it is important to clarify the Hungarian terminology to be used. Above this, the aim of this paper is to present and discuss the homogenous metallic materials used in armored vehicles and the dependence of the actual protecting element thickness-dependence of simple shapes on the angle of the hit.

Keywords: *protecting element, armor penetration, tilted armor, actual armor thickness*

A kézirat benyújtásának dátuma (Date of the submission): (2017.01.30.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.06.

BEVEZETÉS

A lövedékek, repeszek elleni védőelemeket illetve védőanyagokat a legtöbb esetben az anyagvastagságuk, összetételük és a felületi keménységük alapján jellemzik. A helyzet azonban ennél jóval bonyolultabb, és magyar nyelven kevés olyan publikus összefoglaló lelhető fel, amely feldolgozza, illetve bemutatja az anyagok és a kialakítás hatását a védelmi képességekre. A Nemzeti Közszolgálati Egyetem Haditechnikai Tanszékén működő kutatóműhely tevékenysége során jelentős publikációk készültek homogén ballisztikai acéllemezek lövedékek általi átütéséről, de a publikációk [1-2] alapját képező kísérletek alkalmával a merőleges találati szög alapkövetelmény volt. Ennek a publikációnak célja összefoglalni a homogén fémes ballisztikai védőelemek legfontosabb anyagait, kialakítását és a merőleges találati szögtől való eltérés hatását az aktuális védőelem-vastagságra. A téma jelen megközelítése a kinetikai energiát alkalmazó lövedékekre fókuszál, a kumulatív hatás elvén működő lövedékek tárgyalása nem célunk.

FOGALMAK

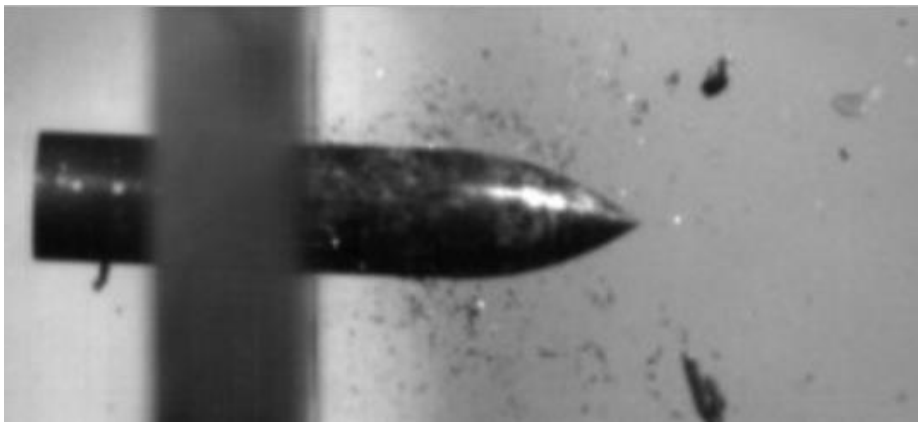
Ballisztikai pályának nevezzük azt a trajektóriát, melyen egy test a ferde hajításnak megfelelő mozgással mozog. Ez igaz a lövedékekre, melyek torkolati sebessége a levegő közegellenállása miatt folyamatosan csökken, illetve igaz bármely robbanásból eredő repesz mozgására. Jelen megközelítés figyelmen kívül hagy a ferde hajítási pályán haladáson kívül minden egyéb mozgást. Az említett nagy sebességű tárgyak elleni védelem a ballisztikai védelem.

A védelem valójában áthatolás elleni védelemként is felfogható, mert az említett tárgyaknak az adott védőanyagból készített védőelemeken történő áthatolását kell meggátolni.

A védőelemekből kialakítható védőelem-rendszer is, azok egymáshoz illesztésével vagy több rétegű, szendvicsszerkezetű elhelyezésével. [3]

A BALLISZTIKAI VÉDŐELEMEK ÉS AZOK MŰKÖDÉSE

A ballisztikai védőelemek célja a lövedékek vagy repeszek áthatolásának, azaz az átütésnek a megakadályozása. Amennyiben a becsapódó tárgy áthatol a védőelemen vagy védelemrendszeren, úgy a megmaradt mozgási energiája, illetve hőenergiája káros hatást idézhet elő a védendő területen. Becsapódáskor a védőelem anyagából repeszek válhatnak/szakadhatnak le, melyek áthatolás esetén szintén a védett terület irányában haladnak tovább. (1.ábra)



1. ábra. A lövedék áthatolása és a repeszek keletkezése [4; 543. o.]

Egyéni védőfelszerelések, például védőmellények esetében a repeszek az emberi testen a lövedék által okozott sebet is szennyezik.

Eredményes áthatolásgátlás esetén a becsapódáskor a lövedék mozgási energiáját a védőelem részben elnyeli, részben a védőelem tartószerkezetének, keretének, támasztékának adja át. Ilyenkor a védőelem, vagy védelemrendszer minden esetben károsodik, ennek a károsodásnak a mértéke számos körülménytől függ. Ezek lehetnek például:

- a lövedékre jellemző fizikai tulajdonságok (kialakítás, keménység1, tömeg),
- a lövedék sebessége,
- a védőelem felületi keménysége,
- a védőelem anyagának szakítószilárdsága,
- a védőelem megtámasztására szolgáló anyag energiaelnyelő képessége,
- a védőelem felülete és a becsapódó tárgy mozgási iránya által bezárt szög.

Az első két tulajdonság az adott lövedéket tüzelő fegyverektől függ. [5] Az utóbbi két tulajdonság a becsapódáskor megváltozhat, ez adja az okospáncélok fejlesztésének alapját. [6]

A FÉMES HOMOGÉN PÁNCÉLOK ÉS SZEREPÜK AZ ELMÚLT ÉVTIZEDEKBEN

Számos anyagot, illetve anyagok kombinációját kipróbáltak már ballisztikai védőelemként. A nagy darabszámban gyártott, védettséggel rendelkező járművek esetén az ötvözött, hőkezelt acélok felhasználása napjainkban is túlnyomó többségben van. Járművek védelmének esetében jelentős az alakíthatóság igénye, és ez a fémes ballisztikai védőelemek alkalmazhatóságát növeli. Ívelt felületeket például kerámialapokból nehéz előállítani, ilyen esetekben a felületet szegmensekre osztják és egyenes lapokkal borítják be. A mai napig alkalmazásban vannak olyan ballisztikai védelemmel rendelkező gépjárművek, melyeknek a külső borítása, vagy maga a jármű felépítménye azonos fémes anyagból van kialakítva, illetve a jármű kontúrján belül fémes anyagú védőelemet helyeznek el. A védőelemek anyagaként alkalmazhatóak homogén fémlemezek, melyek egymáshoz illesztése oldható vagy nem oldható kötésekkel történik. Az oldható kötés általában csavarkötés, ezt a megoldást gyakran alkalmazzák kiegészítő védőelemek rögzítéséhez is. A nem oldható kötések kialakításának módja lehet hegesztés vagy szegecselés, illetve újabban ragasztás, mely oldószerrel oldható. A nem fémes anyagú védőelemek esetében alkalmazható még például tépőzár, mely az acél esetében, annak tömege miatt, nem jöhet szóba.

A fémes ballisztikai védőelemek anyagszerkezeti tulajdonságokból adódó jellemzői [7]:

- hegeszthetőség,
- hideg alakíthatóság,
- forgácsolhatósági szempontok,
- homogén szerkezet (állandó minőség).

Acélötvözetek, ballisztikai acélok

A ballisztikai acélok a szerkezeti acéloknál jóval nagyobb felületi keménységű és szakítószilárdságú acélok, pontosabban acél ötvözetek. Az elmúlt több mint fél évszázad tapasztalatai alapján a klasszikus fémes alapanyag a nikkel- és/vagy krómötvözésű melegen hengerelt acéllemez. [8; 137. o.]

[1] a lövedéké, illetve a lövedék magjáé

A lemezeket vastagság szerint két csoportba lehet osztani: vékony, azaz legfeljebb 25 mm-es vastagságú, illetve vastag, azaz 25 mm-nél vastagabb lemezekre. A vékony lemezek felületi keménysége többnyire 300 - 400 HB, a vastag lemezeké minimum 275 - 325 HB.

Homogén ballisztikai védőelemek esetén a felületi keménység növelése az egyetlen lehetséges módja a védelmi képesség növelésének anélkül, hogy a tömeg tovább növekedne. A mai korszerű anyagok felületi keménysége a hőkezelési eljárástól függően 400 - 600 HB keménységű, vagy még keményebb is lehet. Ezeknek az anyagoknak a szakítószilárdsága eléri az 1,2 -1,6 GPa-t.

Hajlított védőelemeket harcjárművek esetében az orr rész, illetve a torony kialakításánál alkalmaznak [8; 138. o.], illetve a jármű ülései alatt elhelyezett repeszek elleni védőelemként. A hajlított, ívelt védőelem előnye, hogy a hajlítás miatt a lövedék vagy repesz pályájának hossza gyorsabban növekszik a védőelem anyagában a merőleges találati szögtől való eltérés növelésével, mint egyenes védőelemek esetében. Ezt a pályahosszt a továbbiakban aktuális védőelem-vastagságnak nevezzük.

Más ötvözetek

Alumínium-ötvözeteket már az 1940-es évek eleje óta használtak ballisztikai védelem céljára. Al-Mg (kb. 4%) ötvözet jobb ballisztikai védelmet nyújtott az acélnál a kg/m^2-ben mért, egységnyi felületre jutó tömegének arányát tekintve. Az M113-as harcjármű egyes változatainak páncélzata is ebből készült. A hatvanas évek közepén a brit fejlesztésű felderítő járművek esetében már igény mutatkozott a 14,5 mm-es lövedékek elleni védelemre, mely a mai meghatározás szerint a STANAG 4569 Level 4 szintnek felel meg. [9] Az AA7039 kódnevű ötvözet (Al-Zn-Mg) ellenállt a 14,5 mm-es lövedékeknek, illetve a repeszeknek. [8; 139. o.] [10; 142. o.]

A későbbiekben kipróbálásra kerültek titán-ötvözetek is, melyek kb. 30%-os tömegcsökkenést eredményeztek. A kereskedelemben kapható titán szakítószilárdsága elérheti a 400 MPa-t de megfelelő ötvözés esetében akár az 1 GPa-t is meghaladhatja. Ilyen például a Ti-6Al-4V [10; 142. o.], amely jó ballisztikai védelmet nyújtott, alkalmazása tömegcsökkenést eredményezett és jól hegeszthető volt. Az ötvözet elterjedését és széles körű katonai alkalmazását elsősorban a felmerülő költségek akadályozták.

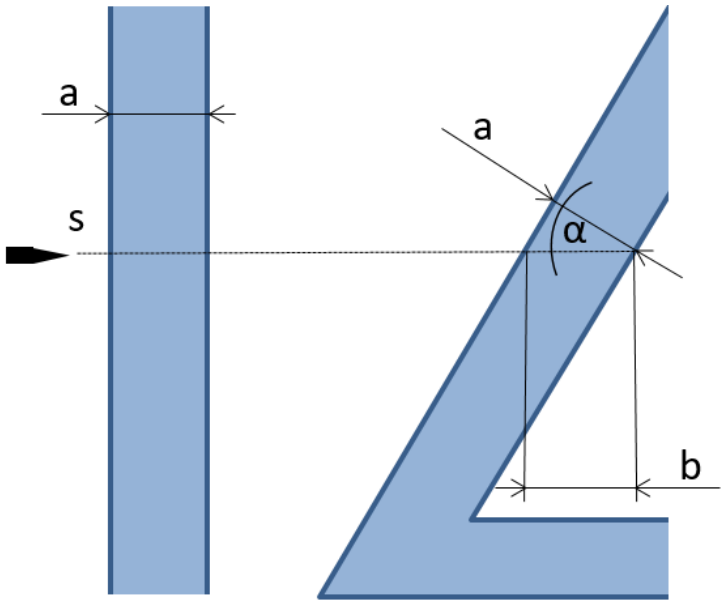
A VÉDŐELEM GEOMETRIÁJÁNAK JELENTŐSÉGE

A ballisztikai védőelemek geometriájának a jelentősége a várható és valós támadási iránytól függ. [8; 136. o.] A támadási irányok valószínűségét a második világháborútól kezdve vizsgálják.[2] Az támadó eszközök találati hatékonysága a célzás pontosságától és a becsapódás irányától. [11] A támadás várható iránya befolyásolja a becsapódás irányát, de egyértelmű, hogy a valószínűséget és a tényleges folyamatot külön kell kezelni egy ballisztikai védőelem védelmi képességének értékelésekor. A haditechnikai eszközök, járművek kiválasztásánál a védelmi szempontok is meghatározóak. [12]

Becsapódáskor a lövedékek pályája a ballisztikai védőelemen halad át. A védelmi szempontokat figyelembe véve a merőleges találati szög a legrosszabb érték. A találati szög a védőelem egyenes felületének síkja, illetve az ívelt felület érintősíkja és a lövedék vagy repesz mozgási iránya által bezárt szög, melyet a következőkben α -val jelölünk. A 2. ábra szemlélteti az aktuális védőelem-vastagság változását a találati szög változásának függvényében. Amennyiben a lövedék pályája (s) és a védőelem felülete a találkozási pontban

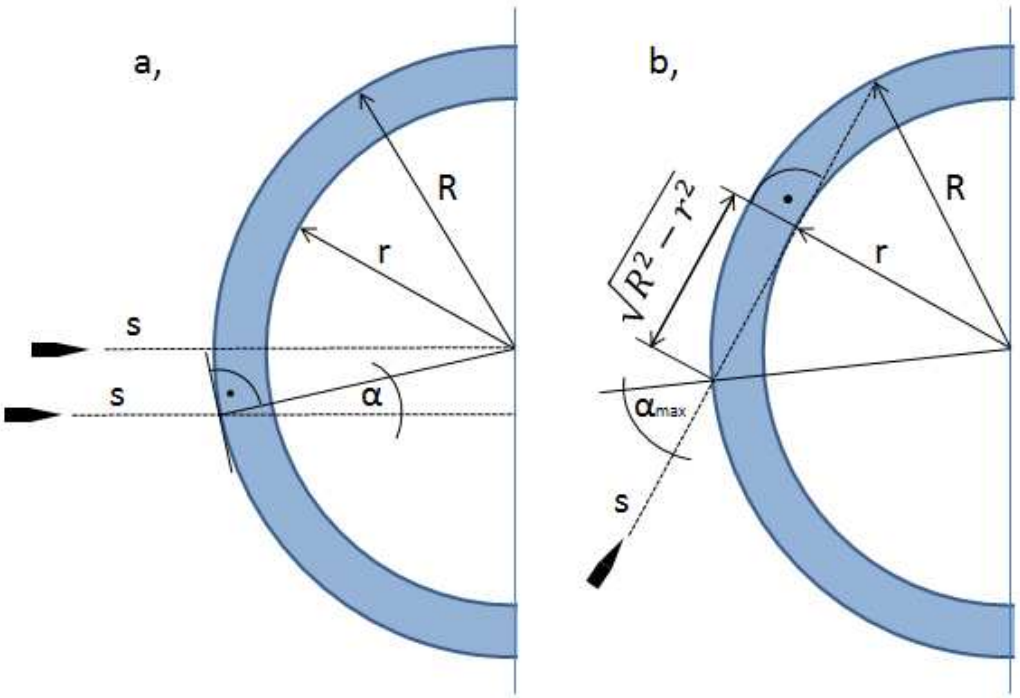
[2] Lt-Col Whittaker tett először komoly kísérletet arra, hogy elemezze a valószínűségét az egyes irányokból érkező támadásoknak. A módszere a DPV, azaz directional probability variation – azaz irányvalószínűségi variáns meghatározta a harckocsik fejlődését. A mai korszerű analitikai módszerek már sokkal komplexebbek, és pontosabbak.

nem 90°-os szöget zár be, úgy nem a védőelem vastagsága (a) hanem az aktuális védőelem-vastagság (b) a mérvadó. Az ábra alapján a lemez felületének vízszintessel bezárt szögét alapul véve, és az egyszerűség kedvéért feltételezve, hogy a lövedék mozgási iránya is vízszintes, az aktuális védőelem-vastagság értéke koszinusz szögfüggvény alapján számítható.



2. ábra Az aktuális védőelem-vastagság változása egyenes és döntött felület esetén (saját szerkesztés)

$$b = \frac{a}{cos\alpha} \tag{1}$$



3. ábra Az aktuális védőelem-vastagság változása ívelt felület esetén (saját szerkesztés)

Első eset - merőleges becsapódás

Ívelt védőelem-felület esetén (3. ábra) több becsapódási esetet kell különválasztani. A legegyszerűbb eset, amikor a lövedék mozgási iránya és a felület érintője egymásra merőlegesek, ekkor az aktuális védőelem-vastagság értéke a szelvény külső (R) és belső sugarának (r) a különbsége (ahol természetesen $r < R$):[3]

$$b = R - r \tag{2}$$

Második eset - ferde becsapódás

A második eset, amikor a lövedék mozgási iránya nem 90°-os szöget zár be az felület érintősíkjával, de a védőelem belső kontúrvonalán is áthalad, azaz $0 < \alpha$. Ebben az esetben az aktuális védőelem-vastagság a 3/a. ábra alapján a koszinusztétel segítségével számítható:

$$r^2 = b^2 + R^2 - 2bR\cos\alpha, \tag{3}$$

ahol r, R és α ismert. Az egyenletet rendezve és b-re megoldva kapjuk:

$$b^2 - (2R\cos\alpha)b + (R^2 - r^2) = 0 \tag{4}$$

$$b_{1,2=}\frac{2R\cos\alpha \pm \sqrt{(2R\cos\alpha)^2 - 4(R^2 - r^2)}}{2} \tag{5}$$

$$b_{1,2=}\frac{2R\cos\alpha \pm \sqrt{4R^2\cos^2\alpha - 4(R^2 - r^2)}}{2} \tag{6}$$

$$b_{1,2=}R\cos\alpha \pm \sqrt{R^2\cos^2\alpha - R^2 + r^2}, \tag{7}$$

ahol a két megoldás közül csak a negatív előjelű ad fizikailag értelmes megoldást: α helyére pl. 0-t helyettesítve a pozitív előjeles megoldás a két görbületi sugár összegét adja maximális pályahossznak, ami nyilvánvalóan csak az egyenlet matematikai megoldása és nem a fizikai problémáé.

A negatív előjelet használva $\alpha = 0$ esetén visszakapjuk az előző eset $R - r$ megoldását, illetve α -t folytonosan növelve egy folytonosan növekvő függvényt kapunk eredményül. Az α szög azonban nem növelhető 90°-ig, mivel akkor a négyzetgyök alatt $r^2 - R^2$ állna, ami nyilvánvalóan negatív. Kell tehát lennie egy α_{max}-szal jelölt határszögnek, ahol a négyzetgyök alatt álló kifejezés éppen nulla. Ez a második eset érvényességét tehát az $0 < \alpha < \alpha_{max}$ szögtartományra korlátozza.

Harmadik eset - a határszög esete

A harmadik eset a határeset, amikor a lövedék pályája éppen érinti a belső kontúrvonalat, azaz amikor a találati szög és a határszög értéke megegyezik ($\alpha = \alpha_{max}$). Ekkor az aktuális védőelem-vastagság a 3/b. ábra alapján Pitagorasz tétel segítségével számolható: a derékszögű

[3] Az aktuális védőelem-vastagság matematikai leírása a szerzők saját munkája.

háromszög átfogója *R*, egyik befogója *r*, másik befogója pedig az aktuális védőelem vastagság fele, azaz

$$R^2 = \left(\frac{b}{2}\right)^2 + r^2. \tag{8}$$

Ebből *b*-t kifejezve:

$$b_{max} = b = 2\sqrt{R^2 - r^2}. \tag{9}$$

Ez az érték az aktuális védőelem vastagság maximális nagysága (b_{max}). Ezt felhasználva a derékszögű háromszögre felírva a koszinusztételt az esetre jellemző határszög, α_{max} értéke is számítható:

$$r^2 = R^2 + (R^2 - r^2) - 2R\sqrt{R^2 - r^2}\,\cos(\alpha_{max}) \tag{10}$$

$$\alpha_{max} = arccos\left(\frac{2R^2 - 2r^2}{2R\sqrt{R^2 - r^2}}\right). \tag{11}$$

Negyedik eset - átütés nélküli becsapódás

A negyedik esetben a lövedék olyan lapos szög alatt érkezik, hogy pályája a belső kontúrvonal érintése nélkül teljes egészében a védőelem anyagában van (azaz $\alpha > \alpha_{max}$), ezért ekkor a védőelem vastagsága a védett terület szempontjából már nem játszik szerepet.

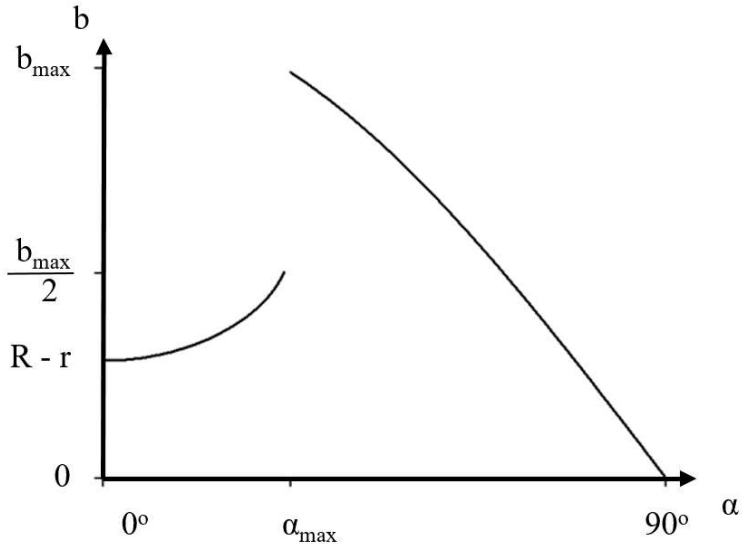
Ebben az esetben a lövedék pályájának és az *R* sugarú körnek a két metszéspontja az *R* sugarú kör középpontjával egy olyan egyenlő szárú háromszöget alkot, melynek két oldala *R*, harmadik oldala *b* nagyságú. Mivel egy háromszög belső szögeinek összege 180°, α ismeretében az ismeretlen harmadik belső szög is kifejezhető. Erre a háromszögre is felírva a koszinusztételt, az aktuális védőelem-vastagság meghatározható:

$$b^2 = R^2 + R^2 - 2RR\cos(180° - 2\alpha) \tag{12}$$

$$b = \sqrt{2R^2 - 2R^2}(-\cos(2\alpha)) \tag{13}$$

$$b = \sqrt{2R^2(1 + \cos(2\alpha))} \tag{14}$$

Az aktuális védőelem-vastagság változását a becsapódási szög függvényében ívelt védőelem esetén a 4. ábrán mutatjuk be grafikusan (az $R = 2r$ esetre). Látható, hogy az aktuális védőelem-vastagság a becsapódási szög növelésével eleinte növekszik, majd az α_{max} határszög elérése után folytonosan csökken nulláig, ami annak az esetnek felel meg, amikor a lövedék pályája éppen elkerüli a védőelemet. Az α_{max} határszög elérésekor az aktuális védőelem-vastagság ugrásszerűen a kétszeresére nő: ez a 3/b. ábra esete, amikor a lövedék védőelembeli pályája már éppen nem metszi a belső kontúrvonalat.



4. ábra Az aktuális védőelem-vastagság változása a becsapódási szög függvényében ívelt védőelem esetén (saját szerkesztés)

KÖVETKEZTETÉSEK

A publikáció röviden bemutatta a homogén fémes ballisztikai védőelemek legfontosabb anyagait, kialakítását, a merőleges találati szögtől való eltérés hatását az aktuális védőelem-vastagságra. Matematikai levezetéssel pontosan meghatározható a találati szög fontossága a ballisztikai védőelemek védelmi képességeinek tekintetében. A publikáció csak olyan esetekkel foglalkozott, amikor a lövedék pályája a becsapódás után egyenes vonalúnak tekinthető, és nem tér ki a feltételezett vízszintes síkból. A találati szög, a cikkben tárgyalt egyszerűsített esetben meghatározó függőleges, és vízszintes síkokhoz képest a valóságban eltér. A jellemző összefüggéseket célszerű a most tárgyalt összefüggések alapján kifejteni.

FELHASZNÁLT IRODALOM

[1] SZAKÁL Z., KALÁCSKA G., GÁVAY GY., GYARMATI J.: Evaluation Methods for Different Armors Hit by Bullets; International Multidisciplinary Conference: 11th Edition. Nyíregyháza: Bessenyei Publishing House, 2015., 151-156. o.

[2] GÁVAY GY., GYARMATI J., SZAKÁL Z., KALÁCSKA G.: Evaluation of bullet resistance of different steel alloys in army application; Proceedings of the International Scientific Conference on Advances in Mechanical Engineering (ISCAME 2014). Debrecen: University of Debrecen Faculty of Engineering, 2014. pp. 34-42.

[3] BOMBAY J., GYARMATI J., TURCSÁNYI K.: Harckocsik 1916-tól napjainkig, Zrínyi kiadó, Budapest, 1999., 14-15. o.

[4] BØRVIK, T., HOPPERSTAD, O.S., PEDERSEN, K.O.: Quasi-brittle fracture during structural impact of AA7075-T651 aluminium plates; International Journal of Impact Engineering vol. 37 pp. 537-551, DOI: 10.1016/j.ijimpeng.2009.11.001 (letöltve: 2016.12.20.)

[5] GYARMATI J.: A nehézpuskát jellemző szempontok fontosságát kifejező súlyszámok számítása és statisztikai vizsgálata, HADITECHNIKA 2006:(2) 11-16. o.

[6] Army TARDEC, Warren, Michigan: Reactive Structure and Smart Armor for Future Ground Vehicles http://www.aerodefensetech.com/component/content/article/12841 (letöltve: 2016.12.01.)

[7] FRANK GY.: Páncélozott pénz és értékszállító biztonsági gépkocsik. Budapest : Zrínyi Miklós Nemzetvédelmi Egyetem, 2000., 53. o.

[8] TYTLER, I.F.B.: Vehicles and bridging; Brassey's Defence Publication, 1985.
[9] NATO STANAG 4569 - PROCEDURES FOR EVALUATING THE PROTECTION LEVELS OF LOGISTIC AND LIGHT ARMOURED VEHICLES FOR KE AND ARTILLERY THREATS, p. 6., http://www.alternatewars.com/BBOW/Ballistics/STANAG_4569_Ed2.pdf (letöltve: 2016.12.21.)
[10] Opportunities in protection materials science and technology for future army applications. Washington D.C.: The National Academic Press. DOI: 10.17226/13157
[11] GYARMATI J., KENDE GY., TURCSÁNYI K., Tüzérségi tűzvezető rendszerek összehasonlítása KATONAI LOGISZTIKA 2002:(2) 137-161. o
[12] TURCSÁNYI K., KENDE GY., GYARMATI J.: Haditechnikai eszközök összehasonlításának korszerű módszerei és ezek alkalmazása: HM 2002. évi kutatási terv 6.1. program 1. alprogram Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2002. 64 o.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

THE ROLE OF INFORMATION OF THE POPULATION IN ELIMINATION OF ACCIDENTS INVOLVING DANGEROUS SUBTANCES

LAKOSSÁG TÁJÉKOZTATÁSÁNAK SZEREPE A VESZÉLYES ANYAGOKKAL KAPCSOLATOS BALESETEK FELSZÁMOLÁSÁBAN

BENYE János

(ORCID: 0000-0003-0132-9425)

jbenye69@gmail.com

Abstract

The activities of disaster management organizations are especially important in liquidation of accidents involving dangerous substances and handling of evolved emergencies. One segment of the public protection task system is the information of the popullation, which also plays an important role in elimination of damage besides primary intervention. The nowaday challenges of disaster management are mainly linked to natural and industrial disasters, therefore in this paper I aim to examine the population information's tasks on efficient elimination of major accidents involving dangerous substances might entering the environment. I demonstrate each subtask by illustrating specific examples, highlighting their importance in prevention and in effective damage cleanup. By my research work I wish to highlight the topicality of the subject, also to assist professionals engaged in information tasks.

Keywords: *dangerous substances, industrial disasters, civil protection, information of the population*

Absztrakt

A katasztrófavédelmi szervezetek tevékenysége a veszélyes anyagokkal kapcsolatos balesetek felszámolásában, a kialakult veszélyhelyzetek kezelésében különösen fontos. A lakosságvédelmi feladatrendszer egyik szegmense a lakosságtájékoztatás, mely az elsődleges beavatkozás mellett szintén fontos szerepet játszik a kárfelszámolásban. Korunk katasztrófavédelmi kihívásai elsősorban a természeti és ipari katasztrófákhoz kapcsolhatók, ezért egy esetleges veszélyes anyag környezetbe jutásával járó baleset hatékony felszámolását nagyban segítő lakosságtájékoztatási feladatokat vizsgálom írásomban. Konkrét példák szemléltetése során mutatom be az egyes részfeladatokat, kiemelve azok jelentőségüket a megelőzésben, valamint a hatékony kárfelszámolásban. Kutatómunkámmal rá kívánok világítani a téma aktualitására, továbbá segítséget nyújtani a tájékoztatási feladatokat végző szakembereknek.

Kulcsszavak: *veszélyes anyagok, ipari katasztrófák, lakosságvédelem, lakosság tájékoztatása*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.13
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.21.

INTRODUCTION

The increasing use of dangerous substances is a necessary consequence of the ongoing social and economic development. Activities involving dangerous substances inherently carry the risk of an occuring accident. One has to take into account occuring accident not only during production, storage or usage at site, but also by the occasion of road, rail, air or sea transport. The members of the organizations engaged in elimination of damage, has to face in more and more cases with dangerous substances during the interventions every day. [1]. The units of disaster management has to respond to increasingly complex tasks faster and faster, more and more professionally, while in many cases these tasks should be carried out by the presence of dangerous substances [2]. Some changes were made in the disaster management system in response to the challenges caused by incidents of various dangerous substances. The examination of the full range of changes is restricted by the size limitations of this essay, therefore I analyze only the information of the population roles related to the topic, furthermore I also examine the role of notification in the activities of prevention and damage elimination.

RELATION OF PREVENTION AND NOTIFICATION

In terms of protection against disasters, the European Union (hereinafter referred to as EU) puts great emphasis on adequate information of the population, in order to effectively prepare and response to the natural and man-made factors riskful to population, furthermore emphasizes the continuous flow of information related to the management of the events occurred. In Hungary a unified disaster management organization was created in 2012, whose task system includes information of the population tasks at the highest priority level. Information of the population related to dangerous substances should be divided into two task groups, one group of normal or accident-free period notification, the other group covers information of the population tasks in case of emergency or accident.

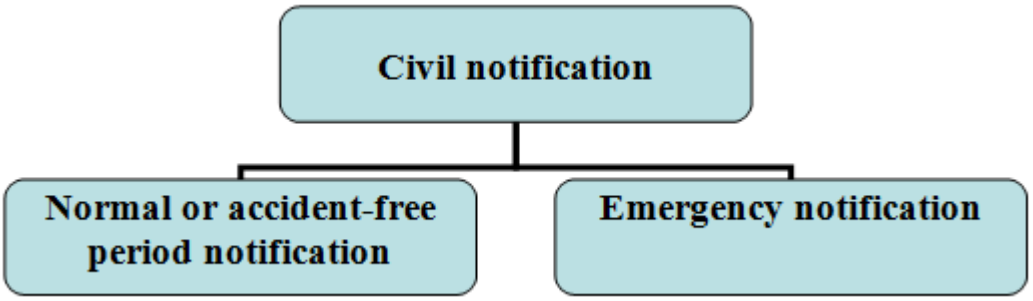


Figure 1. Groups of informatiion of the population, (Source: Author compilation based on [3] Data)

One of the main element of protection against disasters is prevention, which the organization puts large emphasis on. The Act CXXVIII of 2011 on Protection against Disasters in force from 2012 (hereinafter referred to as Disaster Management Act) significantly changed the system of protection against disasters in our country.

The endangerment of disaster had to be assessed at municipal level, and adequate notification and preparation became necessary among the affected population.

The preparation as a key element of the preceding period, represents such tasks in the activities of the organizations affected against disasters defense that can guarantee [3]:

- emergency alert signals and conscious recognition of notices,

- the high proportion of people able to act,
- the expected ability to apply rules of conduct and,
- the increase of self-rescue skills.

It is clear from the above lines that the state puts emphasis on information of the population, however for effective prevention and pretection the involvement of the public is needed, since the population can receive serious tasks in the implementation of provisions of the Act. The public is also responsible, has obligation to notice the hazards of it's immediate vicinity, to possess sufficient knowledge and information adequate to survive and escape from danger, as well as to actively participate in the protection processes. It is particularly important to understand the risk and the appropriate action sequence in case of accidents involving dangerous substances. In favor of effective prevention the government widened the range of controls that cover all areas related to dangerous substances.

Accidents may occur in relation to dangerous substances in the following areas [4]:

- production,
- transport,
- storage, stockage,
- utilization,
- elimination.

The audit had to be extended to all areas, therefore the law has filled a long-time explored gap with creating conditions of the official and threat control of plants below the lowest threshold, and for its implentation has established among other things a national competence general inspectorate, the National Directorate General for Disaster Management [5]. Thus a supervisor authority was formed over many years of research and practical application that can comprehensively verify the dangerous substances producers, suppliers and user organizations. The range of causes of hazards include a variety of flammable and explosive shipments, as well as toxic road and rail cargo. In order to prevent accidents using the analysis realistic plans and organizations should be constitued for the expected tasks [6]. The plans should include analysis of the threats, tasks related to ensure preparation for alarm the population (employees), by the acquisition and allocation of the protective equipment, by providing the protective facilities, the necessary fire-fighting, technical rescue, decontamination, medical equipment, etc; by the possible evacuation, organizing rescue services, tasks related to management and cooperation. So without them the complex technical rescue targeting the elimination of possible accidents would be prolonged for a long time [7].

INFORMATION OF THE POPULATION IN PRACTICE

Areas are above presented where accidents involving dangerous substances may occur. From civil protection point of view, accidents are the greatest risk occurring in residential areas, and within those the industrial disasters [8]. In the past, other factors were involved during the installation of the plants, so more plants are located within a residential area, or near of it. The possible occurrence of a technological accident, whereupon dangerous substances could get into the environment, is a serious threat to the population. In Hungary, due to the strict regulatory requirements, industrial accidents rarely occur, but the probability of occurrence is not zero, thus informing the public living in the vicinity of dangerous plants, and preparing for the correct action plan in case of accident, both should be emphasised.

The information of the population and preparation shall be conducted at such level that in case of an emergency, everyone is able to apply theoretical knowledge in practice. Raising the capacity of receptive skills should begin at early age so that adults can be receptive people. The 3x3 Action Plan for Children and Youth Training has been announced at the National Disaster Management Directorate, Interior Ministry, which defines methods of providing basic information specifically for the young - and open to percieve new informations,

however the most vulnerable – age groups. During the implentation of the Action Plan, alarms, notifications and emergency information also plays an important role among the training topics. The Action Plan engaged in public training deals with other age groups as well, but pays special attention on children. There is no point in increasing the sense of threat in the population to such level, that would perpetuate the sense of fear. For this purpose by the newly developed instructory/preparatory/informative documents rather security-oriented approach is preferred. At present, the priority target group is of children, because their mind can be considerably influenced and formed towards a direction, where the need for security, preventive approach and active participation against disasters becomes automatic. The importance of preparing young people is outstanding, because in the future they will be able effectively contribute to protection against disasters.

The chapters of Seveso II. Directive, recording EU standards, on the protection against major industrial accidents involving dangerous substances, has been adopted in the disaster management law, which has implemented the prevention of sever industrial accidents, and introduced activities reducing harmful consequences of accidents in our country. Disaster management is tasked by law to control state responsibilities related to prevention of major industrial accidents, and to ensure their supply.

According to the Disaster Management Act executives of industrial plants has managerial responsibility to asses risks of dangerous material present in the plants, to the determine the effects occuring during realistically assumed major industrial accidents, as well as to take preventive actions in the plants to protect the public and the environment. These informations are contained by the safety assessment of the dangerous plant. The safety report of dangerous plantations should be accessible to everyone in the local mayor's office. The plant makes internal emergency plan, whose content laid must be ensured all times. The staff of the plant is responsibile to take every expectable action to prevent major industrial accidents and to mitigate the effects of the accidents occured in-house. The mayor of the settlement to treat unexpected unusual events - in cooperation with regional organizations of professional disaster management - prepares external emergency plan, which sets out the tasks for the protection of the population, of tangible property and environment, the conditions related to their implementation, forces and resources. The affected population's own interest to get to know the surrounding dangers, and to be able to cooperate with rescue forces for it's environment and own safety. [9].

For the more efficient implementation of these tasks the Disaster Management Act assigned to mayors of settlements located close to dangerous upper-treshold value plantations to prepare civil information publications as a task.

Active forms are such as the edition of civil information substances, publishing publications, to organize civil forums, passive forms are such as making available these publications, to organize open days of disaster management [10]. An important clause of the edict, that in those settlements, where the number of minority population reaches 5%, there the information brochures must be published in the ethnical language as well.

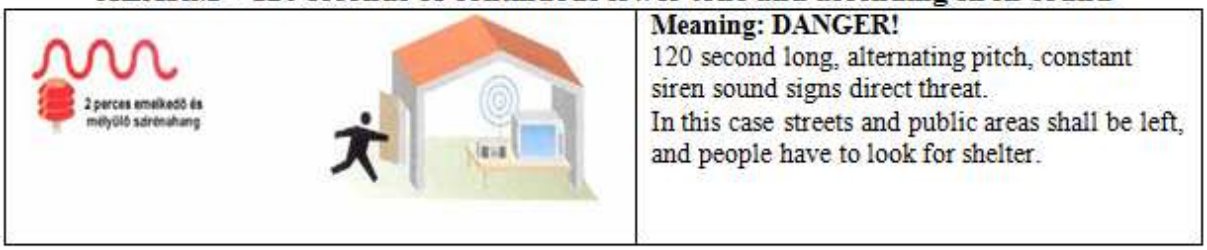
The Regulation sets specific requirements for the content of the active information of the population brochures also concerning [10]

- preparing the population of the alarm signals and methods of identifying,
- the rules of conduct to be followed,
- forms of assistance,
- threatening the natural and human risks specific area,
- the possible ways of countering threats.

Top priority task to install and to keep continuously operating the alarm systems, in lack of this alerting the population can not be performed smoothly. For alarm purpuses siren alarm system was built in Hungary, whose serviceability is continuously monitored. The alarm

occurs by defined siren signals, therefore civil informational publications should contain explanations for the detection of alarm signals, which are explained below.

ALARM – 120 seconds of continuous lower tone and ascending siren sound



DANGER IS OVER – 2 x 30-second continuous steady tone, with a 30 second pause

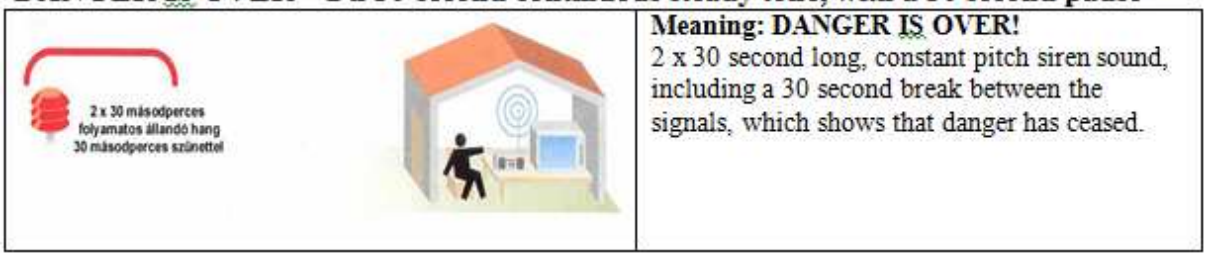


Figure 2. Siren Signals [11]

The above siren signs do not inform on the type of a threat, on the necessary countermeasures, or on detailed information for defense; so the residents can get additional instructions via loudspeaker, the radio, the television, or mobile applications. In order that the inhabitants of the emergency affected areas are able to avoid bodily harm and maintain their health, it is important to comply with the rules of conduct, which are illustrated in the following figures.

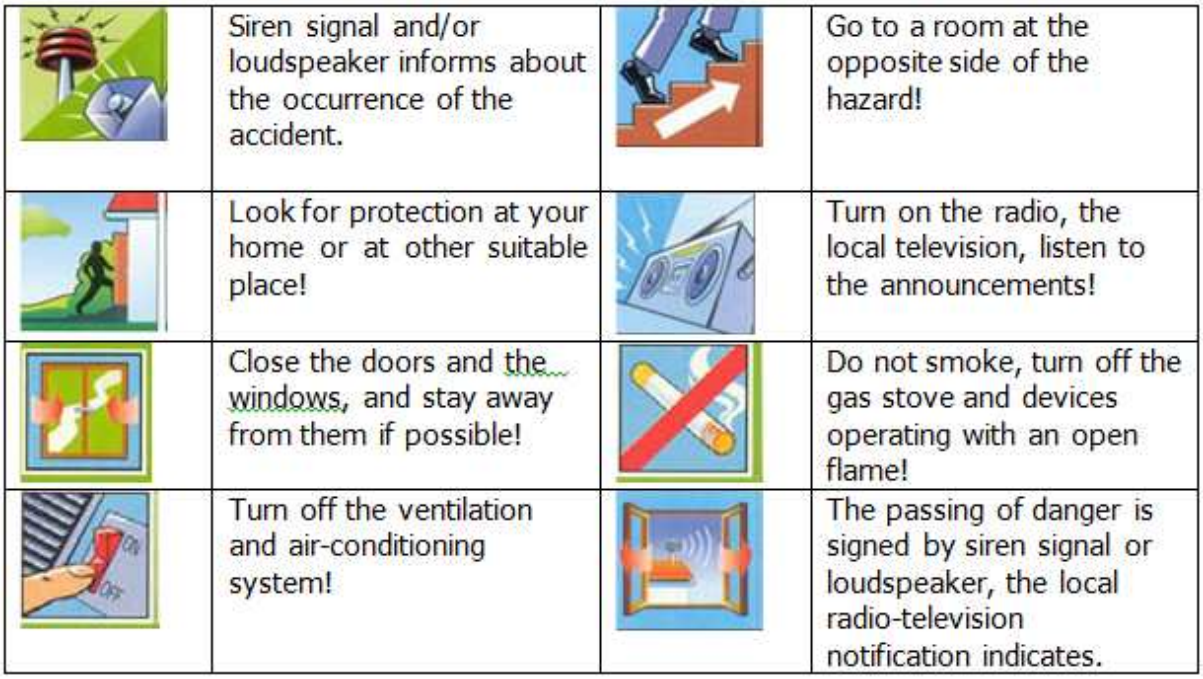


Figure 3. Rules of correct conducts [11]

The publications include forms of providing aid, these are especially important in case of accident related to dangerous substance. An important task is to prepare civil protection and other rescue forces which can be involved in assistance, training if necessary, to supply with equipments, the organization and support of communication, the acquisition of individual protective equipment against the effects of dangerous toxic substances and to keep them alert [12].

The knowledge upon the local threatening risks is important for the population, especially for those who live in the vicinity of a plantation which produces, stors or processes dangerous substances. The disaster management assesses these risks by using advanced/modern risk analysis techniques. These publications shall include the methods of threat defence, covering the public security tasks particularly.

TASKS IN CASE OF CHEMICAL ACIDENTS

In order to reduce consequences of incidents in dangerous industrial plants involving dangerous substances the operator is accountable of the construction and maintenance of safety facilities, operation of an efficient warning system, as well as to be standby on the forces and appliances necessary for eliminating an accident. During installation and operation of the protective equipment special efforts should be done so that a complex technical rescue averting a possible chemical accident will be carried out in the shortest possible time with the greatest efficiency. Continuous exploration and assessment of the situation is essential for the correct and accurate emergency information [13]. Emergency notification is primarily a duty of official disaster management organizations. The information is specifically restricted to the rules of conduct to be kept, to the civil protection arrangements taken or expectable by the authorities, to the notification of important public constraints and to the opportunities for further inquiry. Issuing the notices particular attention should be taken to providing interpretable and useful information a broad layers of the population, therefore editors must refrain from certain technical terms and complex composition [14]. If there is work to be performed outside of the particular plant during elimination, such as decontamination tasks, then it is necessary to inform the public about these concretely in order to avoid panic situation [15]. The emergency information lasts until remediation is completed.

CONCLUSIONS

If we consider exposure to threat caused by natural and man-made disasters, we can gain insight that the new millennium brought new requirements and with it new and severe tasks falling to the implementation of disaster management organizations. One of the main tasks of complex disaster management system is to prevent catastrophes, which activity would not be effective without adequate information of the population. It can be stated, that the elimination of harmful effects of an occuring disaster and saving human lives can be greatly assisted by the appropriate communication, targeted information.

SUMMARY

The number of chemical substances processed has grown steadily, therefore the risk of possible incidents also. In 2012 a unified disaster management organization was established in Hungary whose task system includes information of the population tasks at the highest priority level. The overall conclusion is that the legislative environment to ensure a functioning system consolidates the information of the population with unified legal framework focusing on disaster management. The primary objective of modifications is the prevention of catastrophes, in which information of the population plays an important role,

however, occurence of accidents involving dangerous substances is expectable in the future as well, so preparation and training of the public sector is also a major task in this system. In this paper I have examined the information of the population tasks highly assisting efficient elimination of major accidents involving dangerous substances entering the environment, covering all the sub-areas. By this research I wished to draw attention to the importance of the topic, the application of the procedures and methodes described in the article may assist the practical tasks.

BIBLIOGRAPHY

[1] KUTI R.: Advantages of Water Fog Use as a Fire Extinguisher, AARMS Academic and Applied Researc in Public Management Science 14. 2. pp. 259-264. (2015) http://uni-nke.hu/uploads/media_items/aarms-2015-2-nyomdai.original.pdf (downloaded: 04. 12. 2016.)

[2] KUTI R., FÖLDI L.: Possible use of mobile water fog generators for decontamination tasks, AARMS Academic and Applied Research in Military 8. 1. pp. 127-132. (2009) http://www.zmne.hu/aarms/docs/Volume8/Issue1/pdf/12kuti.pdf (downloaded: 04. 12. 2016.)

[3] MÓGOR J., BONNYAI T.: A katasztrófavédelem lakosságtájékoztatási módszerei és eszközei, Védelem Online: Tűz- és Katasztrófavédelmi Szakkönyvtár, 730. 1-7. o. (2016) http://www.vedelem.hu/letoltes/anyagok/730-a-katasztrofavedelem-lakossagtajekoztatasi-modszerei-es-eszkozei.pdf (downloaded: 04. 12. 2016.)

[4] KUTI R., ZÓLYOMI G.: Intézkedési algoritmus veszélyes anyag balesetek felszámolásához, Védelem katasztrófa- tűz– és polgári védelmi szemle, XV. 4. (2008) 14-15. o.

[5] HOFFMANN I., LÉVAI Z., KÁTAI-URBÁN L., VASS Gy.: Iparbiztonság Magyarországon, Védelem Online: Tűz- és Katasztrófavédelmi Szakkönyvtár, 549. 1-12 o. (2015) http://www.vedelem.hu/letoltes/anyagok/549-dr-hoffmann-imre-dr-levai-zoltan-dr-katai-urban-lajos-dr-vass-gyula.pdf (downloaded: 28. 12. 2016.)

[6] KÁTAI-URBÁN L.: Iparbiztonsági képzés és továbbképzés kialakulása és fejlesztése, 2. rész: Az iparbiztonsági képzési igények és követelmények értékelése, HADTUDOMÁNY 25. 1-2. (2015) 57-68. o.

[7] KUTI R.: Komplex műszaki mentések tervezésének lehetőségei, Védelem Online: Tűz- és Katasztrófavédelmi Szakkönyvtár, 233. 1-7. o. (2010) http://www.vedelem.hu/letoltes/anyagok/233-komplex-muszaki-mentesek-tervezesenek-lehetosegei.pdf (downloaded: 28. 12. 2016.)

[8] NAGY K., HALÁSZ L.: Katasztrófavédelem, Egyetemi jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2002.

[9] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[10] 62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól

[11] CIMER ZS at. al.: Hegymegi Ildikó (szerk.) Mi a teendő vegyi baleset esetén?: Segédleg a súlyos balesetek elleni védekezés lakossági tájékoztató kiadvány elkészítéséhez. pp. 1-46. (2003)

[12] KUTI R.: A tűzoltóképzés sajátosságai Ausztriában, Védelem katasztrófa- tűz- és polgári védelmi szemle, XV. 6. 30-31. o. (2008) http://www.vedelem.hu/letoltes/ujsag/v200806.pdf?13 (downloaded: 28. 12. 2016.)

[13] KUTI R.: Veszélyes anyag balesetek felderítését támogató eszközök a svájci tűzoltóságnál, Védelem katasztrófa- tűz– és polgári védelmi szemle, XIX. 3. 26-27. o. (2012) http://vedelem.hu/letoltes/ujsag/v201203.pdf (downloaded: 28. 12. 2016.)

[14] MÓGOR J.: A lakossági tájékoztatás és a nyilvánosság biztosításának kutatása a súlyos ipari balesetek elleni védekezésben. PhD értekezés, Budapest 2011 http://193.224.76.4/download/konyvtar/digitgy/phd/2010/mogor_judit.pdf (downloaded: 28. 12. 2016.)

[15] KUTI R., FÖLDI L.: Possible use of mobile water fog generators for decontamination tasks, AARMS Academic and Applied Research in Military Science 8. 1. pp. 127-132. (2009) http://www.zmne.hu/aarms/docs/Volume8/Issue1/pdf/12kuti.pdf (downloaded: 28. 12. 2016.)

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

ATOMERŐMŰVI BALESETEK ÉS ÜZEMZAVAROK TANULSÁGAI 1.

NUCLEAR POWER PLANT ACCIDENTS AND MALFUNCTIONS, LESSONS LEARNED 1.

DOBOR József; KOSSA György; PÁTZAY György

(ORCID: 0000-0003-0191-4261); (ORCID:0000-0002-4404-2929);
(ORCID: 0000-0002-5541-8012)

dobor.jozsef@uni-nke.hu; info@intertanker.hu; patzay.gyorgy@uni-nke.hu

Absztrakt

A nukleáris energia jelentősége hazánkban számottevő, Magyarország energiastratégiájának egyik pillére. Nemzetközi értékelések alapján kevésbé veszélyes, mint a fosszilis energiahordozók használatát kísérő veszélyek. A jelentős társadalmi előítélet az elmúlt évtizedekben bekövetkezett káreseményeknek tulajdonítható. A cikk ismerteti az elmúlt évtizedek legjelentősebb nukleáris baleseteit, okait és tanulságait. A publikáció két részben kerül közlésre. Az ismertetett balesetek minden esetben műszaki-tervezési hiányosságok következményei és emberi hibákkal/tényezőkkel képeznek direkt kapcsolatot. Az írás kitér arra, hogy minden káresemény több – sokszor egymástól független – hiba okozataként következik be.

Kulcsszavak: *atomerőművi balesetek, Windscale, Three Mile Island, Chernobil, Fukushima, okok, következmények*

Abstract

Nuclear energy plays an important role in Hungarian energy production. According to frequency-consequence curves for severe accidents in various energy chains fatality rates are lowest for western hydropower and nuclear power plants. On contrary the large nuclear disasters (Chernobyl, Fukushima) caused a negative publicity to nuclear energy. In this paper the four significant nuclear energy disaster in last decades is discussed, including reasons and consequences. Paper has two parts. In these disasters technical, construction errors and deficiencies are the main reasons and human errors are only consequence of existing danger.

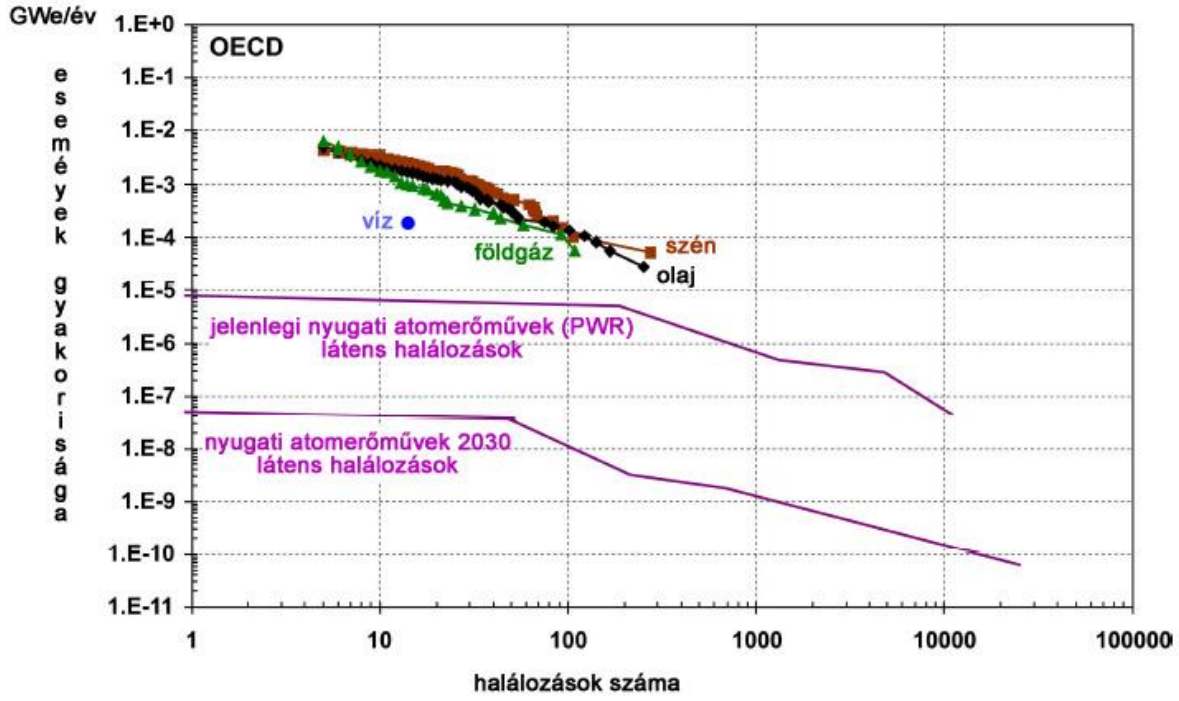
Keywords: *Nuclear energy disasters, Windscale, Three Mile Island, Chernobyl, Fukushima, reasons, consequences*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.06.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.22.

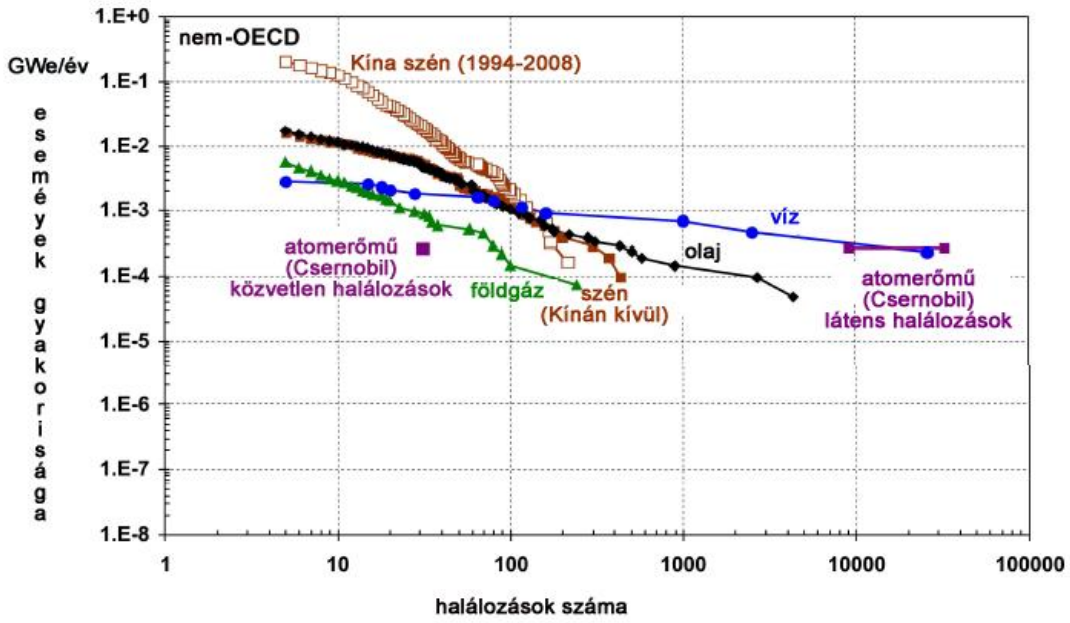
BEVEZETÉS

Az atomenergetika elmúlt évtizedeiben négy komoly atomerőművi baleset és számos üzemzavar következett be. Ezen nem kívánatos események részleges tanulságait és a levonható következtetéseket kívánjuk tárgyalni. Az a tény közismert, hogy az atomerőművek üzemi biztonságával szemben kezdettől fogva maximális követelményeket írtak elő és igyekeztek a biztonsági követelményeket betartani és betartatni. Mégis az elmúlt évtizedekben az egész világra, a közvéleményre, a politikára, az iparbiztonságra jelentősen kiható balesetek és üzemzavarok következtek be, melyeknek tanulságait a mai napig elemzik, értékelik és az atomerőművek biztonságát befolyásoló technikai és szervezési eljárásokat, előírásokat újra és újra átdolgozzák. Cikkünkben röviden összefoglaljuk az eddig bekövetkezett négy legsúlyosabb atomerőművi baleset eseményeit, tanulságait és a levonható következtetéseket.

Az 1-2. ábrák jól mutatják [1], hogy a fejlett és fejlődő világ energiaiparában bekövetkezett baleseti közvetlen és látens halálozások gyakorisága 1,0-1,5 nagyságrenddel kevesebb az atomerőművekben bekövetkezetteknél, mint a fosszilis alapú és vízenergia termelő erőműveknél.

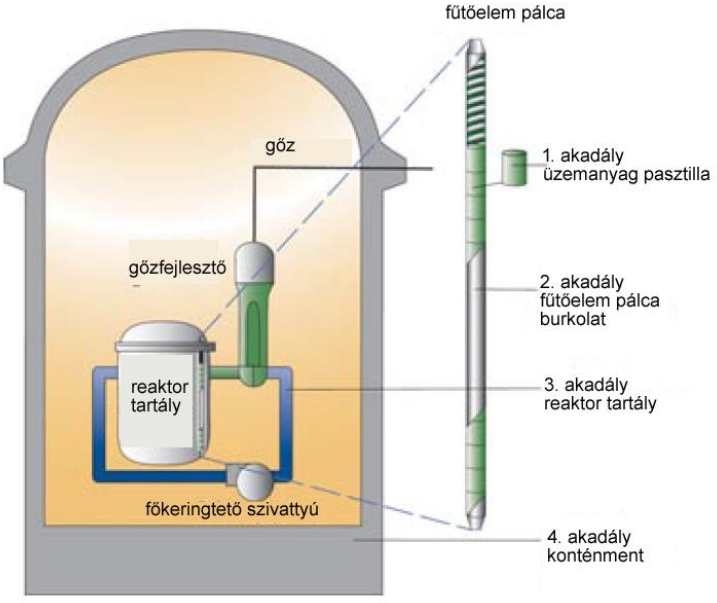


1. ábra OECD országok (1970-2008) energiaiparában a halálozások száma –frekvencia összefüggés [1]



2. ábra nem-OECD országok (1970-2008) energiaiparában a halálozások száma –frekvencia összefüggés (a szerzők szerkesztése a [1] alapján)

Az atomerőművek fő biztonsági alapelve [2] szerint: a tervezés, építés, indítás és üzemelés során sohasem bocsáthat ki a lakosságra káros nagy mennyiségű radioaktív anyagot. Ezt a mélységi védelem filozófiájával biztosítják, a radioaktivitás környezetbe való kikerülését nagyszámú egymás utáni gátakkal akadályozzák meg. A 3. ábrán egy *nyomott vizes* (PWR) atomerőmű sémája [2] mutatja, hogy az orosz „matrjoska babához" hasonló egymásba ágyazott védelmi gátak akadályozzák a radioaktív anyagok környezetbe jutását.



3. ábra A védelmi gátak rendszere (a szerzők szerkesztése a [2] alapján)

Három biztonsági szintet alkalmaznak annak megakadályozására, hogy egyik gát se kerüljön veszélybe olyan rendkívüli esemény, mint berendezés meghibásodás, emberi hiba, vagy természeti jelenség következményeként:

1. Maximális biztonságot terveznek a normális üzemre és maximális tűrési képességet rendszer hibák esetére. Természeténél fogva (inherens) konstrukciós elveket alkalmaznak a biztonságos üzemeléshez, első rendűen fontos a minőség, a túlméretezés, az ellenőrizhetőség és vizsgálhatóság biztosítása üzembevétel előtt és üzemelés során. Például negatív reaktivitás biztosítása, sugárzástűrő anyagok alkalmazása.
2. Feltételezik, hogy a gondos tervezés, konstrukció és üzemeltetés ellenére események és téves műveletek előfordulhatnak. Ezért a biztonsági rendszert úgy alakítják ki, hogy a személyzetet és a lakosságot óvják és ilyen események bekövetkezése során a sérüléseket minimalizálják. Például zóna vészhűtő rendszer (ECCS) alkalmazása primerköri hőhordozó vesztés (LOCA) esetén, vagy feszültségkiesés esetére tartalék dízel generátorok alkalmazása.
3. További biztonsági rendszereket alkalmaznak, hipotetikus üzemzavarok és balesetek hatásainak kezelésére, feltételezve, hogy egyes biztonsági védelmi rendszerek a baleset során meghibásodnak. Előre nem látható és nagyon kis valószínűséggel bekövetkező események hatását is figyelembe veszik. Például ECCS meghibásodik, akkor zónaolvadás lép fel, radioaktív anyag kerül a reaktor épületbe, a biztonsági tartálynak (konténmentnek) tömörnek kell lennie, a sprinkler (zuhanyzó) rendszer üzemelésével le kell csökkenteni a nyomást és a hőmérsékletet, el kell nyeletni az illékony radioaktív izotópokat (^{131}I), biztosítani kell a megfelelő légcserét és szűrést a köztes épületrészekben. A nagyon kis valószínűséggel előforduló üzemzavari baleseti eseményeket figyelembe kell venni, ha előfordulásuk valószínűsége nagyobb, mint 1 esemény 1000 év alatt. Újabban törekednek a 10^{-7}esemény/reaktor év valószínűségi korlát betartására. Ez a legpesszimistább biztonsági feltételezések alkalmazását igényli a biztonsági elemzések során a maximális következmények feltételezése mellett.

Az 1978-ban bekövetkezett USA-beli Three Mile Island-I (TMI) baleset után ezt a biztonsági elemzést kiegészítették az összes új passzív vagy inherens biztonság kialakításánál a meghibásodások biztonságának, a teljes körű ellenőrizhetőségnek, a megfutások biztonságának és az emberi elnézések biztonságának a figyelembe vételével. A meghibásodások biztonságánál biztosítani kell, hogy egy fontos komponens hibája esetén a rendszer biztonságos állapotba visszavihető legyen. A mindenre kiterjedő ellenőrizhetőség biztosítja a védelmet bármilyen veszélyes emberi beavatkozással szemben. A teljesítmény megfutások biztonsága lehetővé teszi, hogy a rendszer megfelelő ideig biztonságban marad egy baleset kezdete során, miután biztonságos állapotba térítették vissza. Az emberi elnézések biztonsága azt jelenti, hogy a reaktor elvisel egy késői vagy hibás emberi beavatkozást baleseti helyzetbe kerülés nélkül. A nukleáris balesetek csoportosítását mutatja az 1. táblázat.

típus	**példa**
reaktivitási balesetek	átmeneti tünet
hűtési elégtelenség	átmeneti tünet
baleset üzemanyag manipuláció során	csere, karbantartás
telephelyre vonatkozó balesetek	földrengések, cunami, repülőgép rázuhanás

1. táblázat Tipikus nukleáris baleseti csoportok (saját szerkesztés)

Fontos biztonsági szempont, hogy a reaktorok leállítás után még jelentős remanens hőtermeléssel (a teljes hőtermelés 7-10%-a) rendelkeznek, és további hűtést igényelnek.

Az alábbiakban röviden áttekintjük a múltban bekövetkezett négy legsúlyosabb, atomerőműben bekövetkezett balesetet és a levonható tanulságokat.

WINDSCALE (ANGLIA, 1957)

Az első windscale-i reaktorok grafitmoderálású, levegő hűtésű, plutóniumtermelő reaktorok voltak (4. ábra).

4.ábra A windscale-i reaktor [3]

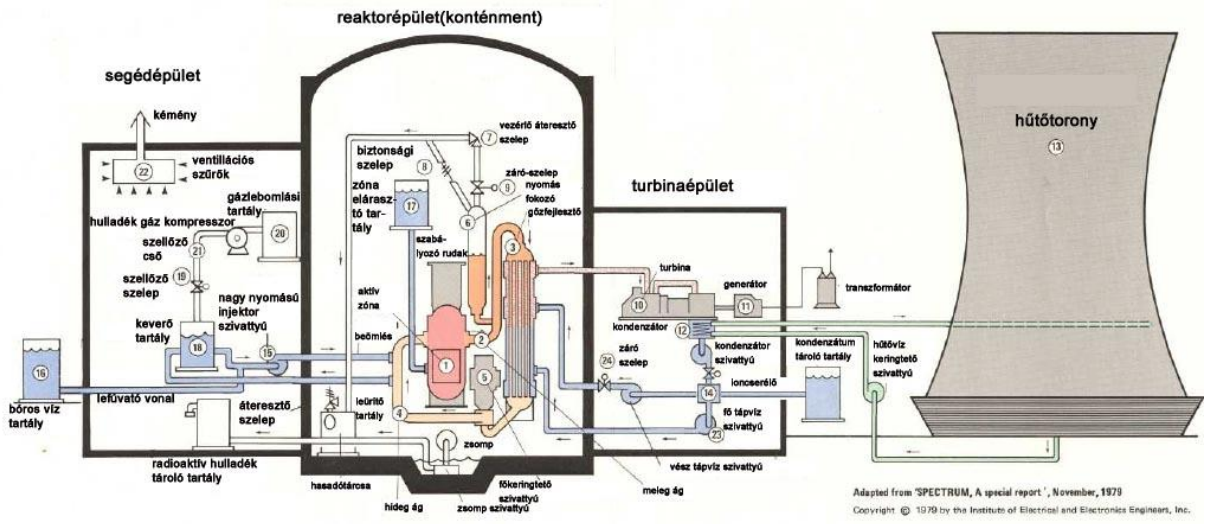
A 200-300 °C hőmérsékletű grafitmoderátorban az alábbi folyamat játszódik le üzem közben: a neutronok a lassulás során a grafitot alkotó szénatomok magjainak ütköznek. A rácshelyből elmozdított szénatom magasabb energiaszintre kerül, ily módon a grafit energiát tárol. Amennyiben azt az "energiával megszívódott" grafitot felmelegítjük, a hőmozgás következtében az atomok visszaugrálnak az eredeti, alacsonyabb energiájú helyeikre, az energiakülönbség pedig hő formájában jelenik meg, tovább melegítve a grafitot. Ez az öngerjesztő folyamat akár a grafit meggyulladásához is vezethet. A folyamatot felfedezőjéről Wigner-effektusnak, vagy wigneritisznek nevezzük. A wigneritisz lehetőségére Wigner Jenő már a hanfordi plutóniumtermelő reaktorok tervezésekor rámutatott és meg is találta annak ellenszerét: mielőtt még a grafit "túlszívná" magát, rendszeresen fel kell melegíteni, hogy a benne tárolt hő felszabaduljon. Ezzel a windscale-i erőműben is tisztában voltak, azonban 1957-ben túl későn és kellő körültekintés nélkül hajtották végre a felmelegítést. Fellépett a Wigner-effektus, október 10-én a reaktor túlforrósodott, végül a grafit meggyulladt. A reaktort elárasztották szén-dioxiddal, de ez nem bizonyult elégségesnek. Végül a vízzel történő oltás mellett döntöttek és október 12-én a tüzet eloltották. A 125 méter magas reaktorkéménybe épített szűrők a reaktorból felszabaduló radioaktivitás zömét visszatartották, így 16,5 PBq összaktivitás került ki a környezetbe, komoly környezeti kárt, illetve emberáldozatot az eset nem követelt. Más források szerint 260, ezen belül 13 halált okozó pajzsmirigyrákos eset kapcsolható a balesethez. Legnagyobb mennyiségben $7 \cdot 10^{14}$ Bq ^{131}I került az atmoszféra alsó rétegeibe, a környező területekre. A reaktor környezetében egy 500 km2-es területen a tejet emberi fogyasztásra alkalmatlannak minősítették és elkobozták, mivel benne a ^{131}I izotóp koncentrációja meghaladta a megengedett értéket. A reaktor személyzetének egy tagja 46 mSv dózist kapott, ami az éves természetes háttérsugárzás 20-szorosa. Egyébként a lakosság sugárterhelése - a hatósági intézkedések következtében - a megengedett érték alatt maradt.

THREE MILE ISLAND ATOMERŐMŰ BALESET (USA, 1978, INES 5)

1979. március 28-án az USA Pennsylvania államában levő Harrisburg várostól 16 km-re épült Three Mile Island atomerőmű 2-es blokkjában (TMI-2) súlyos üzemzavar történt, amely hosszú évekre az egész erőmű üzemkiesését okozta. Az erőmű 1-es blokkját csak a baleset

után 6,6 év múlva 1985-ben indították újra.

A baleset előtt mindössze egy évet üzemelő TMI-2 reaktorblokk vázlatrajzát az 5. ábrán mutatjuk be [4].



5. ábra A TMI-2 blokk vázlatrajza (a szerzők szerkesztése a [4] alapján)

A blokk legfontosabb adatai a következők. Könnyűvizes hűtésű és moderátorú Babcock and Wilcox gyártmányú nyomott vizes reaktor (PWR) bruttó termikus teljesítménye 2772 MW, bruttó elektromos teljesítménye 959 MW, nettó elektromos teljesítménye pedig 907 MW. A nettó hatásfok 32,8 %. Az aktív zóna 3,28x3,66 m méretű, a fűtőelem 2,29-2,90 % dúsítású 0,94x0,78 cm méretű UO_2 egy kötegben 208 rúd található, a teljes töltet 177 fűtőelem-kötegből 37000 fűtőelem-rúdból áll. A töltet tömege 83 t. A közepes fajlagos teljesítmény 31 kW/kg urán; 85,6 kW/dm^3 aktív zóna, a közepes kiégési szint 28800 MW nap/t, a moderátor hűtőközeg 306 °C-os átlagos hőmérsékletű víz. A fűtőelemek maximális hőmérséklete 2343 °C, a hűtőközeg tömegárama 55630 t/h, a víz belépő hőmérséklete 290 °C, kilépő hőmérséklete pedig 318 °C.

A nyomás-szabályozó a primerkör legforróbb része. Tranziens állapotban onnan a motoros biztonsági szelepen, túlnyomás esetén gőz fúvatható le. A lefúvató szelephez kapcsolódó csővezeték a reaktor alatti gyűjtőtartályba vezet. Ebben a tartályban hűtőbordák segítségével hűthető a belépő forró folyadék, vagy gőz. Ha a tartályban túlnyomás alakul ki, egy szelep vezeti ki a folyadékot a reaktor épület lefolyó rendszerébe. A turbógenerátor (1db) 926,5 MW teljesítményű turbinából áll, a belépő gőz hőmérséklete 293 °C, nyomása 62 bar. A rendszer része még 1db 60 Hz-es háromfázisú szinkron-generátor. A kondenzátor 105 400 m^3/h térfogatáramú 13,3 °C -os vízzel üzemel. A teljes primerkör egy 65 m magas, acél bélésbevonattal megerősített 5,29 bar nyomásra tervezett betonköpenyben volt, ez az ún. konténment, amely végül is meggátolta, hogy radioaktív szennyeződés kerüljön ki a környezetbe.

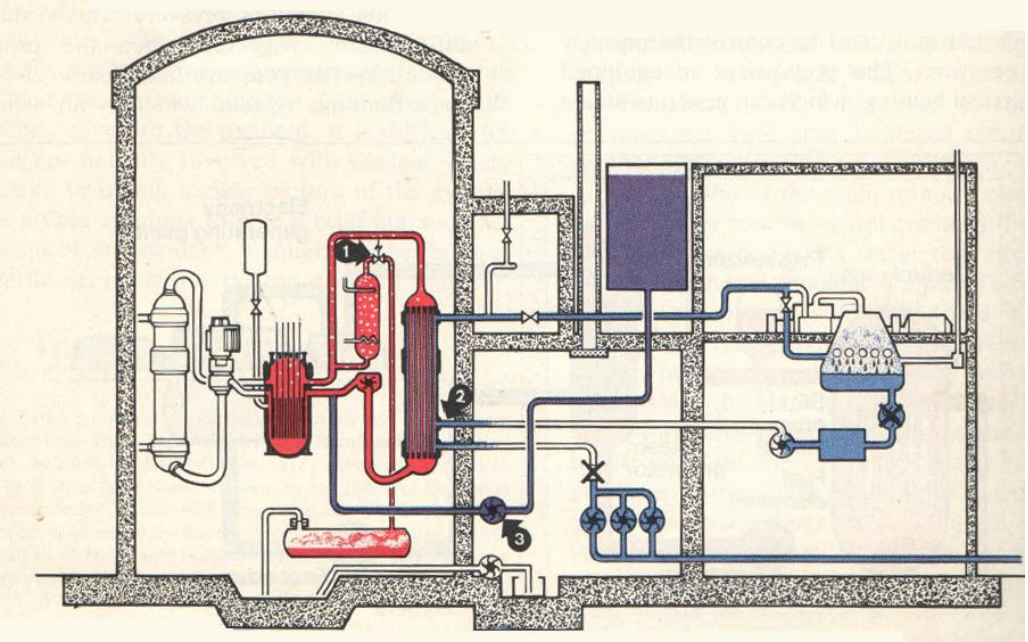
A PWR[1] rendelkezett zóna vészhűtő rendszerrel (nagynyomású injektáló, középnyomású akkumulátor és kisnyomású injektáló). LOCA esetén a konténment tetejéről híg nátrium-hidroxid fecskendeztethető be a jód-gőzök visszatartására és hűtésre. Az üzemzavar menete a

[1] Pressurized Water Reactor

következő volt:

A baleset időrendje [4]:

Turbina kiesés (0-6 perc, 6. ábra)



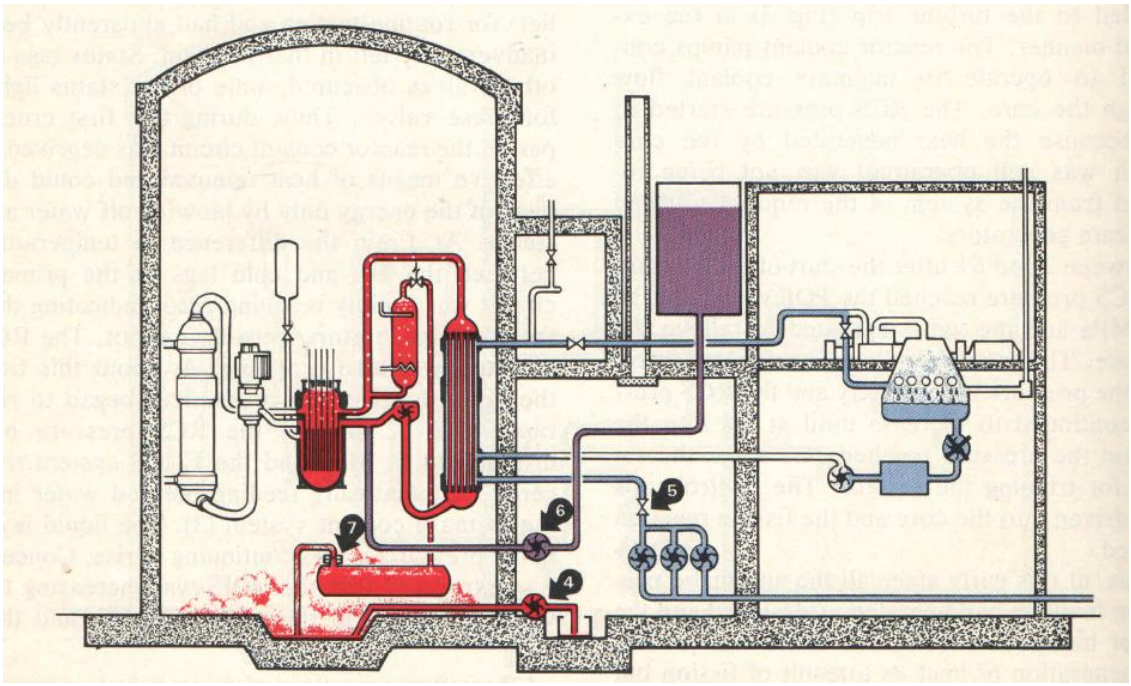
6. ábra 0-6min közötti események (a szerzők szerkesztése a [4] alapján)

Az erőmű teljes 98 %-os üzeme mellett a vészhelyzetben szükséges segéd-tápvízrendszer mindkét tolózára a karbantartás után *zárva maradt.* Az erőmű tápvízrendszere már korábban meghibásodott és 1978-79-ben többször is az 1. blokk leállását eredményezte. 1979. március 28-án hajnali 4 órakor a 2. blokk tápvízszivattyúi leálltak**.** Azonnal beindultak a segéd-tápvízrendszer szivattyúi (3 db), de a lezárt tolózárak (az ábrán x-el jelölve) miatt nem jutott víz a hőcserélőbe. Mivel a primerköri víz nem hűlt le a hőcserélőben nőni kezdett a pimerköri víznyomás. A hiba után 3-6 másodperc között a primerköri nyomás elérte a 155 bar értéket és a gőzfejlesztő lefúvató szelepe (1) kinyitott. A primerköri nyomás a pufferhatás miatt még egy kicsit tovább nőtt 162 bar-ra, ezért az automatika állította a reaktort. *Eddig a biztonsági rendszer helyesen működött!* Ugyanakkor a reaktor töltetben jelentős hőmennyiség halmozódott fel a hasadványok bomlási hője révén (1 perc-109 MW_t, 1 óra-46 MW_t, 1 nap-19 MW_t, 1hét-9 MW_t, 1 hónap-5,4 MW_t). 13 másodperc után a primerköri nyomás visszaesett 152 bar értékre és a lefúvató szelepnek be kellett volna záródnia, de az sajnos nyitott állapotban fennakadt. (Sajnos ez a hiba már korábban 1977-ben egy ugyancsak Babcox-Wilcox gyártmányú atomerőműben a Besse-Davis atomerőműben is bekövetkezett, de ott a lefúvató szelep fönnakadását időben észlelték és a szelepet lezárták komoly elfolyás nélkül. De sajnos nem vonták le a biztonsági következtetéseket és nem keresték meg a fennakadás okát és nem küszöbölték ki azt!) A fennakadt szelepen folyamatosan folyott el a primerköri hűtővíz. Hiába mentek a segéd tápvízrendszer szivattyúi, a lezárt szelepek miatt a pótvíz nem jutott el a hőcserélőbe, melynek szekunder köri vízszintje vészesen csökkent. 1perc után a hőcserélő kiszáradt és megszűnt a primerköri víz hűtése, a nyomásfokozóban szintén csökkent a víz szintje.

2 perc 4 másodperc után a primerköri nyomás 110 bar alá esett és beindult a zóna vészhűtő rendszer nagynyomású befecskendezője és bóros vizet juttatott a reaktor tartályba. Ezért növekedni kezdett a nyomásfokozó vízszintje és folyadékkel telt fel. Ugyanakkor a primerkör egyes részein gőzdugók alakultak ki, tehát nem volt folyamatosan tele vízzel. 4 perc 38

másodperc után a nagynyomású befecskendező egyik szivattyúja kikapcsolt, a másik lefojtva tovább üzemelt.

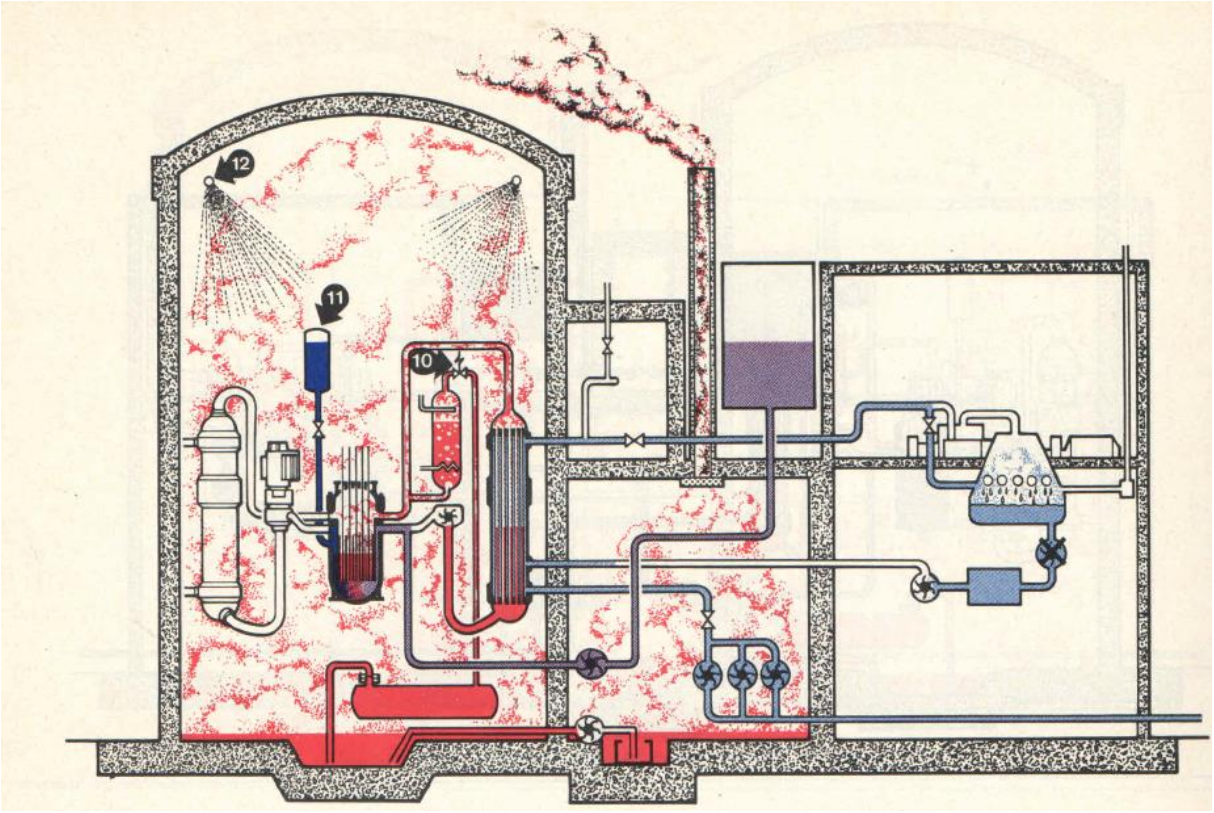
Veszteség a primerköri hűtőközegben (6-20 perc, 7. ábra)[4]



7. ábra 6-20 percek közötti események (a szerzők szerkesztése a [4] alapján)

A 6. percben eltűnt a nyomásfokozó gőzpárnája. Az elfolyt hűtőközeg gyűjtőtartályában gyorsan nőtt a nyomás és 7 perc 43 másodperc után a szivattyú beindult és a tartályból elvezette a vizet a segédépület tartályaiba. A 8. percben az operátorok észrevették, hogy a gőzfejlesztő kiszáradt és a segéd tápvízszivattyúk a lezárt szelepek miatt nem tudják pótolni a vízveszteséget. Kinyitották a lezárt szelepeket (6) és víz kezdett folyni a gőzfejlesztő szekunder oldalára. A hűtés beindulás kalapácsütés szerű zajjal járt. Az üzemzavar után 10 perc 24 másodperccel leállt a második nagynyomású befecskendező szivattyú is. Ennek eredményeként a fönnakadt szelepen több primerköri hűtővíz folyott el, mint amennyi a zóna vészhűtő rendszerből befolyt. A 11. percben a nyomásfokozó szintjelzője újra két fázist jelzett és a folyadék szint gyorsan csökkent. A 15. percben elhasadt a primerköri biztonsági tárcsa (7) és a kiáramló gőz miatt nőni kezdett a nyomás a konténmentben. Ezután a kiáramló primerköri hűtővíz és gőz az elhasadt tárcsán keresztül a konténmentbe jutott, ahonnan az összefolyt vizet a segédépületbe pumpálták. A 18. percben ugrásszerűen megnőtt a szellőzőrendszerben mért radioaktív gázok mennyisége, de ez még nem fűtőelem-sérülésből, hanem a primerköri vízből származott. A primerköri nyomás csak 83 bar volt és csökkent. Eddig a pontig az események nagyon hasonlóak voltak az ugyancsak Babcock-Wilcox gyártmányú Davis-Besse atomerőműben 1977 szeptemberében lejátszódott üzemzavarhoz, de ott ezután észrevéve a nyitott lefúvató szelepet, azt lezárták és nem történt zónaolvadás.

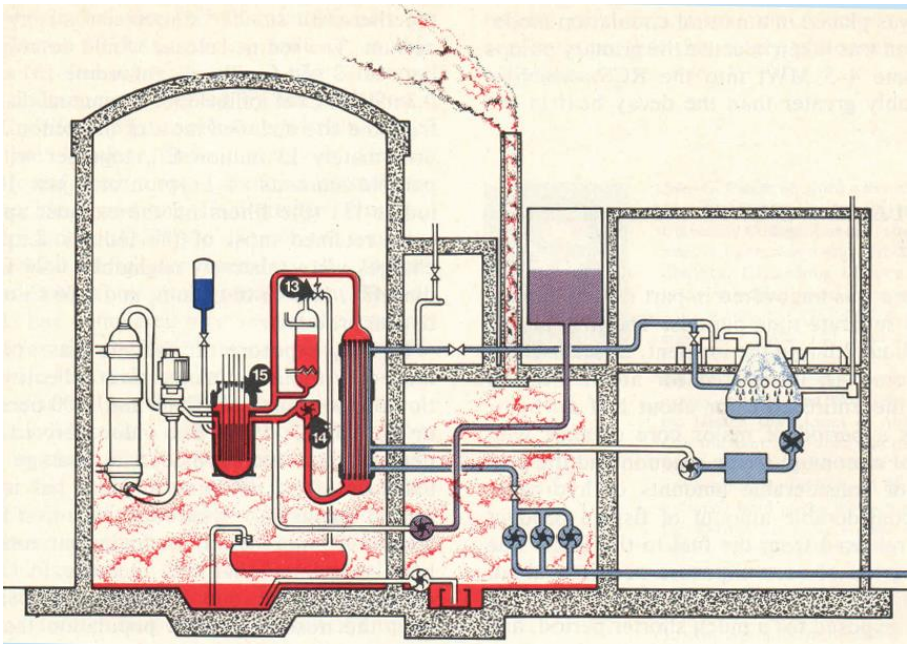
Kiterjedt nyomáscsökkenés (6-11 óra, 8. ábra)[4]



8. ábra 6-11 óra közötti események (a szerzők szerkesztése a [4] alapján)

Az operátorok csökkentették a primerköri nyomást, hogy beinduljon az alacsony-nyomású zóna injektáló rendszer. Ezért 7 óra 38 perckor kinyitották a lefúvató szelepet (10) és 8 óra 41 perckor a nyomás 41 barra csökkent és beindult a zóna elárasztás (11). Sajnos azonban csak kevés vizet sajtolt a reaktorba, mert hibásan vízzel telített zónát észlelt. A nyomáscsökkentés közben a magas hőmérsékleten keletkezett jelentős mennyiségű hidrogén jutott a reaktor épületbe. 9 óra 50 perckor a reaktor épület nyomása 1,93 barra nőtt. Bekapcsoltak a vészhűtő-elnyelető zuhanyok (12) és 6 percig üzemeltek. Több durranógáz robbanás következett be a konténment felső részében, a dómban és a gőzfejlesztőben. A nyomást nem sikerült 30 bar alá csökkenteni. Így a 28 baron beinduló bomláshő elvezető rendszert sem sikerült aktiválni. 11 óra 8 perckor ezért elzárták a lefúvató szelepet. A kiszabadult nagymennyiségű radioaktív jód miatt a jódszűrők áteresztettek és az 5 mérföldön belül lakó terhes nők és 6 éven aluli gyerekek számára kiürítést tanácsoltak. A környező népességet ért sugárdózis sohasem haladta meg a megengedett szintet. A nyomáscsillapító tartályban és a konténmentben a 3. és 10. óra között bekövetkezett hidrogén-robbanások után a primerkör leürítését korlátozták. A gőz, a hasadási gázok és a hidrogén a zárt primerköri rendszer egyes részeiben felhalmozódott, veszélyeztetve ezzel az aktív zóna vízszintjét és a primerköri cirkulációt és további hidrogénrobbanással fenyegetett.

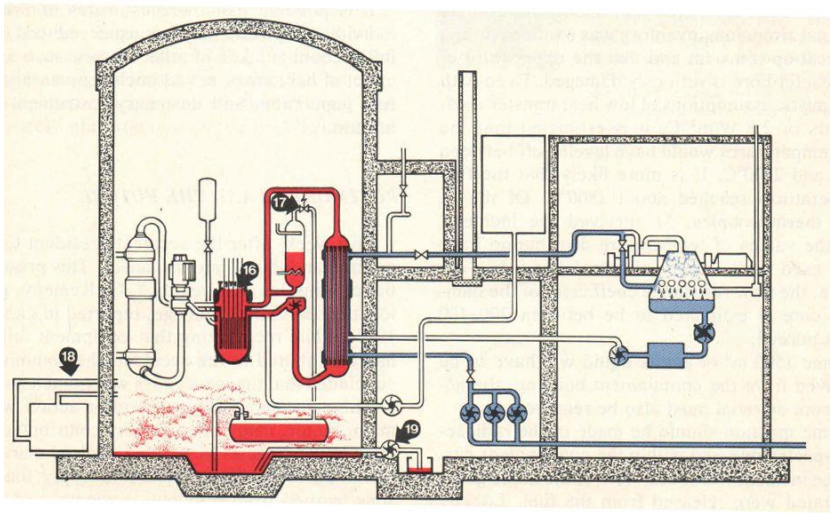
Nyomáscsökkentés és a stabil hűtés helyreállítása (13-16. óra, 9. ábra)[4]



9. ábra 13-16 óra közötti események (a szerzők szerkesztése a [4] alapján)

13 óra 30 perckor ismét lezárták a lefúvató szelepet (13) és beindították a nagynyomású befecskendezést, majd a nyomás helyreállása után 15 óra 51 perckor az „A" (14-es jellel az ábrán) primerköri szivattyút beindították így a kilépő víz 293 °C-os, a belépő pedig 205 °C-ra hűlt.

A hidrogén-buborék eltávolítása (1-8 nap,10. ábra) [4]



10. ábra Az 1-8 nap közötti események (a szerzők szerkesztése a [4] alapján)

A 60. órában egy szakmai krízis-irányító csoportot hoztak létre, amely a következő intézkedéseket hozta:

- a primerköri nyomást 68,9 bar-ra csökkentették,
- bekapcsolták a fő hűtővíz szivattyúkat,

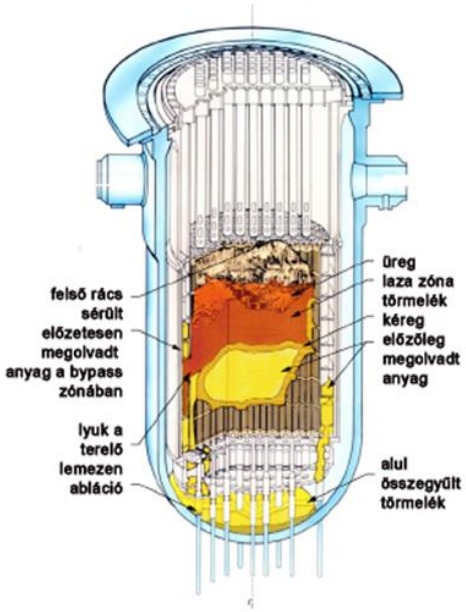
- további hűtésként egy gőzfejlesztő-turbina egységet bekapcsoltak,
- növelték a nagynyomású befecskendezést,
- a konténmentben rekombináló reakciókkal csökkentették a hidrogén koncentrációt,
- a primerkörben levő gázbuborékokat a túlhevítő mentesítő szelepén keresztül és egyéb úton a hidegebb primervízben elnyelették.

A reaktor tartályban kb. 28 m^3 gázsapka alakult ki, melynek zöme hidrogén (16) volt. Ezt fokozatosan a lefúvató szelepen keresztül kiengedték és a 18-as rekombinátorokban eloxidálták. A segéd-épületből a kifolyt vizet visszapumpálták a reaktor épületbe (19). 1 hónap után a bomlási hő annyira lecsökkent, hogy a primerköri keringtető szivattyúkat kikapcsolták és csak természetes áramlás maradt. (Ekkor már a szivattyúk által bevitt meleg is zavart)**.**

A gázbuborékok sikeres csökkentése után a további intézkedések az alábbiak voltak:

- a hulladékvíz-rendszer befogadóképességének biztosítása, a benne levő alacsony aktivitású víz folyóba történő óvatos kiengedésével,
- a hulladékgáz-rendszer befogadóképességének biztosítása (bomlás, kis ürítések a konténmentbe, óvatos kieresztés a kéményen keresztül),
- a telített jód szűrők cseréje,
- a konténment hidrogén-tartalmának további csökkentése rekombinációval,
- üzembe helyezték a normál előkészítő és víztisztító rendszert, hogy megelőzzék további gázbuborékok képződését az alacsony primerköri nyomás miatt,
- magasabb vízszintet biztosítottak a gőzfejlesztőben a biztonságosabb hűtés érdekében.

Ezen intézkedés-sorozattal sikerült a durranógáz robbanás veszélyét elkerülni és a zóna további sérülését megakadályozni. A zónaolvadás sematikus képét mutatja a 11. ábra.



11. ábra A TMI-2 blokk zónaolvadása (a szerzők szerkesztése a [5] alapján)

Az üzemzavar következményei

A baleset következtében az aktív zóna felső középső részében a hőmérséklet elérte 3100 K hőfokot, itt a fűtőelemek és szerkezeti anyagok megolvadtak, csak a külső részen találtak

néhány ép fűtőelem-köteget. Ennek következtében az aktív zónába nagymennyiségű törmelék került (átmérő: 4-10000 μm között) melynek zöme kerámia, megdermedt fémolvadék illetve kőzet jellegű anyag. A reaktor irányítását szolgáló mintegy 50 kg tömegű 3,8 m magas rozsdamentes acélszerkezet a magas hőmérséklet miatt erősen deformálódott, több ponton összeolvadt az eredetileg 1,2 m távolságra levő fűtőelemtartó ráccsal. A fűtőelem-burkolatok sérülése következtében a hasadási nemesgázok kb. 35 %-a szabadult ki. A fűtőelemek tokozatát alkotó Zr-Nb ötvözet kb. 40 %-a reakcióba lépett a hűtővízzel és hidrogént fejlesztett. Az aktív zóna mintegy 35%-a törmelékké vált a felső középső részben. A sokszoros szigetelésnek köszönhetően a hőérzékelő termoelemek az aktív zónában is sértetlenek maradtak. Majdnem a teljes fűtőelem-törmelék a zóna felső részében rekedt, mivel a felfüggesztő rácsozat szitaként visszatartotta, így nem került ki a primerkörbe.

A legnagyobb veszélyt a gyúlékony robbanó gázok képződése okozta. A hidrogénfejlődés következtében a maximális nyomás a konténmentben megközelítette a 3 bar értéket! A hidrogén és egyéb gyúlékony gázok az alábbi reakciókban keletkezhettek a víz közvetlen termikus bontása során:

$$2\ H_2O \rightarrow 2\ H_2 + O_2 \qquad (1)$$

2000 K hőmérsékleten a vízmolekulák kb. 1 %-a bomlik így. A víz radiolízise során hidrogén atomok, hidroxil gyökök képződésén keresztül hidrogén és oxigén gáz keletkezhet. A cirkónium-víz reakció során, az alábbi folyamat szerint keletkezhetett hidrogén

$$Zr + 2\ H2O \rightarrow ZrO2 + 2\ H2 \qquad (2)$$

ez a reakció 1580 °C fölött felgyorsul.

Az aktív zóna olvadéka és a beton közti reakciókban a beton bomlásakor felszabaduló CO_2 és vízgőz a forró olvadékon átáramolva, ennek fémes komponenseit oxidálja:

$$\begin{aligned} Zr + 2\ H2O &\rightarrow ZrO2 + 2\ H2 \\ 2\ Cr + 3\ H2O &\rightarrow Cr2O3 + 3\ H2 \\ 2\ Cr + 3\ CO2 &\rightarrow Cr2O3 + 3\ CO \\ Fe + H2O &\rightarrow FeO + H2 \\ Fe + CO2 &\rightarrow FeO + CO \end{aligned} \qquad (3)$$

A cirkónium és a króm oxidálása teljesen végbemegy, a vas oxidálása egyensúlyra vezet a hőmérséklet függvényében. Először a cirkónium, majd a króm, végül a vas oxidálása megy végbe. A gázfejlődés szempontjából tehát a cirkónium-víz kölcsönhatás volt meghatározó. Ebből a reakcióból mintegy 500 kg hidrogén keletkezhetett és számítások szerint a konténmentben maximálisan 7,9 % hidrogén és 3,7 % vízgőz lehetett.

A baleset környezeti hatásai

A rendelkezésre álló adatok szerint a baleset következtében a környező lakosságra gyakorolt radioaktív sugárhatás elhanyagolható volt. Az 1979-84 években az erőműből évente felszabaduló gáznemű radioaktív anyagok mennyiségét az alábbi 2. táblázat mutatja be:

	1979	1980	1981	1982	1983	1984
Teljes kikerült illékony, izotóp-mennyiség (a trícium kivételével)	$1\ 10^{17}$ Bq	$1{,}63\ 10^{13}$ Bq	$1{,}75\ 10^{12}$ Bq	$3{,}37\ 10^{13}$ Bq	$6{,}4\ 10^{12}$ Bq	$7{,}66\ 10^{12}$ Bq
I-131	$5{,}22\ 10^{11}$ Bq	$6{,}14\ 10^{5}$ Bq	n.a.	n.a.	n.a.	n.a.
H-3	$5{,}43\ 10^{12}$ Bq	$3{,}5\ 10^{13}$ Bq	$2{,}42\ 10^{12}$ Bq	$4{,}14\ 10^{12}$ Bq	$1{,}84\ 10^{12}$ Bq	$5{,}18\ 10^{11}$ Bq

2. táblázat A TMI-2 blokk balesete során környezetbe került radioaktív anyagok (saját szerkesztés)

KÖVETKEZTETÉSEK

A baleset nem következett volna be, ha konstrukciós hiba miatt a lefúvató szelep nem lett volna hajlamos fennakadásra és így lehetőség biztosítására nagy mennyiségű primerköri hűtővíz elfolyására. Ha korábbi Davis-Besse erőműben történtek tanulságait is figyelembe vették volna ugyancsak elkerülhető lett volna a baleset.

A baleset megelőzhető lett volna, ha az operátorok megbízható adatokat kapnak a reaktorban lévő víz mennyiségéről és ennek alapján helyesen értékelik a kialakult helyzetet.

ÖSSZEGZÉS

A Windscale-i és a Three Mile Island-i atomerőművi balesetek során a maradékhő nem megfelelő elvezetése részleges zónaolvadáshoz és illékony radioaktív izotópok kibocsátásoz vezetett. Az USA baleset során különböző kémiai reakciók során keletkezett hidrogén gázrobbanások következtek be. Sajnos ez utóbbi veszélyforrás megjelenését nem vették figyelembe a későbbiek során és az ezután bekövetkezett atomerőművi balesetekben komoly rombolást okoztak a gázrobbanások. Az események következményeiben komoly szerepet játszott az operátorok helytelen reakciója és beavatkozása, valamint az aktív zóna hűtési állapotának ismeretéhez szükséges mérési adatok hiánya, vagy nem megfelelő formában való rendelkezésre állása. A környezetbe került illékony radioaktív izotópok környezetszennyezése döntően időleges volt, emberéletet nem követelt ez a két baleset és tudomásunk szerint bizonyítható egészségkárosodás sem történt. Az USA baleset után javították az operátorok képzési szintjét és a mérőműszerek jobb áttekinthetőségét.

FELHASZNÁLT IRODALOM

[1] HIRSCHBERG, S., BURGHERR, P.: Methods and results of assessing energy-related severe accident risks, PSI, 26. Mai 2013., OECD-NEA Workshop on „Approaches to Estimation of the Costs of a Nuclear Accident”, Paris, France, 28-29 May 2013, Burgherr, P., Hirschberg, S., Hunt, A. and Ortiz, R. A. (2004). External costs from major accidents in non-nuclear fuel chains. Work Package 5 Report to the European Commission, DG Research, Technological Development and Demonstration (RTD), "New Elements for the Assessment of External Costs from Energy Technologies" (NewExt), Vol. Paul Scherrer Institute, Villigen, Switzerland

https://www.oecd-nea.org/ndd/workshops/aecna/presentations/documents/StefanHirschberg-Assessingenergy-relatedsevereaccidentrisks.pdf, letöltés ideje: 2016. 11. 05.

[2] D'HAESELEER, W.: Is Nuclear Power a Sustainable Option after Fukushima?, BNEN 2012-2013 Intro William D'haeseleer, https://set.kuleuven.be/ethiekweek/fukushima2012/dhaeseleer.pdf, letöltés ideje: 2016. 11. 05.

[3] http://avilagtitkai.com/articles/view/5-nuklearis-katasztrofa-melyet-eltitkoltak-a-vilag-elol, letöltés 2017. 01. 10.

[4] COLLIER, J.G., DAVIES,L.M.: The Accident at Three Mile Island, Heat Transfer Engineering, Volume 1, Number 3, Jan-Mar. 1980

[5] REMPE, J., FARMER M., ET AL., Revisiting Insights from Three Mile Island Unit 2 Postaccident Examinations and Evaluations in View of the Fukushima Daiichi Accident, NUCLEAR SCIENCE AND ENGINEERING: 172, 223–248 ~2012!

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017.március

A FELSZÍN ALATTI VIZEK SZENNYEZÉSEINEK ELTÁVOLÍTÁSA, A VÍZMINŐSÉGI KÁRELHÁRÍTÁS MÓDSZEREI 1.RÉSZ

REMOVAL OF GROUNDWATER CONTAMINATION, METHODS OF WATER QUALITY DAMAGE RELIEF PART 1.

HEGEDŰS Hajnalka

(ORCID: 0000-0002-5207-0356)

hegedus.hajnalka@uni-nke.hu

Absztrakt

A modern életmód, a globális felmelegedés és az éghajlatváltozás mind szerepet játszanak a vízgazdálkodás alakulásában. A negatív tendenciák kedvezőtlen hatással vannak a vizeink mennyiségére és minőségére egyaránt. A vízminőség védelme magába foglal mind olyan műszaki, gazdasági és jogi beavatkozást, amelyeket a megfelelő vízminőség érdekében alkalmaznak. Ide sorolandóak azok a beavatkozások, amelyek a vízminőség megtartását, a szennyezések elleni védekezést, valamint a vízminőségi kárelhárítást célozzák.
Ez a kétrészes cikk igyekszik bemutatni azokat a kárelhárítási műszaki módszereket, amelyekkel a már bekövetkezett károk sikeresen elháríthatóak vagy csökkenthetőek a felszín alatti vizek minőségének és fenntarthatóságának érdekében. Az első cikk a szennyezések módjára és fajtáira, valamint a fizikai és kémiai eltávolítási módszerekre koncentrál. A második a kárelhárítás biológiai módszereit helyezi előtérbe, amelyek remélhetőleg mind nagyobb teret kapnak a fenntarthatóság érdekében is.
"A mű a KÖFOP 2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Kulcsszavak: *vízminőség, kárelhárítás, biológiai módszerek*

Abstract

The modern way of life, global warming and climate change all play a role in the development of water management. The negative trends have unfavorable impact on the quantity and quality of our waters as well. Protection of water quality includes all the technical as well as economic and legal interventions that are applied to ensure good water quality. This comprises those interventions that are aimed at maintaining water quality, protection against pollution as well as water damage control.
This two-parted paper attempts to demonstrate the technical methods of damage control, which can successfully eliminate or reduce damages to ensure groundwater quality and sustainability. The first part of the paper focuses on the ways and types of pollution as well as the physical and chemical decontamination methods. The second part turns to the biological methods, which hopefully will gain a more and more prominent role for the sake of sustainability.

Keywords: *water quality, water damage control, biological methods*

A kézirat benyújtásának dátuma (Date of the submission):(2017.02.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.18.

BEVEZETÉS

A víz nélkülözhetetlen az élet számára, teljes mértékben meghatározza az élővilág képét. Élettér, részt vesz az élőlények szervezeti felépítésében, reakcióközeg, ugyanakkor reakciók kiindulási anyaga és végterméke is, diszpergáló és szállító közeg, magas fajhője miatt pedig részt vesz az egyedi, lokális és globális hőszabályozásban is.

Földünk felületének kétharmadát víz fedi, mégis majd´ egy milliárd ember nem jut napi szinten tiszta ivóvízhez. Sokszor az akut vízhiányos területeken az is nehezíti a helyzetet, hogy a meglévő víz jelentős részét mezőgazdasági termelésre fordítják. A nyílt vizekbe kerülő műtrágya, a magas nitrát-tartalmú szennyvizek hatására kórosan elalgásodnak a vizek, melyek következményeként eutrofizáció1, az élőlények és élőhelyek pusztulása, valamint az emberek megbetegedése, fertőzések elterjedése lép fel. Ezért sem meglepő, hogy az egészséges ivóvíz kérdése egyre nagyobb problémát jelent. A vízigényünk a népesség növekedésével, a klimatikus viszonyok változásával folyamatosan és rohamosan nő, ezáltal az elérhető vízkészlet mennyisége globális szinten igen csekély. Komoly zavarok mutatkoznak az emberiség vízellátásában. Elmondható, hogy a víz mára elsőszámú ásványkinccsé lépett elő. Ennek ellenére az emberi faj mégis számos módon veszélyezteti azt. A környezet és a víz szennyezésének hatására vizeinkben a kimerülés jelei mutatkoznak.

A globális felmelegedés és éghajlatváltozás komoly szerepet játszik a vízgazdálkodás alakulásában. Ahogy melegebbé s szárazabbá válik az éghajlat, az állóvizek jobban párolognak, csökken a folyók lefolyása, megváltozik felszíni vizeink vízháztartása, lelassul vízforgalmuk, tehát a víz lassabban cserélődik, felgyorsul az eutrofizáció, amely kedvezőtlenül befolyásolja a vizek oxigéntartalmát és minőségromlás, fertőzésveszély lép fel. A növekvő párolgás a felszín alatti vízkészlet drasztikus csökkenését is okozhatja. A mennyiségi problémák minőségieket is magukkal hoznak. Az időjárási szélsőségek és az emberi beavatkozások hatására egyre több szennyezés kerül vízbázisainkba, komplex okok miatt viszont csökken azok öntisztulási képessége is. A vízminőség védelme magában foglalja az összes olyan műszaki, gazdasági és jogi szabályozást, amelyet egy adott vízminőségi célkitűzés érdekében alkalmaznak. A víz minőségének védelme alá sorolandó minden olyan beavatkozás, amellyel megelőzhető a vízszennyező anyag vízbe kerülése, valamint a vízszennyező hatásokat utólag kiküszöböljük. Ehhez hozzátartozik a vizek állapotának rendszeres vizsgálata, értékelése és minősítése, a vízminőség megtartására szolgáló műszaki beavatkozások végrehajtása, a rendkívüli vízszennyezések elleni védekezés, illetve a vízminőségi kárelhárítás. Már a ´70-es évek óta születnek egyezmények, amelyek a vizek védelmét szolgálják. Ezek azonban keveset érnek, sikertelenek, ha az érintett politikai és gazdasági szereplők elsődlegesen csak a saját érdekeiket tartják szem előtt, melyek minden tekintetben rövidtávúak, illetve sok ország nem is hajlandó csatlakozni hozzájuk. Az éghajlatváltozás enyhítheti, vagy éppen súlyosbíthatja az emberi tényezőkre visszavezethető problémákat, amivel szintén számolni kell, hiszen a dominó elv alapján másodlagos kockázati tényezők jelentkezhetnek. [1]

A víz a jellemző tulajdonságai alapján az élővilág, a társadalom számára nélkülözhetetlen vegyület, amely nélkül lehetetlen lenne a földi élet. A víz többek között az élőlények építőanyaga, testünk és szerveink nagyrészt vízből állnak, ahogy a táplálékaink jelentős százaléka is víz. Az ember esetében ez a részarány majdnem 70 %. Emellett a víz a bioszféra egyik leglényegesebb hőmérséklet szabályozója, a sejtekben lejátszódó biokémiai folyamatok

[1] A vizekben a tápanyag-feldúsulás miatt elszaporodnak az elsődleges termelő szervezetek, a vízben túlszaporodnak a vízinövények.

oldószere. A víz oldószerként is jelentős, nem alakulhatott volna ki nélküle az élet, halmazállapotának megvan a maga jelentősége mind az élővilág, mind az emberek számára. Szilárd állapotában, a jég hozzájárul például a kőzetek változásához, a sziklák aprózódásához, és ezáltal a talaj formálódásához, a talajképződéshez. Ugyanakkor a tavakon képződő jégréteg védi például a mélységi víztömegeket – így az élővilágot is – a fagyástól. Folyékony halmazállapotában igen fontos és sokoldalú szerepet játszik a termelésben is. Az iparban technológiai vízként, hűtővízként szolgál, valamint szociális célból történő felhasználása is jelentős, de a közlekedésben sem elhanyagolható a szerepe, mind a gépek hűtőközegeként, mind pedig közlekedési közegként. A mezőgazdaságban öntözésre, állatok itatására használják mindenekelőtt, de a haltenyésztés esetében a víz a termelőközeg. A forrás utáni gázhalmazállapotot hasznosítják a gőzzel működő gépekben, turbinákban.

Magyarország fekvése, földtani felépítése és medencejellege következtében igen gazdag vizekben. Mindenekelőtt felszín alatti vizeink mennyisége, környezeti és használati értéke kiemelkedő jelentőségű európai viszonylatban is. Hazánk területének nagy részét vastag, medencebeli üledékek fedik, a hegyvidéki területeken pedig a felszín alatt gyakran karsztos képződmények találhatóak. Ezek kiváló felszín alóli vízbeszerzési lehetőséget biztosítanak. Magyarország ivóvízellátásának megközelítőleg 95 %-a felszín alatti vízből történik, de ugyanilyen fontos szerepet töltenek be ezek a vízkészletek a mezőgazdaságban is. Magyarország medencejellege azonban nehézségeket is okoz. Folyóink legtöbbje nem hazánk területén ered, és jelentős mennyiségű szennyeződést hozva érkezik a környező országokból. Mivel a folyók sebessége a hirtelen ellaposodó területeken lecsökken, a szennyeződések nagy része itt rakódik, ülepedik le. A szennyezések mellett meg kell említeni a környező hegyvidékek hóolvadásából származó megnövekedett vízhozamot is, amelyek által az árvíz-, és közvetetten a belvízveszély is növekszik, számottevő károkat okozva a gazdaságban, a lakosság vagyonában, természeti értékeinkben. [2]

A VÍZ JELLEMZŐI

A víz jellemzésekor elkülönítjük egymástól a kémiai értelemben vett tiszta vizet és a természetben is megtalálható vizeket. A kémiai értelemben vett tiszta víz a természetben nem fordul elő. A több ezer méteres magasságban kiváló csapadékvíz ugyan megközelíti annak minőségét, de mire a földfelszínre ér, átveszi a légkörből kimosott gázokat és port, illetve a talajjal érintkezve azonnal sókat old ki onnan. A kémiai tekintetben vett tiszta víz az emberi lét számára nem is ideális, hiszen a szervezet anyagcsere folyamatai a bonyolult ionháztartások egyensúlyára épülnek. A szabadban megtalálható víztestek nem íztelenek és szagtalanok, hanem a természetes ásványi anyagok beoldódásától, a mikroorganizmusok anyagcseretermékeiből, szerves anyagok bomlástermékeiből, illetve a települési szennyvizekből és azok bomlástermékeiből, valamint ipari szennyvizekből és azok bomlástermékeiből származó anyagok miatt lehet különféle ízük és/vagy szaguk.

A víz tulajdonságait jellemzően három csoportra oszthatjuk: fizikai, kémiai és biológiai jellemzők. Ezen jellemzők jelen cikkben nem kerülnek bemutatásra.

A VÍZKÉSZLETEK VESZÉLYEZTETÉSE

A vízkészleteket veszélyeztető tényezőket, a vízszennyezést sokféleképpen definiálhatjuk. Értjük alatta:

- az összes olyan emberi tevékenység hatására kialakuló körülményt, amelyek közvetlenül befolyásolják a felszíni, illetve a felszín alatti vizek minőségét;
- azon folyamatot, amely során a víz fizikai, kémiai, biológiai és bakteriológiai tulajdonságai károsan megváltoznak, a víz részben, vagy teljesen alkalmatlanná

válik emberi használatra, illetve a természetes vízi életfolyamatokra is veszélyesen hat;
- valamint ha az egyes (veszélyes) anyagok mértéke meghaladja a természetes vizeken belüli koncentrációt.

A szennyeződés forrását tekintve azok lehetnek pontszerű szennyezések, nem pontszerű (diffúz) szennyezések, vagy vonalforrású szennyezések is.

A szennyeződés kiterjedésétől és továbbterjedésének mértékétől függően beszélhetünk lokális (helyi), vízgyűjtőre kiterjedő (fluviális), regionális és kontinentálisan fellépő, de akár globális szennyeződésekről.[3]

VÍZSZENNYEZÉSEK OKAI

Hazánk medencejellege miatt Európa egyik leginkább *árvíz*veszélyes területe. Magyarország felszíni vizeinek csak 5%-a ered az ország területén, a többi a határokon kívülről érkezik. Több mint 21 ezer km^2 a mélyen fekvő, lefolyástalan terület, amelyet árvíz esetén elöntés fenyeget. A már felépített töltések, amelyeket kifejezetten az árvíz elleni védekezés miatt építettek, főleg a mentett oldalon elzárják az ott található holt- vagy mellékágakat, ahova a túlzott mennyiségű víz elfolyhatna. A szabályozott folyómedrek, a kiépített partvonalak miatt sokszor hiányzik a parti növényzet. Másrészről elmarad a földterületek elárasztásának lehetősége is. Ezek együttesen kedvezőtlen hatással vannak a vizek ökológiai állapotára árvíz bekövetkeztekor. [4]

A *belvíz* közvetlen és közvetett károkat okoz. A felszín vízzel való elborítása mellett a vízgyűjtő területek tervezettnél nagyobb hidrometeorológiai terhelése okoz gondot. A vízbázisok szennyezése tekintetében viszont a közvetetten kialakuló talajdegradáció[2] kiemelendő, hiszen a talaj szűrő- és védőfunkciójának változása miatt könnyebben elszennyeződhetnek a felszín alatti vizek. Az is tény, hogy a földterülethez kötődő mezőgazdasági feladatok elvégzésének késleltetése, helyreállítási feladatokhoz kapcsolódó infrastruktúra kialakítása, illetve fokozott energiabeviteli körülmények vezethetnek szennyezéshez. [5]

Az *esőzések* is komoly károkozási hatással bírnak. Az elmúlt évtizedek klímaváltozási folyamatainak következményeképpen is megnövekedett a hirtelen, monszunszerű esőzések száma, ami az egységnyi idő alatt lehullott csapadékmagasság drasztikus emelkedésével járt, jóllehet bebizonyították, hogy az egy időszakra jutó átlagos csapadékmennyiség nem változott, csak a csapadék hullásának intenzitása erősödött meg. Általánosan kijelenthető, hogy a vízelvezető és kiegyenlítő műtárgyak elhanyagoltak (még akkor is, ha az utóbbi időben a közmunkások tevékenysége miatt ezen a területen javulás tapasztalható), vagy hiányoznak, ezért az özönvízszerűen lehulló csapadékmennyiséget az amúgy is terhelt csatornahálózat nem tudja elvezetni. Megfelelően méretezett kiegyenlítő műtárgyak hiányában a túlzott esőzések rendkívüli hidraulikai és szennyezőanyag terhelést jelentenek az élővizekre. Az eltömött, vagy nem rendesen tisztított, feliszaposodott árkok gyakran megtalálhatóak az időként előforduló vízminőségi haváriák okai között. [6] Meg kell említeni a lehullott csapadék mennyisége mellett annak minőségét is. Egyrészt a megnövekedett motorizáció, az atmoszférában kiülepedő szennyeződések, a téli időszakban a jegesedés ellen használt sószórás, de a mindennapos emberi tevékenységek is mind a csapadékok minőségének romlásához, és ezáltal a vizek szennyezéséhez járulnak hozzá.

[2] Olyan összetett folyamat, amely a talaj alapvető tulajdonságaiban (szűrő-védő funkció pl.) visszafordítható vagy visszafordíthatatlan változásokat okoz.

Jóllehet manapság az infrastruktúra fejlődésével egyes iparágak már helytől és nyersanyagtól függetlenül településhetnek, elmondható, hogy az *ipar* telepítési tényezői közül még mindig jelentős szerepet játszanak az ásványkincsek, energiahordozók, éghajlati tényezők, a víz, etc., mint a természeti, földrajzi környezet elemei. A Paksi Atomerőmű esetében például nem volt kérdéses, hogy csakis a Duna mellé településhet, hiszen az üzemnek akkora a hűtővízigénye, hogy azt még második legnagyobb hozamú folyónk, a Tisza sem tudta volna kielégíteni.

A környezet védelme érdekében is legtöbb esetben igyekeznek jogszabályi úton beszabályozni az ipari tevékenységek megkezdését, illetve folytatását, az esetleges környezetszennyező tevékenységre vonatkozó megelőzési és kárelhárítási tervek megalkotását. Magyarországon az 57/2013. (II.27.) Kormányrendelet a telepengedély, illetve a telep létesítésének bejelentése alapján gyakorolható egyes termelő és egyes szolgáltató tevékenységekről, valamint a telepengedélyezés rendjéről és a bejelentés szabályairól rendelkezik arról, hogy mely ipari tevékenységek folytathatóak telepengedély birtokában és melyek csak bejelentés alapján. Mindezek azonban nem jelentenek teljes biztonságot, bármikor felléphetnek ipari balesetek. Ahogy nem tekinthetünk el azon szennyezések figyelembe vételétől sem, amelyek 20-30 éve bezárt ipari telepek „örökségeként" kerülnek napvilágra.

Az ipari eredetű és természetes szennyezések mellett vannak *egyéb szennyezési* módok is. Nem egy, részben korszerűtlensége, részben telítettsége miatt már bezárt hulladéklerakó a mai napig lokális szinten kockázatot jelent. A belőlük származó terhelést nem lehet rekultivációval sem felszámolni tökéletesen. Az általános hulladéklerakók szennyező hatása mellett az is gondot jelent, hogy sokszor a hulladékot, a veszélyes ipari melléktermékeket a drága elhelyezési és/vagy ártalmatlanítási költségek miatt illegális módon helyezik le, tüntetik el, például erdőszélekre kihajítva, vízelvezető árkokba helyezve, tavakba, folyókba kezeletlenül, direkt módon belevezetve. Amellett, hogy a talajba és ezáltal a felszín alatti vizekbe bemosódva már a lerakás helyszínén is kárt okoznak, a mozgó vízáramok magukkal viszik a szennyezéseket, egy nagyobb folyó vagy egy árhullám esetében akár több száz kilométerrel a szennyezés eredeti helyszínétől okozva problémát. Hazánk e tekintetben is hátrányos helyzetben van, elsődlegesen a Felső-Tisza környékén található zömében külföldi eredetű hulladék és szennyezés. Itt kell megemlíteni a szándékos károkozásokat is. [3]

VÍZMINŐSÉGI KÁRELHÁRÍTÁS

Hazánkban szervezett vízminőség-védelmi tevékenységről az 1960-as évek óta beszélhetünk. A vízminőség-védelmi feladatok részét képezi a vízminőségi kárelhárítás, ami több fázisból áll [7]:

- a védekezésre való felkészülésből, a rendkívüli szennyezések megelőzéséből,
- a rendkívüli szennyezések észleléséből, felderítéséből és minősítéséből,
- a kárelhárítás műveleti végrehajtásából, valamint a szennyezés megszüntetését követő intézkedésekből.

Magyarország tranzit szerepe is hozzájárul ahhoz, hogy a közutakon kiemelkedő számú haváriahelyzet alakuljon ki műszaki hiba, gondatlanság vagy baleset miatt. Földrajzi és geopolitikai elhelyezkedésünkből kifolyólag is különlegesen kedvezőtlen helyzetben vagyunk. A társadalmi-gazdasági átalakulás a volt keleti blokk utódállamaiban sem feltétlenül volt jó hatással a környezetvédelemre (törekedés a gyors haszonszerzésre, távoli országokból érkező befektetők, akik nem tartják be, illetve akikkel nem tartatják be a környezetvédelmi előírásokat, csakhogy befektetőként megszerezhessék őket; és akiktől károkozás esetében sem lehet behajtani a kárelhárítás költségeit – ld. ausztrál befektető és a tiszai ciánszennyezés). Hazánk Uniós csatlakozásával a vízminőség-védelem, a vízminőségi kárelhárítás fő

irányvonalai, a feladatok részletes szabályozása a közösségi normákhoz kapcsolódóan is megtörtént. A megváltozott feltételek, illetve szabályok további segítséget nyújtanak a magyar vízminőségi kárelhárítási szakembereknek a rendkívüli szennyezések megelőzésében, észlelésében, nyomon követésében, minősítésében és elhárításában egyaránt.

Rendkívüli (vagy váratlan) vízszennyezésnek nevezzük a felszíni és felszín alatti vizek minőségi állapotát, öntisztulási képességét, valamint a felhasználásra való alkalmasságát alapvetően veszélyeztető vagy jelentős mértékben korlátozó emissziókat. Ezek a szennyezések a potenciális szennyező források műszaki hibája vagy gondatlan kezelése, baleseti vagy természeti okokból következhetnek be. Ha a szennyezés váratlanul, hirtelen valamely baleset, műszaki meghibásodás, mulasztás hatására helyi jelentőséggel, erőteljesen következik be, akkor havária szennyezésről beszélünk [3]. Az ez elleni védekezés magában foglalja mind a szükséges megelőző védekezési intézkedéseket, mind a már szennyezett víz által esetlegesen okozható további káresetek megakadályozását.

Napjainkban a potenciális vízszennyező forrásként számításba vehető üzemek, intézmények, telephelyek már az engedélyezési eljárásnál meg kell, hogy oldják a belső technológiai és üzemi szabályozásuk során mindazon feladatokat, amelyek a tevékenységből fakadó vízgazdálkodási problémák megelőzését célozzák. Egy vágóhíd vagy húsfeldolgozó üzemből származó víz például nem számít veszélyes hulladéknak, viszonylag egyszerű szűrő- és zsírfogó rendszeren való átvezetés után bevezethető a települési szennyvízhálózatba. A katasztrófavédelem sokéves tapasztalata azonban azt mutatja, hogy a legnagyobb erőfeszítések árán sem lehet mindig megelőzni a rendkívüli vízszennyezéseket, ezért a vízminőségi károk elhárítására, illetve csökkentésére fel kell készülni.

A felszíni vizek szennyeződésekor a vízfolyások szennyeződése szerencsésebb. A lassú mozgású vagy állóvizek esetében sokszor a negatív hatás nem azonnal jelentkezik, hisz a szennyezés hatására megnövekedhet a vizek oldott só- és szervesanyag-tartalma, elindulhat az eutrofizáció, vagy a szennyezések az iszapba kiülepedve okozhatnak kárt. Ilyenkor a vízminőségi kárelhárítás kettős feladattal rendelkezik. Fel kell számolni a bekövetkezett káreseményt, illetve meg kell előzni a vízi ökoszisztéma károsodását.

A már említett 219/2004. Kormányrendelet szerint a kármentesítés fogalma magában foglal minden olyan helyreállítási intézkedést, amely „*a felszín alatti víz és földtani közeg károsodásának enyhítésére, az eredeti állapot vagy ahhoz közeli állapot helyreállítására, valamint a felszín alatti víz által nyújtott szolgáltatás helyreállítására vagy azzal egyenértékű szolgáltatás biztosítására irányul, így különösen az a műszaki, gazdasági és igazgatási tevékenység, amely a veszélyeztetett, szennyezett, károsodott felszín alatti víz, illetőleg földtani közeg megismerése, illetőleg a szennyezettség, károsodás és a kockázat mértékének csökkentése, megszüntetése, továbbá monitorozása érdekében szükséges.”* [8]

A kárelhárítás módszerének megválasztásakor általában abból indulnak ki, hogy a szennyezett terület talajában, és ezáltal az ottani vízbázisban található szennyező anyagok mértéke eléri-e a 6/2009. (IV.14.) kvVM-EüM-FVM együttes rendelete által meghatározott (B)[3] szennyezettségi értéket[4]. A kárelhárítás során nem a teljes kárfelszámolás, illetve a szennyezőanyagok teljes eltávolítása a cél, hanem az, hogy a műszaki beavatkozások

[3](B) szennyezettségi határérték: jogszabályban, illetve ennek hiányában hatósági határozatban meghatározott olyan szennyezőanyag-koncentráció, illetve egyéb minőségi állapotjellemzők olyan szintje a felszín alatti vízben, a földtani közegben, amelynek bekövetkeztekor a földtani közeg, a felszín alatti víz szennyezettnek minősül, figyelembe véve a felszín alatti víznél az ivóvízminőség és a vízi ökoszisztémák, továbbá a felszín alatti víztől függő szárazföldi ökoszisztémák igényeit, földtani közeg esetében pedig a talajok többes rendeltetését és a felszín alatti vizek szennyezéssel szembeni érzékenységét – 219/2004. Kormányrendelet 3§. 3.

[4] A felszín alatti vizekre vonatkozó határértékeket a rendelet 2. sz. melléklete tartalmazza.

következtében az egyes szennyező anyagok mértéke a (B) értékzónából a (D)[5] határérték alá csökkenjen.

KÁRMENTESÍTÉSI MEGOLDÁSOK

A kármentesítési eljárás kiválasztásakor együttesen kell figyelembe venni a humán, a környezeti és környezetvédelmi kockázatokat. A legalkalmasabb módszer egy adott szennyezés mentesítésére számos tényezőtől függ. A szennyező anyag fizikai és kémiai tulajdonságai, a szennyezett közeg hidrogeológiai adottságai, hogy van-e a közelben vízkivételi műtárgy, a mentesítést követő tervezett területhasználat, valamint hatósági és lakossági vélemények mind szerepet játszanak benne. [9] Természetesen az alkalmas technológia megválasztásakor szerepet játszik a költséghatékonyság, de a fenntarthatóság elve is. Pont ez a fenntarthatósági tényező az, ami miatt az utóbbi időben a kármentesítés az egyes fizikai és kémiai módszerek felől egyre inkább eltolódik a biodegradációs módszerek irányába, azaz a bioremediáció[6] felé. A fizikai és kémiai tisztítás során sokszor a szennyező anyag nem szűnik meg létezni, csak annak térfogata csökken, valamint veszélyes hulladék és melléktermék is képződik, amelynek megsemmisítéséről szintén gondoskodni kell (pl. hazánk esetében a dorogi hulladékégetőbe kerül, ahol bár a mellékesen keletkező hőt hasznosítani tudják a távhőszolgáltatásban, korántsem járul hozzá a fenntarthatósághoz). Jóllehet a fizikai és kémiai technológiák hatékonysága, a szennyezés felszámolásának mértéke eléri a 95-98%-ot, ráadásul a kivitelezés ideje is elég gyors, nem tekinthető költséghatékonynak. A biológiai tisztítási módszerek hátránya viszont, hogy csak bizonyos típusú szennyezőanyagok és szennyezési koncentrációk mellett alkalmazhatóak, és a környezeti állapot változása befolyásolhatja a folyamatot. Ugyanakkor jóval költséghatékonyabb eljárás, mint bármelyik másik. Sok esetben, mivel a (főleg nagy kiterjedésű) szennyezett területek kármentesítésénél nem a célterület teljes mentesítése, csak a „D" határérték elérése a cél, előnyben kell részesíteni a biológiai, in situ megoldásokat. [3]

A szennyezések eltávolítása történhet helyben (in situ) és lokalizálás után kiemelve, eltávolítva (ex situ) is. Ez utóbbinak két típusa ismert, az on site és az off site. Az on site mentesítési folyamat alatt azt értjük, amikor a szennyezett környezeti közeget kiemelve kezelik, viszont a kitermelt talajt, vagy talajvizet a művelet helyszínén tisztítják meg. Ezzel szemben az ex situ, off site mentesítés abban tér el az eddigiektől, hogy a kitermelt közeg elszállításra kerül és azt a kitermelés helyszínétől távol mentesítik. Sokszor az in situ eljárások ex situ elemekkel együtt működnek. Az in situ eljárások többnyire helyspecifikusak, egyediek, amelyeket az érintett területek heterogenitása miatt nem egyszer módosítani kell a helyszíni adottságokra szabva. [9]

FIZIKAI ÉS KÉMIAI MÓDSZEREK

Fizikai módszereknek tekinthetőek mindazok, melyek során a vízkészletekre károsan ható oldott szennyeződéseket úgy távolítják el, hogy a szennyezett vizet, vagy a vízben található

[5](D) kármentesítési célállapot határérték: hatósági határozatban előírt koncentráció, amit a kármentesítés eredményeként kell elérni az emberi egészség és az ökoszisztéma, illetve a környezeti elemek károsodásának megelőzése érdekében; meghatározása a kármentesítési eljárás keretében végzett komplex értékelésen, a szennyező anyagnak a környezeti elemek közötti megoszlására, viselkedésére, terjedésére vonatkozó méréseken, modellszámításokon, kármentesítési mennyiségi kockázatfelmérésen alapul a területhasználat figyelembevételével – 219/2004. Kormányrendelet 3§. 4.

[6]Gyógyítás, ártalmatlanítás, esetünkben a vegyi anyagokkal szennyezett környezeti elemek kockázatának elfogadható mértékűre csökkentése

szennyeződéseket valamely módon felduzzasztva és/vagy visszatározva lokalizálják és eltávolítják. A fizikai eljárásokat többnyire nem egyedien használják, sokszor valamely kémiai vagy esetleg biológiai elhárítási módszerrel együtt alkalmazzák. A kémiai módszerek elsődlegesen a vízben oldott anyagok eltávolítását, csökkentését célozzák meg kémiai reakciók segítségével, például valamely reagens anyag (savas/bázisos/a levegő oxigénje) hozzáadása által. Ezek a reagensek lépnek például redox reakcióba a szennyezés adott komponensével (komponenseivel), és valamely veszélytelen vagy kevésbé veszélyes terméket képeznek. A kémiai kezelés alatt többnyire a víz pH értékének az élettani szempontok szerinti határok közötti értékre való visszaállítását értjük a természetesen kissé lúgos, általában 7 és 8 közötti pH értékre. A savas szennyezők közömbösítése lúgos anyagokkal, például mésztej, szóda adagolásával történik a pH-érték növelése céljából, ezzel szemben a lúgos szennyezők közömbösítésére, a pH-érték csökkentésére savas anyagokat használnak. A mérgező gázok, mint ammónia és kénhidrogén esetében olyan egyéb vegyi anyagokat kell a vízhez adagolni, amelyeknél oldott gáz állapotban maradnak a vízben, ahonnan aztán levegőztetéssel eltávolíthatóak („kihajtás" – stripping, purging). Tehát a kémiai módszereket is gyakran kiegészítik fizikai beavatkozással. [3]

Az egyik legjellemzőbb fizikai-kémiai beavatkozás a *levegőztetés*, amelynek során a szennyezett víztömeget mesterséges beavatkozással oxigénben dúsítják. A műveletnek az a célja, hogy a biológiailag bontható szerves anyagokat, az elszíneződést okozó szennyezéseket, valamint a vízben oldott mérgező gázokat távolítsa el a szennyezett vízből. A víz oldott oxigéntartalma a következő módszerekkel növelhető: porlasztás, permetezés, csörgedeztetés, légbefúvás. [3] Gyakorlati megvalósítása nem mindig lehetséges, sokszor nem gazdaságos, a helyszíni adottságok nem mindig engedik. A levegőztetést megoldhatják például a helyszínen lévő műtárgyak (zsilip, duzzasztómű) felhasználásával, ami gyors és egyszerű megoldás, hiszen nem kell extra technikai eszközöket felvonultatni, hátránya viszont szintén ebből származik, mert helyhez kötött, s csak ott megvalósítható, ahol a műtárgy létezik. Hasonló funkciót tölthetnek be a bukógátak, amelyeknek az az előnye, hogy meglétük hiányában akár ideiglenesen is kiépíthetőek homokzsákból, kőből, farönkökből, etc. Mobil – és jól bevált – megoldást jelent a szivattyúzás vízsugárképzéssel, melynek során a kiáramoltatott, porlasztott víz nagy felületen képes oxigénnel dúsulni, és ezáltal lebontja az oxidálható szennyeződéseket. Léteznek mindezek mellett felületi levegőztető és légbefúvó berendezések is.

Úszó olajszennyezéseket el lehet távolítani vákuumos szabadfázis kitermeléssel, ötvözve a technológiát a bioventillációval. A bioventilláció elősegíti a szénhidrogének aerob lebomlását, a vákuumos szabadfázis kitermeléssel a könnyű, felúszó szennyezőktől szabadítják meg a vízfelszínt, vagy akár a talajkapillárisokat is (részletesebben erről a 2. cikkben). [10]

A levegővel történő *sztrippelés* egy olyan ex situ eljárás, amely szintén alkalmas mind felszín alatti, mind felszíni és csurgalékvizek kezelésére. Ennek során úgy választják el a szerves vegyületeket a vízbázistól, hogy megnövelik a szennyezett víz levegővel érintkező felületét. Mindez történhet töltetes tornyokban, diffúz vagy tálcás levegőztetőkkel és permetezéssel. Az eljárás során a szennyező anyagok a vízből a levegőbe áramlanak. De sztrippeléses eljáráson alapul például a talajvíz-keringető kút is. Ezen esetben a kút talpszintjén és a talajvízszint magasságában is megszűrik a vizet. Egy injektáló csövön keresztül levegőt nyomnak a kút vízszintje alá, amitől felfelé irányuló vízáramlás alakul ki, és az illékony szennyező anyagok sztrippelődnek. A távozó szennyezett levegőt felfogják és továbbkezelik, a mentesített víz pedig visszajut az eredeti helyére. Mivel a talajvízkivétel és -visszajuttatás eltérő mélységben történik, a környező víztartó zónában megindul a talajvíz keringése, és az érintett talajzóna is alaposan átöblítődik, hidraulikusan tisztul.

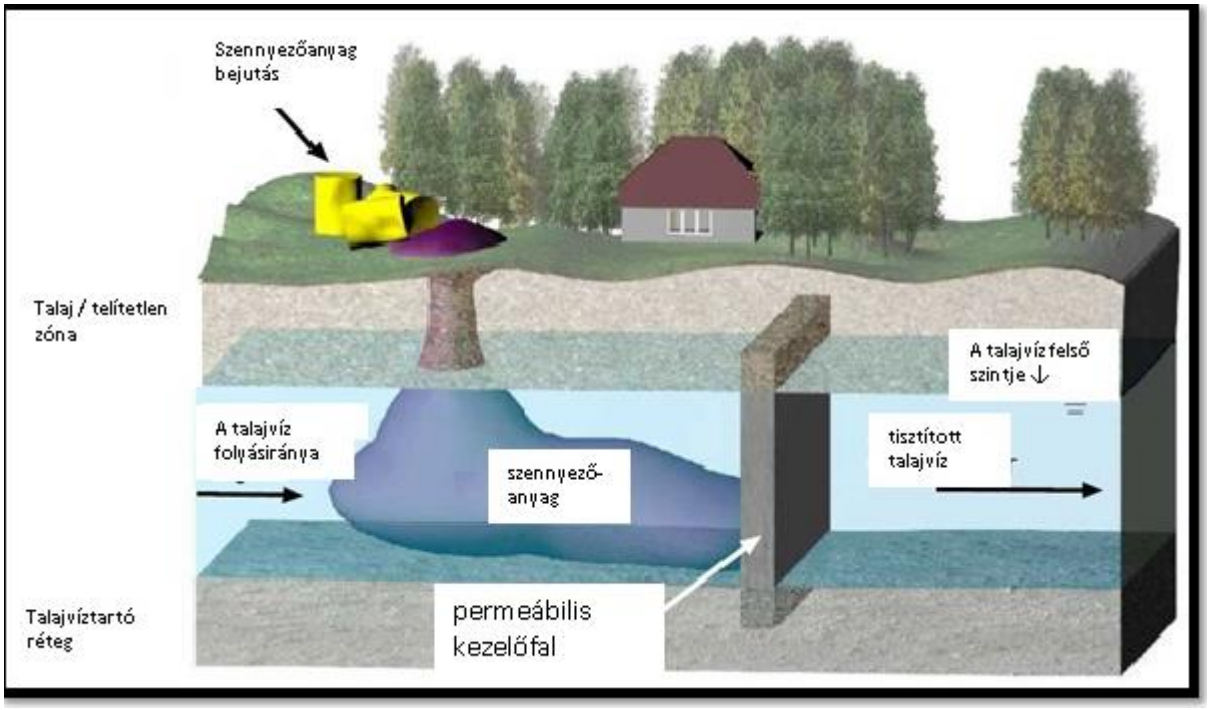
A vízben található lebegőanyag tartalom eltávolítása történhet még *fáziselválasztás*sal. A fáziselválasztás alkalmazható szennyezett felszíni, felszín alatti és csurgalékvizek kezelésére.

A fáziselválasztás során a szennyezőket a hordozó közegtől (jelen esetben a vízből) próbálják fizikai és/vagy kémiai úton elválasztani. A fáziselválasztás számos módon megvalósítható: desztilláció, szűrés, fagyasztásos kristályosítás, fordított ozmózis stb.

Az *adszorpción* alapuló eljárás során a vízbázisokban oldott szennyező anyagok egy adszorbens felületén megkötődnek, így csökken a koncentrációjuk a folyadékban. A leggyakoribb adszorbens az aktív szén, de használnak még egyéb ásványi anyagot, például zeolitot, illetve szintetikus gyantákat is. Az adszorpciós eljárás ex situ folyamat, amikor is a szennyezett víz kitermelésre kerül, és azt átvezetik az adszorbens felületen, amely így megköti a szennyező anyagokat. Általában szerves eredetű szennyezések eltávolítására alkalmas. Az adszorbenst regenerálni kell/lehet, kivéve, ha az nehézfémekkel szennyezett. Ilyenkor veszélyes hulladékként kezelve biztonságos elhelyezése szükséges. Adszorpciós eljárással távolítják el például a felszíni vizekbe került olajszennyeződéseket is.[3] Az utóbbi időben egyre gyakrabban használnak *zeolit*ot adszorbensként, annak számos előnye miatt. Megtalálható a természetben, de viszonylag könnyen előállítható mesterségesen is. A zeolitok felületén üregek találhatóak, amelyeket alumínium-, szilícium- és oxigénatomok alkotnak. Ezek az üregek, pórusok molekulaméretűek és ezek segítségével óriási hálókat tudnak alkotni, hatalmas aktív felülettel, ahol a zeolit ki tudja fejteni a katalitikus hatást. Arra is van lehetőség, hogy egyes fémeket beültessenek ezekbe az üregekbe, ahol a zeolit képes az egyes alkánokat megfogni, kisebb méretűvé alakítani. A zeolitokat több területen fel tudják használni, katalitikus és abszorbens hatása mellett a pH szabályozó hatása is ismert, lágyítja a vizet, megakadályozza annak túl lúgosodását. A zeolitot molekulaszitának is nevezik, mert az olyan kis méretű molekulákat, mint például a víz vagy a metán átengedi, de az elágazó láncú szénhidrogéneket vagy a nagyobb molekulákat, például a benzolt már nem. Kiváló adszorbeáló tulajdonsága mellett emiatt is használják a kármentesítéskor. Ráadásul a zeolit módosítható, ami által változhat a „szita” mérete, azaz szabályozható, mekkora molekula mehet át rajta. [11]

Vannak esetek, amikor a kármentesítés során például a szennyező forrásokhoz nem lehet hozzáférni, a további szennyezést nem lehet megállítani, és a kármentesítés csak a szennyező csóvában lehetséges. Amennyiben a szennyezési terhelés nem túl nagy, a víz áramlására merőlegesen elhelyezett *permeábilis kezelőfalak* alkalmazása lehetséges. Természetesen ez inkább csak a kockázatcsökkentést szolgálja. Alkalmas nehézfémek kicsapatására, illetve illékony klórozott szerves vegyületek dehalogénezésére is. Ahogy a neve is mutatja, a kezelőfalak víz által átjárható építmények, elemek, amelyeket reaktív közeggel töltenek fel. A szennyezett talajvíz keresztüláramlik a falon (ld. 1. ábra), illetve a benne elhelyezett töltőanyagon, amely a szennyező anyagokat vagy megköti, vagy visszatartja. Élettartamuk hosszú, kevés karbantartást igényelnek. Lehetnek biológiailag reaktívak, például komposztot, faforgácsot tartalmaznak, melyhez a pH-értéket korrigálandó mészkövet adagolnak. Alkalmazható benne például aktív szén is, ráadásul ennek felületére speciális lebontó mikroorganizmusokat is lehet telepíteni. Amennyiben nem kell ezt a kezelőfalat túl mélyre juttatni, akár a bioreaktív töltetek cserélhetőek, regenerálhatóak is. Hátránya, hogy folyamatos monitorozása szükséges, hiszen a felfogott szennyező anyagok miatt a fal permeabilitása[7] csökkenhet, amelynek következtében az áramló víz megkerülheti a kezelőfalat. [12]

[7] áteresztőképesség

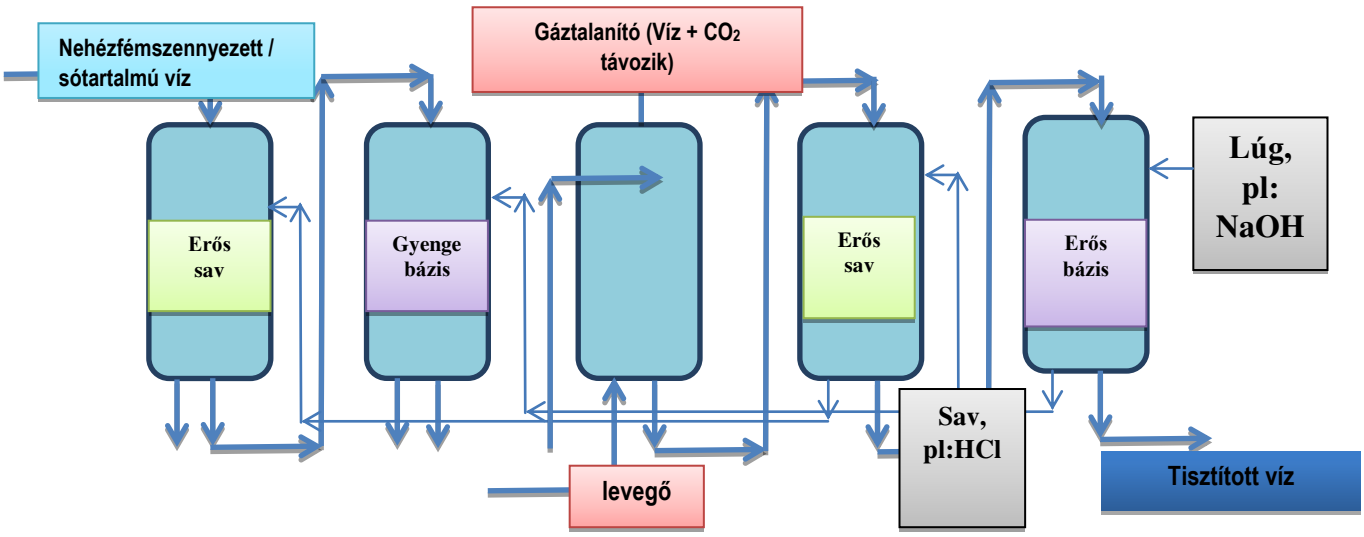


1. ábra Permeábilis kezelőfal elhelyezése a szennyeződések továbbjutásának megakadályozására [13]

A *kicsapatás* és *derítés* alkalmas mind szennyezett felszíni, mind felszín alatti vizek kezelésére ex situ kémiai eljárással, amely során a vízben oldott formában jelenlévő szennyezőket szilárd, nem oldódó, kis átmérőjű szuszpendált részecskékké alakítják, azaz kicsapatják. Miután ezeket koagulációval, flokkulációval alkalmassá teszik a fáziselválasztásra, ülepítéssel vagy szűréssel eltávolítják. Jelen esetben is kémiai és fizikai módszerek vegyítése történik. Ezt a módszert elsősorban nehézfém- és radioaktív izotóp szennyezők esetén érdemes alkalmazni.

Ioncserés eljáráskor a vizes fázis ionjait az ioncserélő közeg ionjai váltják fel. Ioncserélő közegként különböző gyanták szolgálnak, amelyek lehetnek természetesek, de mesterségesen előállítottak is. Az eljárás során használt gyanták regenerálhatóak és újrafelhasználhatóak. A vízből mind a nehézfémeket, mind a víz sótartalmát el lehet távolítani ioncserével. Az ioncsere szorpciós folyamat, ahol az ioncserélő – pozitív vagy negatív töltésű ionos aktív csoport – az egyes ionjait a vizes oldatban lévő, azonos töltésű ionokkal képes kicserélni. A folyamat reverzibilis, az oda-, ill. visszacsere feltételeinek biztosításától függően. Ezáltal biztosítható az ioncserélő anyagok kimerítése ill. regenerálása. Az ioncserélő gyanták akkor képesek ioncserére, ha a kicserélendő ionoknak nagyobb az affinitása az aktív csoporthoz, mint a benne lévő ioné, vagy pedig az oldatban lévő ionok koncentrációja elég nagy ahhoz, hogy a tömeghatás törvényének érvényesülésével az egyensúly felboruljon. Az erősen bázisos anioncserélő gyanták kvaterner-ammónium aktív csoportokat tartalmaznak, amelyek affinitása a OH^- -ionokhoz kicsi, ezért azt bármely más anionra kicserélik. Regenerálásukhoz éppen ezért erős lúgra van szükség. [13] A leghatékonyabb mentesítést négylépcsős rendszerrel lehet elérni. Ebben a rendszerben az ellenionhatást használják ki. A H^+ formájú erősen savas kationcserélő oszlop után elhelyezett OH^- formájú, gyengén bázisos oszlopot gáztalanító követi, ahol a keletkezett szén-dioxid eltávozhat, majd ismét erősen savas H^+ és erősen bázisos OH^- formájú oszlop. Ezt a rendszert mutatja be a 2. sz. ábra. A nehézfémek vízből való kicsapatása összetett folyamat, ami ahhoz kell, hogy eltávolítható legyen a szennyvízből. Be kell állítani ehhez a biológiai folyamatokra ártalmatlan pH értéket, másrészt

a megfelelő reagens anyagot kell használni, hogy az oldott nehézfémek átalakítása nehezen oldódó hidroxidokká vagy bázikus sókká megvalósulhasson, hogy azok a szennyvízből eltávolíthatók legyenek.



2. ábra Négylépcsős ioncserélő rendszer (saját szerkesztés [14] számára)

Az *ozonizálás* és az *UV-oxidáció* alkalmas mind felszíni vizek, mind felszín alatti vizek ex situ kezelésére, mindenekelőtt kőolaj származékok, növényvédőszerek, gyomirtók és egyéb toxikus anyagok eliminálására. A szennyezést úgy távolítják el, hogy ózon és hidrogén-peroxid segítségével létrehozzák a hidroxil gyököt, amely kifejezetten agresszív oxidatív hatással rendelkezik. A hidrogén-peroxidot a szennyezett vízhez keverik, az ózont pedig ellenáramoltatják a peroxiddal dúsított vízben, miközben az egészet UV lámpával világítják meg. Ezt a folyamatot többször is megismétlik egymás után. Az UV világítás hatására jön létre az a reakció, amely a hidroxil gyököt létrehozza és oxidálja a szennyezést. A reakció során maradhat felesleges ózon, amelyet oxigénné redukálnak és elvezetnek.

KÖVETKEZTETÉSEK

A vízbázisaink védelmével kapcsolatos jelenlegi és jövőbeli feladatok meghatározásánál figyelembe kell venni, hogy mennyire érzékenyek ezek a mindennapi életünkhöz szükséges rendszerek, hogy azok egyes elemei bizonyos mértékig könnyen támadhatóak, a közhasználat miatt nehezen védhetőek, egynémelyük kiiktatása – ha csak időlegesen is – nem igényel sem különösebb szakértelmet, sem szervezést. Fenntartható életmódunk megkívánja, hogy ne a kármentesítés legyen az elsődleges feladatunk, hanem az egyes környezeti elemek szennyeződésének megelőzése.

A bemutatott kármentesítési módszerek sokban hozzájárulnak ahhoz, hogy megszabadíthassuk környezetünket, és ezen belül vízkészleteinket bizonyos szennyezésektől. Ezen cikk kifejezetten a vízbázisokat érő szennyezések mellett az azok mentesítésére alkalmazott fizikai és kémiai elvű műszaki megoldásokat célozta bemutatni, illetve a cikk második része fog kitérni a biológiai mentesítési módszerekre. Az itt felsorolt technológiák külön-külön vagy egymással ötvözve, egymást kiegészítve is alkalmasak a felszíni, felszín alatti, a csurgalék- és talajvizek megtisztítására, az egyes szennyezőanyagok eltávolítására. Ahogy az általános technológia, úgy a kármentesítési módszerek is rohamosan fejlődnek, egyre újabbakat kísérleteznek ki, és egyre nagyobb hangsúlyt fektetnek a környezetbarát

technológiák alkalmazására, amelyek kevéssé drasztikus beavatkozással járnak, ezért azok egyre inkább teret nyernek, hiszen „zöldebbek" és „környezetközelibbek", mint jó néhány korábban alkalmazott és itt bemutatott ex situ eljárás.

FELHASZNÁLT IRODALOM

[1] A felszín alatti vizekkel kapcsolatos fontosabb nemzetközi és hazai jogi szabályozás, http://www.kvvm.hu/szakmai/karmentes/kiadvanyok/fav/favm/favm03.htm, (letöltve: 2017. március 18.)

[2] MÁDLNÉ Dr. Sz. J. (szerk.): Hidrogeológia, http://elte.prompt.hu/sites/default/files/tananyagok/Hidrogeologia/ch02s03.html (letöltve: 2017. március 18.)

[3] PREGUN Cs., JUHÁSZ Cs.: Vízminőség; http://www.agr.unideb.hu/ebook/vizminoseg/ (letöltve: 2015. február 28.)

[4] DR. KONECSNY K.: A víz, mint erőforrás és kockázat, http://www.tankonyvtar.hu/hu/tartalom/tamop425/0038_foldrajz_konecsnykaroly/ch01s02.html, (letöltve: 2017. március 18.)

[5] BÁRDOS Z., MUHORAY Á.: A belvíz kialakulása és az ellene való védekezés lehetőségének vizsgálata, Hadmérnök VII. évfolyam, 1. 2012, pp.79-80.

[6] VARGA M., VÁRADI J.: Vízvisszatartás – tározás – vidékfejlesztés, MTA Történettudományi Intézet – MTA Társadalomkutató Központ, Budapest, 2010, 97.o.

[7] DR. FEKETE E.: Vízminőség, kárelhárítás; http://www2.ativizig.hu/karelhx/vizmin.aspx, (letöltve: 2014. március 27.)

[8] 219/2004. (VII. 21.) Kormányrendelet a felszín alatti vizek védelméről (letöltve: 2015. március 27.)

[9] DR. HALÁSZ L., DR. FÖLDI L.: Környezetvédelem II., ZMNE-BJKMK, ABV Tanszék, Budapest, 2007

[10] Kármentesítési kézikönyv 4, Kármentesítési technológiák, Környezetvédelmi Minisztérium, Budapest, 2001, http://www.kvvm.hu/szakmai/karmentes/kiadvanyok/karmkezikk4/4-07.htm (letöltve: 2015. Április 16.)

[11] Zeolit: Education in Chemistry, Molekulamagazin, http://www.kfki.hu/~cheminfo/hun/tudakozo/mm/zeolit.html (letöltve: 2015.május 19.)

[12] U. FÖRSTNER, P. GRATHWOHL: Ingenieurgeochemie, Technische Geochemie - Konzepte und Praxis, Springer Verlag, 2003, p.244.

[13] http://www.rubin-online.de/deutsch/einleitung/wasist/ (letöltve: 2015. május 22.)

[14] DR. DOBOR J., HEGEDŰS H.: Особенности гидроксида натрия, его использование, значение в наши дни, Hadmérnök, X. évfolyam, 1. 2015, p.86.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

A BIZTONSÁGUNKAT VESZÉLYEZTETŐ TÉNYEZŐK, ÉS A KATASZTRÓFÁK ELLENI VÉDEKEZÉS ÁTFOGÓ MEGKÖZELÍTÉSE

FACTORS THREATENING OUT SECURITY AND A COMPREHENSIVE APPROACH TO THE PROTECTION AGAINST DISASTERS

HORNYACSEK Júlia

(ORCID ID: 8695713152-13391)

hornyacsek.julia@uni-nke.hu

Absztrakt

A körülöttünk lévő veszélyek ismerete, és az azokra való felkészülés elengedhetetlen feltétele annak, hogy legyen esélyünk elkerülni az események negatív hatásait, minimalizálni a veszteségeket, károkat. Az állam és a közszféra feladata az ország, a lakosság és az anyagi javak védelme, de egyre inkább terjed az az átfogó megközelítés, miszerint a veszélyeztető tényezők elleni küzdelem össztársadalmi feladat, melyben szerep hárul a hivatásos mentőszervekre és a közigazgatás miden szintjére is.

A cikkben a szerző vizsgálja a veszélyeztető tényezőkkel kapcsolatos hazai irodalmak megállapításait, bemutatja a lehetséges hatásokat, valamint a katasztrófa-kárterületek jellemzőit, az ott végzendő, főleg műszaki jellegű feladatokat, javaslatot tesz a katasztrófa-kihívásokra válaszként működtetett védelmi rendszerre, és annak alrendszerei átfogó megközelítésére.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Zrínyi Miklós Habilitációs Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak *komprehenzív megközelítés, biztonságot veszélyeztető tényezők*

Abstract

Knowledge and preparedness for the threats around us are essential prerequisites to decrease the negative impacts of these events and to minimize losses and damages. Protecting the country and its inhabitants are primarily tasks of the State and public sector, but according to a comprehensive approach it shall be contribution of the whole society. This involves professional emergency organizations, public administration at all levels, non-governmental organizations and citizens.

In this article the author examines ascertainments of the national bibliography related to risk factors, presents the potential impacts of disasters, the characteristics of the disaster-damage areas along with the connected technical tasks and proposes to use a comprehensive approach for disaster management system and its sub-components.

Keywords *comprehensive approach, safety risk factors*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.24.

BEVEZETÉS

A „Bízzál Istenben és tartsd szárazon a puskaport!"-gondolat nem mai keletű, az angol polgárháború idején az independensek jelszava volt, és jól tükrözte, hogy már az akkori emberek is tudták, hogy akkor van esélye a túlélésnek, ha felkészültek a veszélyekre, ha számítanak a váratlan helyzetekre, és megvannak a képességeik a megfelelő válaszra. Bármennyire is véget ért a kétpólusú világrend és a hidegháborús korszak, a biztonsági környezet megváltozása és a megjelenő új kihívások okán, újra az államok és az állampolgárok fő célkitűzése lett, és fókuszba került a biztonságra való törekvés. A felkészülés igénye mára a mindennapjaink részévé vált. Bizonyított tény, hogy a rendkívüli helyzetek megelőzése, vagy bekövetkezésük esetén az emberi élet mentése, a károk elhárítása és felszámolása jelentős mértékben függ attól, hogy mennyire felkészültek a mentőerők és az állampolgárok. Mivel minden veszély, és az általa kialakult helyzet egyedi, ezért szükség van olyan ismeretekre, amelyek olyan átfogó tudásanyagot tartalmaznak, amelyek általánosak, több helyzetre vonatkoztathatóak, de könnyen kapcsolhatóak hozzájuk az egyedi, speciális helyzetek túléléséhez szükséges tudnivalók is. A hivatásos mentőerők, a védelmi igazgatás[1] szervezeti elemei, de a civil szervezetek körében is számtalan szakmai kiadvány és felkészítő anyag foglalkozik a témával, ezért nem nehéz hozzájutni a szükséges ismeretekhez. Ezek egy része az említett szervezetek saját állománya, tagsága stb. szakmai munkáját segíti, más része az érintett lakosság felkészítését szolgálja. A rendkívüli helyzetek felszámolása során azonban a fenti csoportoknak nem szeparáltan, hanem közösen kell megoldaniuk a problémát, együtt kell működniük, aminek elengedhetetlen feltétele az adott helyzet, valamint egymás működésének, tevékenységének, szabályzási kérdései hátterének ismerete.

Felmerül a kérdés, hogy mennyire ismerjük a körülöttünk lévő veszélyeket, azok hatásait? Milyen események várhatóak a jövőben, és ezek kapcsán milyen intézkedéseket kell hozni, adott esetben milyen feladatok hárulnak a közszférára, és milyenek a lakosságra? A fenti kérdések megválaszolásához meg kell vizsgálnunk a veszélyeztető tényezőket, azok lehetséges következményeit, és az adott esemény hatásmechanizmusát. Elemeznünk kell a várható kárterületek jellemzőit, prognosztizálni kell a szükséges feladatokat, nem szem elől tévesztve azok folyamat-jellegét, és az átfogó megközelítés szükségességét a kérdéskörben. Felmerül továbbá a kérdés, hogy milyen válaszokat ad hazánk a veszélyeztető tényezőkre, a jelenlegi védelmi rendszer hogyan működik, és hol helyezkedik el ebben a katasztrófavédelem rendszere. Az sem érdektelen, hogy milyen képességekkel kell rendelkezni az új kihívások tükrében a rendkívüli helyzetek elhárításához, a lakosság és az anyagi javak védelme érdekében.

Ebben a kutatásban célul tűztem ki, hogy a fenti kérdések megválaszolásával, a veszélyeztető tényezők, a várható események, a védelmi rendszer és működésének elemzése alapján olyan javaslatok kidolgozását, amelyek hatékonyabbá tehetik a veszélyekre való felkészülést, a katasztrófa-kárterületen végzett munkát, a lakosság és az anyagi javak védelmét.

[1]*Honvédelmi igazgatás:* a védelmi igazgatás részét képező feladat- és szervezetrendszer, amelynek keretében az ország védelmére létrehozott, valamint e feladatra kijelölt közigazgatási szervek, továbbá a honvédelemben közreműködő más szervek ellátják a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény (a továbbiakban: Hvt.) 1. § (3) bekezdésében meghatározottak honvédelemre való felkészítésével, az ország-védelemmel, és a honvédelmi kötelezettségek teljesítésével kapcsolatos feladatokat. [1;1.§]

Ennek érdekében tudományos módszerekkel az alábbi kérdéseket vizsgáltam:

1. Milyen tényezők veszélyeztetik napjainkban és a jövőben az ország és lakosainak biztonságát, ez hogyan jelenik meg a hazai tudományos publikációkban?
2. Milyen következménye lehet ezeknek a veszélyeztető tényezőknek, és a rendkívüli események során milyen kárterület, és kárterületi jellemzők alakulhatnak ki (fókuszálva a katasztrófa-kárterületekre), továbbá milyen feladatokat kell végezni az adott kárterületen?
3. Milyen az ország védelmi rendszere, és hol helyezkedik el benne a katasztrófavédelem, valamint annak hivatásos és civil ága, és hogyan lehet a rendszert a veszélyeztető tényezőknek leginkább megfeleltetni?
4. Melyek a katasztrófavédelmi kárterületi feladatok, és milyen a védekezés végrehajtási gyakorlata, továbbá miért szükséges az átfogó megközelítés (comprehensive approach) a katasztrófák elleni védelemben is?

Mivel a biztonságot veszélyeztető tényezők, és ezek között a katasztrófák elleni védelem is össztársadalmi feladat, melyben a közigazgatás (védelmi igazgatás) és a védelmi szféra minden ágának jelentős szerepe van, ezért a kutatás eredményei közvetve hozzájárulhatnak a védelmi feladatok ellátásáért felelős közszolgálati hivatásrendek hatékonyabb munkájához.

A kutatás és az alkalmazott módszerek leírása

A kutatás során elsősorban az analízis módszerével elemeztem a vonatkozó elektronikus és a nyomtatott hazai szak- és tudományos irodalmakat, a rendkívüli események esettanulmányait, a témával kapcsolatos jogszabályokat és védelemszakmai- és szakpolitikai szabályzókat. Ezután főként másodlagos adatok gyűjtésével és elemzésével dolgozva, az indukció módszerével vontam le következtetéseket.

A téma vizsgálandó fogalmainak azonosításához, lehatárolásához és változóinak meghatározásához, mélyinterjúkat készítettem gyakorló szakemberekkel és a szakmai gyakorlatom tapasztalatait is figyelembe véve alakítottam ki a vizsgálat menetét, főbb sarokpontjait. A kutatás indításakor a témában az eddig megjelent tudományos ismeretek rendszerére támaszkodtam, és mind a hermeneutikai, mind a természettudományos megismerési szemléletmódot igyekeztem megtartani és attól függően alkalmazni, hogy melyik részkutatáshoz mi felelt meg jobban. A veszélyek feltérképezésénél elsősorban a leíró, a kárterületi feladatok végrehajtása elemzésénél pedig a korrelációs kutatási stratégiát alkalmaztam. Feltételeztem, hogy a biztonság és az azt fenyegető veszélyek megjelenése az irodalmakban olyan következtetésekre ad lehetőséget, amelyből elindulva viszonylag jól prognosztizálható a következő időszak veszélyeztetettsége. Feltételeztem továbbá, hogy a katasztrófák következtében kialakult kárterületek összetettsége, az ott végzendő feladatok sokszínűsége miatt a katonai terminológiában használatos átfogó megközelítés a katasztrófavédelem[2] területén is szükséges, és időszerűvé vált azoknak a szegmenseknek a meghatározása, amelyek szükségszerűen az átfogó megközelítés szerint működnek, de annak tudományos igényű alátámasztása még várat magára.

[2] Fontos megjegyezni, hogy a katasztrófavédelem fogalom alatt nem a hivatásos katasztrófavédelmet értem, hanem a katasztrófák elleni védelemre létrehozott komplex rendszert, amely szervesen illeszkedik az ország védelmi rendszerébe, és amelynek hivatásos (BM OKF és alárendelt szervei, és nem hivatásos ága (védelmi igazgatási szervek, civil szervezetek, állampolgárok, gazdálkodók, MH és alakulatai stb.) van.

A kutatás „terv-végrehajtáson” alapuló munka, azaz előre rögzített terv alapján az elővizsgálat, az adatgyűjtés, az adatfeldolgozás- és adatelemzés menetén haladt, de ötvöződött a „folyamat közben” alakuló kutatási formával, hiszen menet közben a nyert eredményeket figyelembe véve, ezekre alapozva tervezetem és végeztem a következő vizsgálati szakaszt.

Idődimenzió szerint koncentrikus, azaz közös középpontú kutatással végeztem el a felmerült kérdések vizsgálatát, majd egybevettem a különböző síkokon nyert eredményeket egymással. Az elemzéseket a standard tudományos elvek mentén, tudományos módszereket és technikákat alkalmazva végeztem el. A következtetések kialakításánál az „egy forrás nem forrás elvét” alkalmazva, több szemszögből is megvizsgáltam, és visszaellenőriztem az adott kérdést. A következtetésekre alapozott javaslatokat úgy foglaltam össze, hogy azok a további tudományos kutatásokban és a gyakorlati szakmai munkában a védelmi szervek állománya részére egyaránt használhatók a legyenek, valamint szükség esetén az oktatáshoz is megalapozott ismereteket tartalmazzanak.

A BIZTONSÁGOT VESZÉLYEZTETŐ TÉNYEZŐK MEGJELENÉSE A HAZAI TUDOMÁNYOS KUTATÁSOKBAN ÉS IRODALMAKBAN

A körülöttünk lévő veszélyek azonosítása, természetük, jellemzőik feltérképezése mindig is alapját és feltételét képezte a hatékony védelmi munkának. A biztonságpolitikai és védelmi szakmódszertani írások tartalma, a vizsgálódások célja, iránya, módszerei nagyban függtek az adott korszak politikai, társadalmi, gazdasági tendenciáitól, az aktuális rendkívüli eseményektől is, és többnyire kevés teret adtak az ezektől eltérő gondolkodásnak. Minden időszak- és rendszer hatással volt az adott kutatásokra, és az azok eredményeit bemutató írásokra. Mások voltak a prioritások a hidegháború idején, a rendszerváltás előtti- és körüli időszakban, amikor viszonylagos állandóság volt érzékelhető a megközelítés és a jelenségek értelmezése tekintetében, így egymástól nem nagyon tértek el az elemzések. A felgyorsult fejlődés és a kilencvenes évek változásai miatt, a múlt század biztonsági elemzései idejétmúlttá, hiányossá vagy aktualizálandóvá váltak, új elgondolások születtek. Felmerül a kérdés, hogy mit tükröznek a rendszerváltást követő biztonságpolitikai és védelem-szempontú szakmai írások. Hogyan jelennek meg bennük a veszélyeztető tényezők, és milyen prognózist lehet adni ezek alapján a közeljövő veszélyeire?

Az elmúlt időszak új biztonsági környezetének kialakulása, a veszélyeztető tényezők számának, jellegének változása, valamint a hazai védelmi szféra intézményeiben és feladatrendszerében a századforduló után bekövetkezett rapid és átfogó változások indokolttá tették a biztonság újra-értelmezését, a veszélyeztető tényezők korszerű elvek mentén való elemzését, és a kihívásokra adott válaszok vizsgálatát. Ez a helyzet nagy hatással volt a kutatásokra és a kutatókra is. Állami, önkormányzati és civil szervezetek, oktatási intézmények és kutatóhelyek egyaránt elkezdtek foglalkozni a biztonsággal és annak értelmezésével, az ellene ható tényezők és a szükséges védelmi képességek vizsgálatával, és mind a szakpolitikai, mind a szakmamódszertani kiadványokban, mind pedig az adekvát tudományos vizsgálatokat bemutató fórumokon közzétették az eredményeiket. Ennek eredményeként igen nagyszámú irodalom készült.[3]

[3] Az új elméletek kialakításánál eleinte „csak” szakfordításokkal (sajnos közöttük kevésbé jól sikerültekkel is) találkozhattunk, majd megjelentek a hazai viszonyokat az új felfogásokkal összevető, kreatív megközelítésű írások.

A század végén és a 2000. után keletkező, általam vizsgált irodalmak túlnyomó része olyan témákat elemez, amelyek aktuálisak voltak az adott időszakban, és azok napjainkban is, és a kutatásukra régen várt a védelmi szakterület. Ha röviden akarjuk jellemezni őket, elmondható, hogy ezek a hiánypótló írások tartalmukban és formájukban is alapjául szolgálhatnak a témával kapcsolatos további kutatásoknak, a jogszabályalkotók munkájának, de bennük összefoglalt ismeretanyag a közszféra ezirányú munkájának átgondolásában is nagy segítséget nyújthat. A nagyszámú irodalom feldolgozásából a következő áttekintésben csak arra vállalkozhattam, hogy a főbb csoportokat, és azokból egy-egy neves, vagy a témám szempontjából fontos területet vizsgáló kutató, szerző művéből emelek ki olyan kulcsgondolatokat, amelyekre a további elemzések épülhetnek.

A témával foglalkozó újabb, és már *átfogó megközelítéssel íródott* irodalmakat áttekintve megállapítható, hogy *az egyik nagy csoportot* a biztonság-fogalmat értelmező, a biztonsági tanulmányok tendenciáit, és a klasszikus és új veszélyek meghatározását vizsgáló kutatások, valamint az azok eredményét összefoglaló biztonságpolitikai szemszögből készült publikációk, könyvek, egyetemi jegyzetek adják. *A századelő témával kapcsolatos, több további műnek kiinduló alapot jelentő, már az új szemléletmód „csíráit" magán viselő elemzés Kőszegvári Tibor* nevéhez fűződik. „A nemzetközi biztonságot fenyegető új kihívások és kockázatok" című írásával. [2] *Bognár Károly*, „a háború fogalmának, tartalmának múltja, jelene és jövője" c. útkereső írása is messzire tekint a témában. [3].
Sok szempontból átfogó képet ad Európa, Ázsia és Afrika országai tekintetében a biztonságpolitikai kockázatokról és dilemmákról, a biztonságpolitikai stratégiákban megfogalmazott értékekről, és a veszélyeztető tényezőkről *Koós Anna* és 18 szerzőtársa a munkája, amely biztonságpolitikai prognózist is nyújt a vizsgált országok és Magyarország tekintetében. A szerzők a világ válságterületeihez fűződő viszonyunkat, és a missziós tevékenységünk tendenciáit is áttekintették. [4]

Gazdag Ferenc „A Biztonsági tanulmányok alapjai" c. művében a biztonság kérdéskörét vizsgálja, és bemutatja a biztonsági tanulmányok tudományterület alapvető kérdéseit, változásait. Elemzi az új szemléletű biztonság-értelmezéseket, és elvégzi a biztonság ellen ható veszélyeztető tényezők csoportosítását, bemutatja azok különböző osztályzását, valamint vizsgálja a védelem kérdéskörét is. Ismerteti napjaink védelempolitikai törekvéseit, valamint bizonyítja az átfogó biztonságfelfogás-megközelítés szükségességét. A biztonságot fenyegető tényezőket a szerző az államok, és nem az egyén biztonsága szempontjából vizsgálja. Fokozat és intenzitás alapján 5 kategóriába sorolja azokat: a kihívások vagy kockázatok, feszültségek vagy fenyegetések, a válság, a konfliktus és a háború. [5; 34-37. o.]

Csiki Tamás és *Tálas Péter a Biztonsági tanulmányok alapjai* c. kötet társszerzőiként a nemzetközi biztonsági környezet alakulását, a veszélyeztető tényezőket, a bipoláris korból adódó, konkrét szektorális és globalizációs kihívásokat elemzik. Külön felhívják a figyelmet az állami, kormányzati rendszereket, a gazdasági folyamatokat és a természeti és épített környezet összetevőit fenyegető veszélyekre, és azok természetének megváltozására. [6; 115-136. o.]

Az elemzések másik csoportja egy-egy veszélyeztető tényezővel és annak természetével foglalkozik mélyrehatóan. *Sokan kutatták tudományos igénnyel a tanulmányok írói közül a legnagyobb intenzitású veszély, a háború különböző értelmezését mind a hazai, mind a külföldi irodalmakban. Nem érdemtelen Samuel Huntington nevét említeni, akinek a műve a további kutatók „Bibliája"-ként szolgált, és aki már nem a nemzetállamok, mind inkább*a civilizációk összecsapását prognosztizálta, és rámutatott arra, hogy a hagyományos háborúk korszaka lejárt.[7] hatása ma is érezhető a kutatókra.

Szenes Zoltán a Katonai kihívások a 21. század elején c. cikkében a hadviselési módok változásait vizsgálta, és a háború „jövőképét" a 21. században. Elemzéseiben a nemzetközi biztonság jellemzőinek átfogó értelmezésén túl, a katonai elméletek fejlődését is bemutatja. Rámutat arra, hogy a kihívások tükrében az államközpontú védelmi szisztéma mellett, az államszint alatti, és államok felett átnyúló biztonsági formák megjelenése törvényszerű és szükségszerű. Bemutatja az új megjelenő fogalmakat, mint a modern, a posztmodern és a premodern háború, valamint a hadügyi forradalom gondolatkört. A témánk szempontjából figyelemre méltó része a cikknek az 1990-es évektől megjelenő új katonai elméletek bemutatása, melyek mindegyike hangsúlyozza a hagyományos háborúforma háttérbe szorulását, és az aszimmetrikus hadviselés, többvariációs háború, multinacionális katonai műveletek stb. formákra kell készülni. [8]

Az irodalmak jól vázolják, hogy a hadviselés megváltozásával annak hatásai is változnak, másként, és másfajta károkat okoznak, de a békeidőszaki veszélyek (katasztrófák) is megszaporodtak, így a felkészülést, valamint a háborús és/vagy katasztrófa-kárterületen a lakosság és az anyagi javak védelmére vonatkozó tevékenységeket is más elvek mentén, és más módszerekkel kell végezni, mint korábban, mely gondolatkörre a cikk második felében térek ki.

Az elemzések *következő csoportját* a veszélyeztető tényezők, és azok lehetséges következményeit, valamint konkrét megjelenési formáit vizsgáló írások képezik. Ezek már az átfogó biztonság-értelmezést követve, annak komplexitását és a szektoralitást hangsúlyozzák. Megközelítésük eltérő ugyan, de elemzéseik főként arra fókuszálnak, hogy a demográfiai problémák, a migráció, az élelmiszerhiány, a természete környezet pusztítása, az édesvíz-szűkösség, az urbanizáció és a nemzetközi terrorizmus hogyan veszélyeztetik a biztonságot, és milyen következményeik várhatóak. [9] A kutatások a legtöbb esetben kitérnek a veszélyek rendkívüli eseménnyé válásához vezető okokra, folyamatokra, a következményekre és a védekezés lehetőségeire. Jól látható az irodalmakban az a tendencia, hogy a nemzetközi események[4] hatására időről-időre újra előtérbe kerülnek az aktuális eseményekkel, így a terror-támadások kapcsán például, a migrációval és a terrorizmussal összefüggő kutatások és elemzések.

Endresz Ernő a nemzetközi terrorizmus sajátosságai című tanulmányában a terrorizmus fogalmát értelmezi, vizsgálja a fajtáit, és az ellene való küzdelem típusait. Magyarország érintettségét elemezve megállapítja, hogy hazánk nem tartozik a terrorizmus elsődleges célországai közé. [10; 87. o.]

Marján Attila és szerzőtársai az EU és Magyarország helyzetét vizsgálják a globális erőtérben, és a körülöttünk zajló események tendenciáit. Felteszik a kérdést, hogy vajon a jövőben alkalmazza-e az EU a harccsoportjait gyors és hatékony intervenciós beavatkozásokra, vagy megmarad a jelenlegi alkalmi haderő-felállítási politikánál. Rámutatnak, hogy az elmúlt időszak hibái, késedelmes vagy téves döntései veszélyeztethetik az egyébként „törékeny biztonságot". A szerzők célszerűnek látják, hogy az államok és az EU „stratégiai képességeket (hírszerzés, szállítóképesség, mobil erők, önálló logisztika, kiberbiztonság, határvédelem, tengeri biztonság) fejlesszenek. [11; 10. o.]

[4]londoni, madridi terrortámadások, a természeti katasztrófák, a környezetszennyezések stb.

*Simicskó István „*A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével" című cikkében a terrorizmus elleni fellépés különleges jogrendi kereteit vázolja illetve a terrorizmus elleni fellépés összetett feladatrendszerét elemzi. [50; 2. o.]

Padányi József kutatásában ötvözte két terület, az éghajlatváltozás és a haderő kérdéskörét, és bemutatta, hogyan járulhatnak hozzá a negatív környezeti hatások megakadályozásához a hadseregek. Elemezte, hogy hogyan hat az éghajlatváltozás a különböző országok haderőire, és azok (köztük a Magyar Honvédség is) miként tudnak részt venni a klímaváltozás okozta helyzetek megelőzésében és megoldásában. Megállapította, hogy a jövőbeni kutatásoknak arra kell irányulniuk, hogy hogyan tehetjük a katonákat leginkább képessé az éghajlatváltozás okozta helyzetekhez való alkalmazkodásra [12], [48].

A témával kapcsolatos irodalmak *következő kategóriáját* a szakpolitikai és szakmódszertani írások jelentik, amelyek többnyire a kihívásokra válaszként működtetett védelmi szektor felépítésével, változási tendenciáival, és a velük szemben megfogalmazott elvárásokkal foglalkoznak, vagy egy konkrét esemény tapasztalatai kapcsán a működésükre, módszereikre vonatkozóan javaslatokat tesznek a reformokra. A kutatások konzekvensen vizsgálják a katonai védelmi honvédelmi rendszert, és a katonai feladatok rendszerét is, de egy jelentős részük pedig a kihívások közül főként a katasztrófákra fókuszál, elemzi azok kialakulását, okait, következményeit, és a megelőzés lehetőségeit. *Földi László és Halász László* a Katasztrófavédelem c. könyvükben a katasztrófák tipizálását adták meg, és a hatás-mechanizmusukat is elemezték. [13]

Popelyák Pál és Kátai-Urbán Lajos az ipari balesetekkel kapcsolatos helyzeteket, és az elkerülés lehetőségeit vizsgálták, kiemelve a veszélyhelyzeti tervezés jelentőségét. [14] *Endrődi István* a Katasztrófa-elhárításra felkészítő ismeretek c. írásában a katasztrófák bemutatása mellett, a lakosság felkészítéséhez ad hasznos információkat. [15] *Veres Viktória* és szerzőtársa a biztonságpolitikai és a katasztrófavédelmi szakma-módszertani ismereteket ötvözve elemezték és mutatták ki a katasztrófák, a biztonság és a sebezhetőség összefüggéseit. [16]

A védelemmel összefüggő szakmódszertani tudományos irodalmak a rendkívüli események következtében kialakult helyzetek felszámolását célzó rendszerek kialakítására, működésére, azok alrendszereinek összetevőire, és a következmények felszámolásának, a károk mérséklésének hatékony formáira megoldásokat is javasolnak. *Vágvölgyi Zoltán* például egy konkrét katasztrófa hatását, és a kárelhárítási folyamatot vizsgálva mutatja be a lehetséges és szükséges kárhelyszíni teendőket. [17] *Tóth Rudolf* „A repülőeszközök alkalmazásának lehetséges területei és korlátai" c. munkájában a kárterület és a kárelhárítás új értelmezését és a légijárművek katasztrófák következményei felszámolásába való bevonása lehetőségeit vizsgálja. [18] *Hornyacsek Júlia* egy hazai egyetemtűz esetéből kiindulva kezdte kutatni a felsőoktatási intézmények veszélyeztető tényezőit, a biztonságos működtetés feltételeit, és javaslatot tett a veszélyek elkerülésének módjaira, és az intézményi veszélyhelyzeti tervezés módszereire. [19] A kritikus infrastruktúra kérdéskörben is számos elemzés készült.

A kutatási tendenciákat vizsgálva megállapítható, hogy a biztonságpolitikai elemzések és kutatási eredmények széleskörű terjedésével szükségszerűen jutottak el a kutatók ahhoz, hogy a jelenlegi védelmi rendszerre, annak alrendszereire jellemző folyamatokat is elemezni kezdjék.

Szenes Zoltán a magyar hadügyi forradalom jellemzőit, valamint kutatás-fejlesztés helyzetét vizsgálta a védelmi szektorban a haderő szemszögéből, és hangsúlyozza, hogy „A modern haderőkben is meghatározó szerepet kap a tudás és technikai felkészültség, a korszerű oktatás és kiképzés, a civil és katonai szakterületek együttműködése". [20; 201. o.]

A szerző „A védelemgazdaság problémái Magyarországon" c. cikkében pedig a védelemgazdaság elmúlt időszaki változásaival, lehetséges útjaival foglalkozik, és vizsgálatai alapján javaslatot tesz a hiányzó területek megoldására, és egy komplex ország védelmi stratégia kidolgozására. [21]

Muhoray Árpád a katasztrófavédelem átalakulási folyamatát elemezve, áttekintést ad a magyar katasztrófavédelem elmúlt időszakban történt változásairól, szervezet-, feladat- és irányítási rendszere korszerűsítésének fontosabb mozzanatairól, aktuális feladatairól, jövőképéről. [22]

Felházi Sándor és Ruszin Romulusz az összfegyvernemi erők tűztámogatásának kérdéseit kutatva, a tüzér fegyvernem alrendszereit, és azok alkalmazásának lehetőségeit elemezték, és eredményeikkel a professzionális haderő kialakításához kívántak hozzájárulni. Célszerűnek vélik a fegyvernemi és harci támogató kötelékek multifunkcionalitását kihasználni, a még meglévő képességekre építeni, és ennek megfelelően kialakítani a közép- és hosszú távú terveket. [23]

Tálas Péter, elemezve a „biztonságiasítás" (securitization) kérdését, a terrorveszély helyzetét az EU-ban, és arra a következtetésre jut, hogy „stratégiai" jellegű terrortámadásokra – mely véleménye szerint nem stratégiai mértékű károkozást jelent –, hazánkban nem kell számítunk, hanem a terrorfenyegetettség mértékében kell látnunk a veszélyt, azaz a növekvő tendenciát. A szerző rámutat, hogy „a társadalmak az úgynevezett biztonsági helyzetekben (vagyis akkor, amikor valamit fenyegetésként értelmeznek és élnek meg), mindig a végrehajtó hatalom, vagyis a kormányok felé fordulnak, tőlük várják a megoldást, s ehhez általában megadják a bizalmat is. [24; 41-43. o.].

Hornyacsek Júlia két konkrét külföldi katasztrófa (Katrina hurrikán, Fukushima földrengés) tapasztalatainak feldolgozásáról írt cikkében is javaslatot tett a hazai lakosságvédelem újszerű értelmezésére, új felosztására, feladatainak hatékony megoldására.[25], [26]

A téma adekvát irodalmak *egy másik nagy csoportját* a biztonság szektorális értelmezését továbbvivő szerzők munkái (*Haig Zsolt, Munk Sándor, Felner Rita* at al) és elemzései adják. Egy újabb biztonságdimenzió megjelenését hangsúlyozva vizsgálják az új veszélyeket, elemzik például az információbiztonság és a kiberbiztonság aktuális kérdéseit. Kiemelik, hogy mivel az infokommunikációs rendszerek ellen irányuló támadások száma növekszik, a támadók módszerei változnak, és a károk egyre nagyobb mértéket öltenek mind a magán, mind a civil szférában, ezért a védelmi rendszernek erre is fel kell készülnie. [27],[28] A szerzők nagy százaléka igyekszik megoldási javaslatokat is adni az általa vizsgált problémakörhöz.

Kovács László és Krasznay Csaba empirikus kutatásukat összefoglaló cikkükben következtetésként azt hangsúlyozzák, hogy „a védelem területén egy átfogó – a kritikus információs infrastruktúrák komplex védelmére vonatkozó– védelmi stratégia kidolgozása az első lépés, amelyet meg kell tenni". [29]

Az irodalmak elemzésénél jól érzékelhető, hogy a katasztrófák vonatkozásában nem egyértelmű a megközelítés. Egyes esetekben a kutatók vagy a szakemberek azokat *veszélyeztető tényezőként*, más esetekben a veszélyeztető tényezők következményeként, azaz

hatásként fogják fel. Ezen túlmenően, a katasztrófák típusainak megnevezése, az egyes típusokhoz tartozó események azonosítása sem egységes. Vannak megfogalmazások, amelyek például a katasztrófák közé sorolnak, olyan eseményeket, jelenségeket, amelyek önmagukban nem azok, de jellegüknél fogva katasztrófához vezethetnek migráció, terrorizmus stb.).

Ebben a kutatásban a katasztrófákat önálló veszélyeztető tényezőként értelmezem, amelyeknek hatására különböző kárterületek alakulnak ki.

A fent bemutatott kutatók egyöntetűen megfogalmazták, hogy a jövőben sem csökkennek az ország és a lakosság biztonságára ható negatív események, és a jellegük, intenzitásuk, valamint a következményeik különbözősége miatt, más-más felkészülést igényelnek. Ez magával hozza és feltételezi a közszolgálati hivatásrendek átalakítását is a védelem vonatkozásában. Az is megállapítható a kutatások eredményeiből, hogy bár a civil szférának nagyobb szerepet kell vállalnia a veszélyek elhárításában, de a jövőben sem csökkenhet az állam és a közszféra felelőssége a rendkívüli helyzetek megelőzése és a következményeik felszámolása területén. Az elmúlt időszakban kialakult reform-elképzelések a *jó állam, jó kormányzás, jó közigazgatás* kialakítását célzó koncepcióban jelennek meg, amely minden területen aktívan fellépő, cselekvőképes államot céloz meg. Ennek részét képezik a védelmi igazgatás és annak alrendszerei, mint a honvédelmi- és a katasztrófavédelmi igazgatás elemei, amelyek az elmúlt időszakban jelentős átalakuláson mentek át annak érdekében, hogy a lakosság és az anyagi javak védelme minél magasabb színvonalon történhessen. Összecseng ezekkel a törekvésekkel és a kutatásokban bemutatott eredményekkel *„A jó állam jelentés 2015.”,* amely öt dimenzióban méri a kormányzati képesség és tevékenység folyamatait, eredményét és hatását a biztonság és a bizalom témájában. A „Biztonság és bizalom a kormányzatban” területhez sorolja a veszélyek elleni védekezés fő pillérét a rendvédelmet és a katasztrófavédelmi képességet is, „amely a természeti vagy ipari káreseményekkel szembeni védettséget biztosítja”. A közbiztonság területben jelenik meg a kormányzati törekvés és képesség arra, hogy a lakosságot veszélyeztető vagy sértő jelenségeket megelőzze, feltárja és megbüntetesse.[30] A „képességek” nevesítése a témában újabb irányt szab a kutatásoknak és a védelem-szakmai törekvéseknek, de a védelmi rendszer kialakítását célzó szabályzásoknak is.

Végül, de nem utolsó sorban, rá kell mutatnunk arra, hogy a Hadtudományi Kollégium szerzői közössége által meghatározott, hadtudományi stratégiai kutatási irányok között is kiemelt figyelmet kapnak a katasztrófák elleni védekezés elméleti és gyakorlati kérdései. [49]

A LAKOSSÁG BIZTONSÁGÁT VESZÉLYEZTETŐ KATASZTRÓFÁK LEHETSÉGES FAJTÁI, ÉS BEKÖVETKEZÉSÜK PROGNÓZISA

A fenti és a további, itt nem elemzett irodalmak széles spektrumát vonultatják fel a veszélyeztető tényezőknek, melyek a lakosság életét és az anyagi javakat károsító eseményekhez vezethetnek. Megállapítható az is, hogy a tudományos vizsgálatok a veszélyek okait, lehetséges következményeit elemezve, elméleti síkon alapozzák meg a védelmi munkát, annak kereteit, elveit, módszereit.

A szakmai módszertani anyagok pedig többnyire a védekezés, mentés oldaláról vizsgálják ugyanezeket az eseményeket, az ezzel összefüggő jogszabály-elemzések pedig a szervezetek kialakítása, feltételek biztosítása és a tevékenységek szabályozása szempontjából. Ahhoz, hogy prognosztizálni tudjuk a várható katasztrófákat, javaslatot tudjunk tenni a következtükben kialakuló kárterületen végzendő feladatok körére, és az ott közreműködők együttműködésének legoptimálisabb formáira, a három kategóriát együtt kell vizsgálnunk, és

egy dimenzióba kell hoznunk, és a katasztrófákat veszélyeztető tényezőként és nem azok hatásaként tekintenünk. Milyen eszközök szolgálnak ehhez?

A konkrét veszélyeztető tényezők feltérképezésének, és az erre épülő védelmi rendszer kialakításának alapját napjainkban a tudományos kutatásokra és a szakpolitikai elemzésekre épülő biztonságpolitikai dokumentumok képzik.

Mint a 2004-ben, a rendszerváltozás után először kiadott, és a jelenleg hatályos, megfelelően aktualizált, 2012-ben kiadott Nemzeti Biztonsági Stratégia [31, 32], melyek meghatározták az alapvető értékeket, az ellenük ható veszélyeztető tényezőket, a biztonságpolitikai célokat, és a stratégia végrehajtásának eszközrendszerét. A 2004-es stratégia a veszélyeket az alábbi módon nevesítette és csoportosította:

- *Globális kihívások:* a terrorizmus, a tömegpusztító fegyverek terjedése, instabil régiók, az illegális migráció, gazdasági instabilitás, az információs társadalom kihívásai, a globális természeti, civilizációs és egészségügyi veszélyforrások.
- *Regionális kihívások* körét Európa, a FÁK országok, a mediterrán térség, a Közel-Kelet és a Közép-Kelet problémái adják.
- *Belső kihívások:* szervezett bűnözés, feketegazdaság korrupció, kábítószerek terjedése, politikai és vallási szélsőségek, demográfiai kihívások. [31]

Az itt lefektetett értékek, az értéket fenyegető veszélyek, valamint a biztonságpolitikai célkitűzéseink köre bővült ugyan a 2012-es stratégiában, de alapvetően nem változott. Új kategóriák is bekerültek a felsorolásba, mint a kiberbiztonság, energiabiztonság, a globális környezet- és éghajlatváltozás, a környezet védelme a fenntarthatóság ellen ható tényezőktől, valamint erősebb hangsúlyt kapott a migráció, és a természeti és ipari katasztrófák köre. [32; III/27., 33., 35. pont]. A katasztrófákat a stratégia tehát veszélyeztető tényezőként értelmezte, és a kihívások közé sorolta. A dokumentumokban nevesített veszélyeztető tényezők mindegyikére ez a kutatás nem térhet ki, ezért a katasztrófákra, és azoknak a különleges jogrendi kategória, a veszélyhelyzet[5] kihirdetését előidéző eseteire fókuszál.

A biztonsági stratégiákkal összhangban készült szabályzó, a katasztrófavédelmi törvény [33] szerint katasztrófák kialakulásakor az alábbi esetekben lehet és kell veszélyhelyzetet kihirdetni:

„a) elemi csapások, természeti eredetű veszélyek, különösen:

aa) árvízvédekezés során, ha az előrejelzések szerint az áradó víz az addig észlelt legmagasabb vízállást megközelíti és további jelentős áradás várható, vagy elháríthatatlan jégtorlasz keletkezett, vagy töltésszakadás veszélye fenyeget,

ab) belvízvédekezés során, ha a belvíz lakott területeket, ipartelepeket, fő közlekedési utakat, vasutakat veszélyeztet és a veszélyeztetés olyan mértékű, hogy a kár megelőzése, az újabb elöntések elhárítása meghaladja az erre rendelt szervezetek védekezési lehetőségeit,

ac) több napon keresztül tartó kiterjedő, folyamatos, intenzív, megmaradó hóesés vagy hófúvás,

[5] A különleges jogrendi kategóriákat az Alaptörvényben fogalmazták meg, az alkalmazandó részletes szabályokat sarkalatos törvény (2011. évi CXIII. tv. 1-38. § (6), 39. § VII-IX. fejezet, 80-81. §, 84. §).

ad) más szélsőséges időjárás következtében az emberek életét, anyagi javait a lakosság alapvető ellátását veszélyeztető helyzet következik be,
ae) földtani veszélyforrások.

b) ipari szerencsétlenség, civilizációs eredetű veszélyek, különösen:

ba) a veszélyes anyagokkal és hulladékokkal történő tevékenység során a szabadba kerülő anyag az emberi életet, egészséget, továbbá a környezetet tömeges méretekben és súlyosan veszélyezteti,
bb) nem tervezett radioaktív kiszóródás és egyéb sugárterhelés, amely a biztonságot kedvezőtlenül befolyásolja és a lakosság nem tervezett sugárterhelését idézi elő.

c) egyéb eredetű veszélyek, különösen:

ca) tömeges megbetegedést okozó humánjárvány vagy járványveszély, valamint állatjárvány,
cb) ivóvíz célú vízkivétellel érintett felszíni és felszín alatti vizek havária-szerű szennyezése,
cc) bármely okból létrejövő olyan mértékű légszennyezettség, amely a külön jogszabályban meghatározott riasztási küszöbértéket meghaladja,
cd) a kritikus infrastruktúrák olyan mértékű működési zavara, melynek következtében a lakosság alapvető ellátása több napon keresztül, vagy több megyét érintően akadályozott." [33; 44.§]

A felsorolásból látható, hogy ezek az események, jelenségek olyan mértéket érhetnek el, hogy olyan hatással vannak a lakosság életére, hogy az ellenük való védekezés meghaladhatja az erre rendelt szervezetek normál időszaki működését, és más szervezetekkel való közös munkát, azaz különleges jogrend bevezetését igényli. Ezekkel a tényezőkkel tehát feltétlenül számolnunk kell a jövőben. Ez a csoportba sorolás és leírás alapja lehet a hazánkban bekövetkezhető katasztrófák meghatározásnak, valamint a bekövetkezés valószínűsége meghatározásának (prognózis) is, de nem elegendő. A várható konkrét katasztrófatípusok nevesítésénél célszerű a nemzeti kockázatértékeléseket és az azokból készült jelentéseket is figyelembe venni. [34, 35]

A katasztrófák bekövetkezése valószínűségét vizsgáló kockázatelemzési anyagok

Az első, ún. *Nemzeti kockázat értékelés 2011.* c. összefoglaló a biztonság ellen ható tényezők között 7 kockázat típust jelöl meg, ezek az:

- ár- és belvíz,
- földrengés,
- erdőtüzek,
- ipari balesetek,
- a rendkívüli időjárás,
- iparbiztonsági jellegű katasztrófák,
- társadalmi eredetű veszélyek katasztrófák (tömegrendezvények, terror, migráció, demográfiai problémák stb.). [34]

Az elemzés erőssége, hogy a veszélyeztető kategóriák kialakítását és a prognózist adatokkal, vizsgálatokkal támasztották alá, beleértve ellenük való védettség helyzetét is, ezért valószínűleg ezekkel a jövőben is számolni kell. A megnevezett a jelenségek nem elméleti szinten, távoli lehetőségként fenyegetnek, hanem a mindennapjaink részét képezik, hiszen alig

telik el nap olyan sajnálatos hírek nélkül, mint a belvizek, árvizek, rendkívüli időjárás. Ezek következményei jelentősen kihatnak az ország életére, a termelésre, a gazdaságra egyaránt.

A témához kapcsolódó jogszabályokat elemezve megállapítható, hogy az állam és az önkormányzatok a szabályozások eszközével is igyekeznek a felkészülést fokozni erre a veszélyre, és már a normál időszakban kialakítani azokat a védelmi képességeket, amelyek adott esetben hozzájárulnak a károk mérsékléséhez.

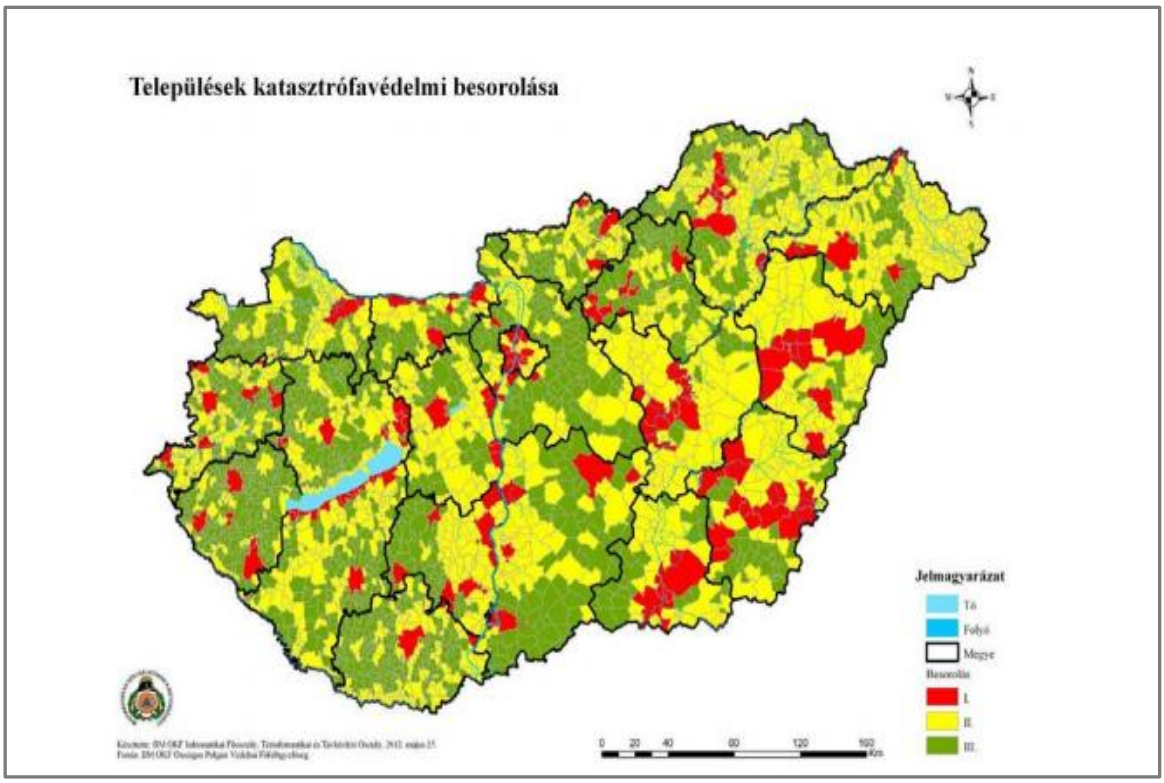
A kockázatértékelés és a vonatkozó jogszabályok alapján például a hazai települések katasztrófavédelmi sorolása is megtörtént, amelyet folyamatosan felülvizsgálnak. A kockázatalapú soroláskor 155 település I., 1325 II., 1696 település pedig III. sorolású lett. [34 b; 4. o.] A sorolásuk a lehetséges természeti veszélyektől, a területen folyó ipari tevékenységtől függ. Az alábbi 1. sz. ábrán jól látható, hogy szinte az egész ország területén soroltak a települések. A Tiszántúl jelentősen veszélyeztetett, és vannak olyan területek, ahol a veszélyeztető tényezők száma nagyobb, vannak, ahol jellegüknél fogva okozhatnak fennakadásokat. A védelmi képességek kiépítése és a védelmi rendszer működtetése ezeken a területeken komoly koordinációt igényel.

A Jelentés Magyarország kockázatértékelési módszertanáról és annak eredményeiről c. anyag háttere, hogy a veszélyekre való felkészülésben új irányt szabott – és egyben lehetővé teszi az egzaktabb katasztrófa-prognózist is – a kockázatkezelési-kockázatértékelési technikákról készült nemzetközi szabvány [IEC/FDIS31010:2009 (E)], melynek megfelelve, Magyarország az elmúlt időszakban alkalmazott nemzeti katasztrófa-kockázat értékelési gyakorlat alapján elkészített egy módszertani dokumentumot. A benne bemutatott módszerrel összegezte és nevesítette a valós kockázatokat, a várható veszélyeket is [35].[6] A dokumentum a veszélyeztető tényezőket és jellegüket tekintve, a természeti események, a súlyos balesetek, és a szándékosan előidézett események kategóriákba sorolja. Azonosítja az érdekek és értékek ellen ható veszélyeket, valamint az azokat kiváltó eseményeket, mint kockázati területeket. Ezek a következők:

- Szélsőséges időjárás
- Vizek kártételei
- Földtani kockázatok
- Járványok
- Űridőjárás
- Veszélyes anyagok
- Közlekedési baleset
- Nukleárisbaleset
- Terrorizmus
- Kibertámadás
- Biztonságpolitikai válság
- Energiaellátási válság. [35; 46-48. o.][7]

[6] A biztonságpolitikai eljárásrendeknek megfelelően meghatározták az alapvető érdekeket (emberi, gazdasági környezeti, politikai, társadalmi), és az ehhez köthető érdekeket és a hozzájuk kapcsolható értékeket. [35; 16. o.]

[7] Megjegyzendő, hogy a klasszikus biztonságpolitikai válságfogalom-felfogásban fokozati, intenzitásbeli szintet jelölt, itt önálló kockázatként szerepeltetik.



1. ábra A települések katasztrófavédelmi sorolása. Forrás: [34 b 5. o.]

A hatásokat nyolc csoportba sorolták, ezek a következők: haláleset, sérülések és betegség, tartós természeti és környezeti kár, pénzügyi és anyagi veszteségek, társadalmi zavargás, zavarok a mindennapi életben, az országos szintű kormányzóképesség gyengülése, területi igazgatás gyengülése. Ezekhez, mint elemi változókat, újabb lehetséges következményeket rendeltek, így a pénzügyi anyagi veszteségeknél például a vagyoni károkat, az egészségügyi károk költségeit, pénzügyi veszteségeket, és a káresemény elhárításának költségét nevesítették, majd hozzákötötték (A-E szintekbe sorolva) a hatások lehetséges mértékét besorolási szintként,[8] és így alakították ki az úgynevezett *aggregált hatásértékeket* mind a nyolc kategóriára.

A veszélyeztető hatások és a bekövetkezési valószínűség mértékének összegéből meghatározták az egyes kockázatok mértékét is, és a várható események jövőbeni bekövetkezési valószínűségét.[9] Ezen túlmenően, a veszélyhelyzetekre és a tényleges fenyegetettségre[10] vonatkozóan is megállapítottak kategóriákat, de a bizonytalansági tényezőket is figyelembe vették, majd 30 kockázati forgatókönyv készült. [11] [35; 24. o.]

A veszélyek előzetes azonosításának szükségességét érzékelik tehát a kutatók és a szakemberek is, ezért egyre több kutatásban is megjelennek a különböző veszély-elemzési

[8]Ezek: csekély mértékű, jelentős, súlyos, nagyon súlyos, katasztrofális mértékű következmények

[9] Az elemzéseknél a 10-es számrendszeren alapuló exponenciális értékfüggvényeket alkalmaztak, melyben az A, B, C, D és E szintek a 10 hatványaiként aránylanak egymáshoz, és az E értéke 10^4=10000, de normaként E=1 értéket vették alapul, azaz No = $0/10^4$=0; A = 10^0/10= 0,0001stb.[35; 25. o.]

[10] Mennyire valószínűsíthető a bekövetkezése, és van-e ráutaló jel?

[11] Kritériumai: vannak-e vonatkozó statisztikai adatok? Van-e ismert hibalehetőség, van-e releváns esetleírás?

módszerek. Cseh Gábor például kutatásában 51 féle elemzési formát mutat be az ipari kockázatelemzési szakterületen, és azok erősségeit, gyengeségeit is ismerteti. Kiemelten javasolja a technológiai kockázatok azonosítását, mert véleménye szerint ezek veszélyeztetik a biztonságunkat leginkább, és ezeknek nagy a valószínűsége a bekövetkezésre. [36; 77-79. o.]

A CIVPRO 0865R2 EU projekt a veszélyek és a károk megelőzését célozta meg, és keretében a kutatók bemutattak több további veszélyelemzési módot, amelyeket a szerint válogattak ki, hogy a településeknek a felkészüléshez mit célszerű alkalmazni. A veszélyek azonosítására a településeken a hibafa-elemzést, a hibamód- és hatáselemzést, a vezetési tévedés- és kockázatfa módszert, valamint a veszély és működőképesség vizsgálatot javasolják felhasználni. [37; 9. o.]

A kockázat-elemző módszerekkel az elmúlt években a meghatározott veszélyek nevesítése és csoportosítása is megtörtént, hiszen a védelmi rendszer kialakításához erre szükség volt. Az elemzéseket vizsgálva, itt is megállapítható, hogy a veszélyeztető tényezők nevesítése és csoportosítása nem egységes a különböző dokumentumokban. A Nemzeti Biztonsági Stratégiában megjelölt veszélyeztető tényezők hatásszintek szerint lettek csoportosítva, és ide sorolták a katasztrófákat is. A katasztrófavédelmi törvény a katasztrófák veszélyeztető tényezők, és a veszélyhelyzet kihirdetését előidéző katasztrófa-eseményeket a természeti és civilizációs, valamint egyéb eredetű veszélyek csoportjába sorolja. A nemzeti kockázat-értékelésekben [34, 35] megint más csoportokat találhatunk, de ezek már egymással összecsengnek. A „Biztonságpolitikai prognózis” 2005-ig c. tudományos elemzésben pedig látható, hogy a kutatók a biztonsági stratégiában megfogalmazott globális kihívásokat elfogadták, de a veszélyeket más csoportosításban ábrázolják. Magyarország biztonságára kockázatot jelentő tényezőként nevesítik például az alábbiakat:

- „az ország területén és környezetében előforduló ipari és természeti katasztrófák,
- környezetszennyezések, járványok;
- a kritikus infrastruktúra elleni támadások;
- az instabil országok belső feszültsége következtében kialakuló, a szervezett bűnözéssel összefonódó nagyobb méretű migráció és illegális kereskedelem;
- a térség egyes országaiban illegálisan, illetve ellenőrizetlenül tartott nagy mennyiségű fegyver, lőszer és robbanóanyag.” [4; 358. o.]

A 234/2011. (XI. 10.) Korm. rendelet is rendszerezi az ország lakosságára ható negatív tényezőket, közöttük a katasztrófákat is,[12] és 4 csoportra osztotta a katasztrófa-veszélyeket, ezek a következők:

- a természeti eredetű veszélyek (1. csoport);
- a civilizációs eredetű veszélyek (2. csoport),
- egyéb eredetű veszélyek (3. csoport),
- a kritikus infrastruktúrákkal kapcsolatos kockázati kategóriák (4. csoport). [38; 2. melléklet]

[12] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról.

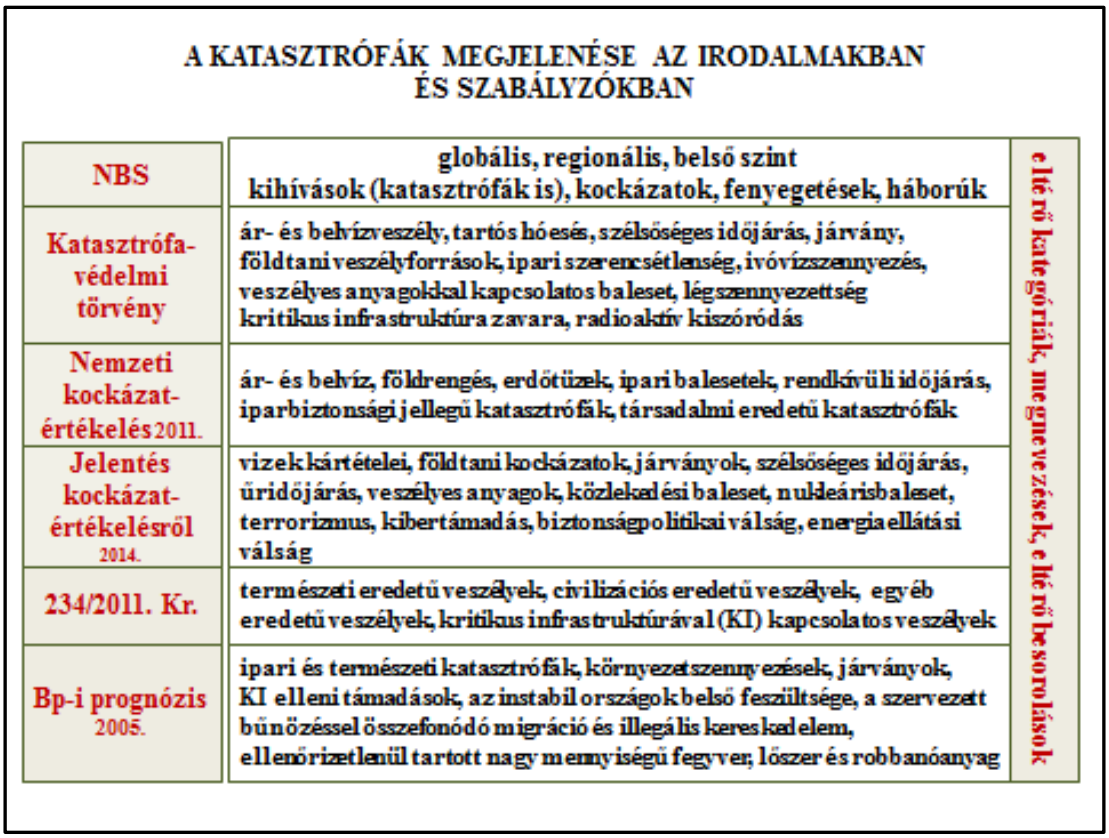
Az első csoportba az árvíz, a belvíz, a rendkívüli időjárás esetei, valamint a földtani veszélyforrások (földrengés, földcsuszamlás, beszakadás, talajsüllyedés, partfalomlás) kerültek.

A második csoportba sorolták a katasztrófavédelmi törvény IV. fejezetének hatálya alá tartozó üzemek kockázatain túl, a hatály alá nem tartozó, más létesítmény általi veszélyeztető hatást, valamint a veszélyes anyag szabadba kerülése esetét, továbbá a nukleáris létesítmény veszélyét. Ebbe a kategóriába került a területen lévő közlekedési csomópontok veszélye, valamint a katasztrófavédelmi törvény IV. fejezetének hatálya alá nem tartozó, katonai célból üzemeltetett veszélyes anyagokkal foglalkozó üzemek, és veszélyes anyagokkal foglalkozó más létesítmények megléte egy területen.

A harmadik csoportba, az egyéb eredetű veszélyek kategóriájába sorolták a felszíni és felszín alatti vizek szennyezését, azok sérülékenységét, a humán járványokat és az állatjárványokat. Új elemként szerepeltetik a riasztási küszöböt elérő mértékű légszennyezettséget.

A negyedik csoportba a lakosság alapvető ellátását biztosító infrastruktúrák, a közlekedés, valamint a közigazgatás és a lakosság ellátását közvetve biztosító infrastruktúrák sérülékenységét, és azokra ható veszélyeket sorolták. A jogszabályi tipizálás hasonló veszélyeket nevesít, mint az előző felsorolások, de más kontextusban.

Ahogy a 2. sz. ábrán is jól látható, az elnevezések, a csoportba-sorolások a különböző szabályzásokban és a szakmai dokumentumokban eltérőek. Emiatt a veszélyeztető tényezőkre való felkészülés irányainak kijelölése, illetve a szükséges védelmi képességek kialakításában a prioritások meghatározása hibalehetőségeket rejt magában. A fentiek alapján megállapítható, hogy a különböző szabályzók, kockázatelemzések eredményei a veszélyeztető tényezők tekintetében egyezést mutatnak a tudományos irodalmakban megjelenítettekkel, de azok megnevezése, csoportba-sorolása a szabályzók és a dokumentumok céljától függően eltérőek. Célszerű lenne egy egységes felsorolást és csoportba-sorolást kialakítani, és azt egységesen használni a védelmi szféra civil és hivatásos ágában egyaránt. Javasolt továbbá a veszélyeztető tényezők bekövetkezése prognózisánál elkészíteni és alkalmazni a gyakorisági térképeket, valamint a kialakulást befolyásoló tényezők mindegyikét figyelembe venni. Célszerű továbbá azokat statisztikai elemzésekkel kiegészíteni a helyi szintű terezésnél is, mint azt a korábban említett, 2011-es Nemzeti Katasztrófa kockázat értékelés c. kiadványban is láttuk [4].



2. ábra A katasztrófák megjelenése az irodalmakban és szabályzókban (Készítette: a szerző, forrás: [31, 33, 34, 35, 38, 4])

A katasztrófák várható bekövetkezésére vonatkozó prognózis

A várható katasztrófák típusára vonatkozó lehetséges prognózis a szabályzókban, szakmai anyagokban, kutatások leírásaiban megfogalmazottakon alapszik, de kialakítását segítheti a korábbi események, és az ezekről számot adó dokumentumok vizsgálata is. A nagyobb biztosító társaságok közzéteszik a világ katasztrófáiról szóló összegzéseiket, amely egyben a várható események meghatározásához is segíthet.

A müncheni legnagyobb biztosító, a Münich RE kutatási eredményei figyelemre méltóak. Ezek szerint a nagy jelentőségű, nagy kárt okozó természeti katasztrófák száma 2015-ben 1060 volt a világban. Ezek 42%-a a hidrológiai, 41%-a meteorológiai esetekből származott. Az összkár 100 milliárd US$-ra tehető, aminek a zöme, 47%-a meteorológiai eredetű volt. A halálozások (23 000 fő) többségét, 42%-át viszont a földrengések, földcsuszamlások okozták. [39 a] A világban történt természeti katasztrófákról készült térképen hazánk és a régiónk területére az áradások és a rendkívüli időjárás okozta események voltak főként jellemzőek, vélhetően ez a tendencia nem változik. [39 b] A bozót- és erdőtüzek vonatkozásában Közép-Európa országai, köztük hazánk is jelezve vannak a térképen, 2015-ben (április és augusztus között) ebben a térségben már 1800 millió USD kár keletkezett a természeti tüzekből. [39 c]

A katasztrófa-prognózis készítésénél figyelembe kell venni, hogy egy terület földrajzi jellemzői, iparszerkezete, a közlekedés, a településszerkezet jellemzői, az ellátórendszerek „veszélyekkel szembeni állékonysága," a területen folytatott mezőgazdasági tevékenység stb., mind potenciális veszélyforrások lehetnek, amit fokozhat, ha a lakosság nem kellően veszélytudatos, nem alakultak ki azok az önvédelmi reflexek, amellyel megelőzik, elkerülik a

károkozást. A veszélyek következtében kialakuló helyzetek súlyosságát befolyásolja a területen lévő infrastruktúra milyensége, a közlekedési csomópontok megléte, a védelmi rendszer szervezettsége és felkészültsége is. Ezeknek a feltérképezése, valamint a lakosság felkészítése kulcsfontosságú a megelőző időszaki feladatok sorában. A korábban lezajlott katasztrófa-események gyakorisági és intenzitásbeli mutatóit is szem előtt kell tartanunk.

A különböző szakmai anyagok, tankönyvek [40; 26-27] is felhívják a figyelmet arra, de a veszélyek kialakulását befolyásoló egyéb tényezők alakulása is bizonyítja, hogy hazánkban a természeti veszélyeztető tényezők közül az árvízre, a szélviharokra, tartós hidegre, fagyokra, belvízre, szél- és hóviharokra, jégesőkre, valamint a tartós szárazság okozta helyzetekre kell számítani. A civilizációs veszélyek közül pedig főként a veszélyes anyagok gyártása, tárolása, szállítása során keletkezett balesetek várhatóak, de nem zárható ki teljes biztonsággal egy atomerőművi baleset sem. Adott esetben a terrorcselekmények vagy a következtükben kialakult helyzetek is vezethetnek katasztrófákhoz.

Ha ezek a katasztrófák bekövetkeznek, akkor hatásukra kárterületek és ott károk alakulnak ki, amelyek csökkenthetők, ha a felkészülés időszakában megfelelő védelmi rendszert, védelmi képességeket és magatartási szabályokat alakítottunk ki, és a mentés időszakában összehangolt, hatékony feladat végrehajtásra kerül sor. Ezek csak az átfogó megközelítéssel kezelhetőek, amire a cikk befejező részében térek rá.

A szakterminológia bővülése: katasztrófavédelmi reagáló műveletek

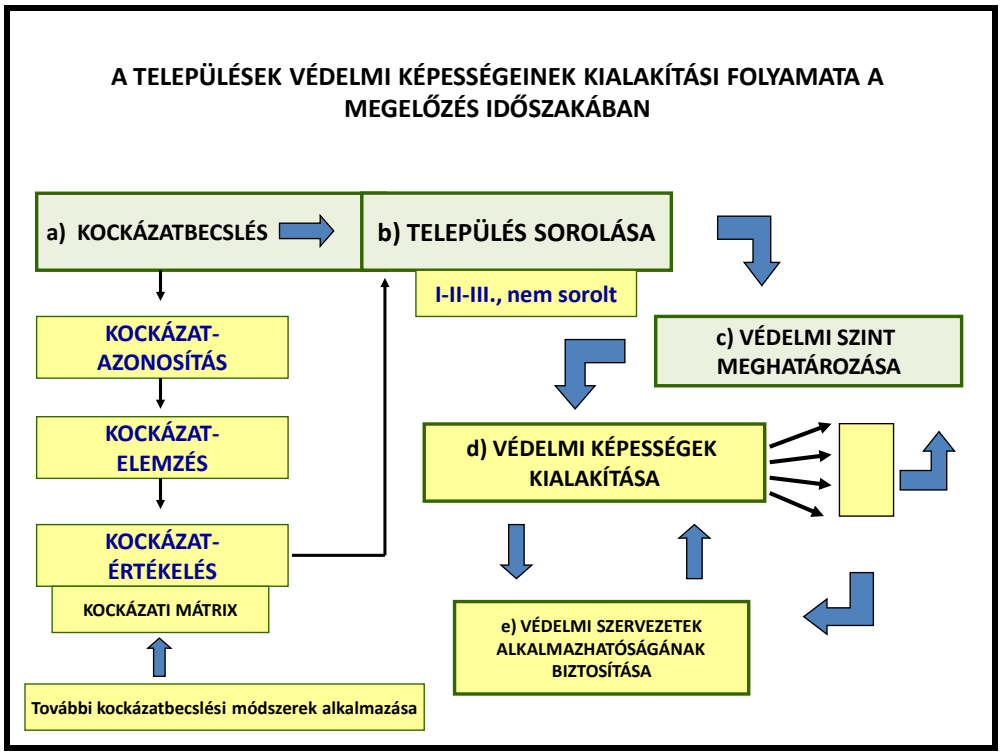
A kockázatok és várható következmények vizsgálata során a veszélyek elleni védelemben napjainkban új fogalom merült fel, a katonai feladatok ellátása kapcsán már ismert kifejezés, az ún. *reagáló műveletek*. Mára a fogalmat nemcsak a katonai jellegű cselekmények válasz-mechanizmusaként értelmezzük, hanem a többi veszélyeztető tényező kapcsán, így a katasztrófák elleni védelemben is felmerült. A biztonságunk érdekében az ellene ható veszélyek megelőzése, a következmények felszámolása és a helyreállítás érdekében az érintett szervek, szervezetek, hatóságok, szolgáltatók stb. katasztrófák esetén „reagálnak”, azaz terveznek, szerveznek, végrehajtanak feladatokat. Ezek a reagáló műveletek céljukat tekintve három nagy csoportot alkotnak (megelőzés, védekezés, helyreállítás), és további feladatokra oszthatóak.

A megelőzési célú reagáló műveletek célja a károk kialakulásnak megakadályozása, a védelmi képességeinek növelése és azoknak a feltételeknek a kialakítása, amelyek szükség esetén a védekezésben kellenek. *A védekezési időszaki reagáló műveletek* célja a gyors és hatékony beavatkozás végrehajtása, a mentési feladatok célirányos lebonyolítása és az eszkalálódás eredményes megakadályozása. *A helyreállítási célú reagáló műveletek* célja a károk teljes felszámolása, az élet feltételeinek kialakítása és biztosítása, a kárterület teljes rehabilitálása.

Mindhárom csoport fontos, de egyre inkább előtérbe kerül a veszélyekre való felkészülés, azaz a megelőzés-célú reagálás, hiszen a bajok megelőzése sokkal egyszerűbb, mint a már kialakult helyzet kezelése. Hozzá tartozik a felkészülés a veszélyek elleni védekezésre, a megelőző műszaki védelem, a jogszabályi háttér kialakítása, a védelmi képességek kiépítése stb.

A megelőzési célú reagálás, mint feladat és tevékenység, országos, megyei, helyi és települési szinteken egyaránt folyik. A katasztrófák szempontjából a legérintettebb a

települési szint, ezért a településeken végzett megelőzés-célú reagáló műveletek célja, hogy olyan feladatok kerüljenek végrehajtásra, amelyek biztosítják a település szükséges védelmi szintjének elérését. A folyamat a települések kockázatbecslésen alapuló veszélyességi besorolásával kezdődik, amit az erre épülő védelmi szint meghatározása, majd a szükséges védelmi képességek kialakítása követ. Mivel „a puding próbája az evés", a védelmi képességek is akkor megfelelőek és hasznosak, ha a védelmi szervezetek alkalmazhatóságát biztosítják. Lásd. 3. sz. ábra.



3. ábra A települések védelmi képességeinek kialakítási folyamata a megelőzés időszakában. (Készítette a szerző)

A védekezési és a helyreállítási célú reagáló feladatok alapjában véve a kialakult kárterületi jellemzőktől függnek. Vizsgáljuk meg ezeket!

A KATASZTRÓFÁK KÖVETKEZMÉNYEKÉNT KIALAKULT KÁRTERÜLETEK, ÉS AZOK JELLEMZŐI

A katasztrófák okozta kárterületek különböző típusúak, és az ott végrehajtandó feladatok szerteágazóak, így eltérő módon hatnak a környezetre, a társadalomra és az egyes emberre is. Annak eldöntésénél, hogy milyen következményekkel számolhatunk, és azok hogyan jelennek meg, több kutató is foglalkozott.[13]

[13] Nikodém Edit kutatásában például kimutatta, hogy hazánkban egy adott idő-intervallumban, 1980-2010 között a katasztrófa- események száma nem volt jelentős, ugyanakkor az érintettek száma (181 000) és a halálos áldozatok (716) száma, valamint a gazdasági károk mértéke (1793 millió USD) igen, és ez a következmények mérséklése szempontjából nem elhanyagolható, hiszen a védelmi erők fejlesztésénél és a felkészítésénél ezt is figyelembe kell venni. [41; 59. o.]

Mivel az elmúlt időszakban a kutatások nagy része, az okokból kiindulva, és típusonként mutatta be a katasztrófákat, illetve a társadalomra kifejtett általános hatásuk szemszögéből, jelen alfejezetben a kialakult *kárterületi jellemzők alapján, valamint az ott végrehajtandó feladatok jellege szerint* vizsgálom azokat.

A katasztrófa-kárterület fogalma, fajtái és alapvető jellemzői

A kárterület fogalma a polgári védelmi feladatok ellátásával kapcsolatban került a védelmi szakterminológiába. Több meghatározása van, az egyértelműség érdekében az alábbi értelmezésben használom:

Kárterületen azt a területet értjük, ahol az adott esemény bekövetkeztetett, és/vagy a veszélyeztető hatása érvényesül, és ahol a mentést, valamint a következmények felszámolását, illetve szükség esetén korlátozó intézkedéseket végezni kell.[14]

A veszélyt okozó katasztrófa típusa alapján a kárterület biológiai, nukleáris, hidrológiai, meteorológiai, földrengés okozta stb. lehet. Gyakran találkozunk ezek kombinációjával. A kárterületet alapvető jellemzői a következők:

- a kiterjedése, mérete,
- a kialakult helyzet bonyolultsága,
- az élőerők vesztesége és a fellépő károsodásuk mértéke,
- a környezet károsodása,
- a végrehajtandó feladatok összetettsége, kapcsolódása, végrehajtási sorrendje.

Kiterjedés szempontjából lokális, regionális, országos és országhatáron átívelő kárterületről lehet beszélni. A bonyolultságát a földrajzi és beépítettség jellemzői, valamint a kárterületen kialakult hatások összetettsége, komplexitása adja. Az élőerők vesztesége szempontjából lehet olyan, ahol sok sérült, halott van, vagy a veszélyeztetettek száma nagy. A környezet károsodása szempontjából az épített és a természeti környezet rombolódását, pusztulását kell figyelembe venni (épületek, közművek rongálódása, az ökológia károsodása stb.). A végrehajtandó feladatok összetettségét az adja, hogy a mentőerőknek a kárterület jellegéből adódóan tűzvédelmi, műszaki, egészségügyi, vegyi védelmi vagy nukleáris, valamint lakoság-ellátási feladatokat kell végrehajtani.

A különböző katasztrófák esetleírásait vizsgálva[15] megállapítható, hogy a leggyakrabban biológiai és vegyi kárterületek alakulnak ki, de a legsúlyosabb következménye a nukleáris katasztrófáknak van. Ezek következtében összetett kárterületek alakulnak ki, ahol az elsődleges hatásokon túl, az eszkalálódás miatt, számolni kell a másodlagos hatásokkal is. [42; 2-3. o.]

A kárterületek bonyolultsága a vizsgált esetekben azt mutatta, hogy a mentés során a mentőerők olyan problémákkal is szembe találták magukat, amelyek nem tartoznak szorosan a szakmai feladataik közé, de azok végrehajtását alapvetően befolyásolják. Felléphet az

[14] A háború, mint a legnagyobb civilizációs katasztrófa kárterülete sajátos jellemzőkkel bír, attól függően, hogy a pusztítást milyen fegyverrel hozták létre: hagyományos vagy tömegpusztító fegyverrel. A fegyveres küzdelemnek másodlagos hatásaként területek vízelárasztása, közlekedési infrastruktúrák tönkretétele, tüzek alakulhatnak ki.

[15] Kolerajárvány 2010. Haiti, H5N1 madárinfluenza járvány USA, 2009., tiszai cianid és nehézfém szennyezés, 2000, Seveso katasztrófa 1976., Bophal vegyi baleset 1984., vörösiszap katasztrófa Kolontár-Devecser, 2010., Csernobil atomerőmű balesete 1986., Fukushima nukleáris baleset, 2011.

információ-áramlás zavara, negatív pszichés jelenségek, a mentőerők munka-hatékonyságának romlása, kapacitás-kimerülés stb.

Az épített környezet, utak hidak, épületek, átjárók stb. sérülése, rombolódása miatt járhatatlanná válhatnak bizonyos területek, és ez nehezítheti a mentést is. Számolni kell a közlekedés túlterheltségével, akadozásával, esetleg megszűnésével. Elhúzódó esetekben a közbiztonság zavara sem kizárt, és sok esetben az információhiány és váratlanság miatt a lakosok önmaguk okoznak további károkat. Előfordulhat, hogy a mentőerők kapacitás-vagy kommunikációs zavar miatt szakmailag hibás döntést hoznak, és ezzel „rontják" a károk mérséklésének lehetőségét. Az egészségügyi rendszer terhelése megnő, kapacitása kimerülhet. Az események következtében nőhet a fertőzések száma, ami járványok kialakulásához vezethet, és ez még jobban leterheli az egészségügyi rendszert, csökkenti a védekező erők számát is. Esetenként a szolgáltatások és az igazgatási feladatok ellátása is zavart szenved. A helyzet önmagát rontó folyamattá válhat.

A fentiek miatt, a mentés hatékony végrehajtása érdekében fontos ismerni a következmények felszámolását célzó folyamat elveit, kereteit, szereplőit", a kárterületi feladatokat, azok végrehajtásának folyamatát, és a megoldáshoz szükséges eszközöket. A következő fejezetben elemzem a kárterületen végrehajtandó feladatok fajtáit, és azok műszaki jellegét, sajátosságait.

A KÁRTERÜLETEN VÉGREHAJTANÓ MENTÉSI ÉS HELYREÁLLÍTÁSI FELADATOK, ÉS AZOK MŰSZAKI TARTALMA

A katasztrófák- okozta kárterületen végzendő feladatok végrehajtásának feltételeit már a megelőző időszakban ki kell alakítani, így a védekezés során a mentési és a helyreállítási feladatokkal kell számolni. A feladatokat a kárterület jellemzői és összetettsége határozzák meg, és több csoportba sorolhatóak. Lehetnek a polgári védelmi feladatok, mint például a lakosság kimenekítése vagy kitelepítése, lehetnek tűzvédelmi feladatok, mint például a tűzoltás, de lehetnek vegyi és nukleáris jellegű események felszámolását célzó feladatok, mint például a mentesítés, fertőtlenítés. Valamennyi tevékenységben vannak műszaki jellegű feladatok. A mentés során például szükség lehet romok alóli mentésre, vagy a kitelepítettek elhelyezését szolgáló épületek kialakítására, a tüzek oltásánál biztosítani kell a vízellátást, a kárterületre történő bejutást, illetve tűzzáró szakaszok kialakítását stb.

A mentési időszakban olyan operatív intézkedéseket kell végrehajtani, amelyek biztosítják az azonnali beavatkozást igénylő, legtöbb esetben műszaki tartalmú feladatok végrehajtását és az ahhoz szükséges feltételeket. Ezek közé tartozik:

- a kárterület felderítése, a kialakult helyzet tisztázása,
- a károk továbbterjedésének megakadályozása, a következmények mérséklése,
- a kialakult károk enyhítése.

Kiemelt feladat az azonnali élet- és vagyonmentés, valamint a súlyos környezeti károk kialakulásának megakadályozása. Ezt ki kell egészítenie a kialakult helyzet értékelésének, prognózisok készítésének és az operatív vezetés-irányítás aktivizálásának, működtetésének, a minősített helyzet esetleges kihirdetésével kapcsolatos döntések meghozatalának. Kardinális feladat továbbá az integrált védelmi rendszer aktiválása. A mentési feladatok végrehajtása során a különböző szakfeladatokat kombináltan kell kezelni és végrehajtani.

A helyreállítási időszakban végre kell hajtani mindazokat a műszaki tartalmú feladatokat, amelyek biztosítják a keletkezett károk, és a katasztrófa következményeinek teljes

felszámolását, a kárterületen az élet feltételeinek normalizálását, valamint az állampolgári jogok és kötelezettségek gyakorlási feltételeinek újbóli megteremtését.

Ezek az alábbiak:

- a műszaki kárfelszámoláshoz szükséges kárfelmérések,
- a kárterületről a különböző érték- és vagyonmentési feladatok végrehajtása.
- a természetes és épített környezeti károk stabilizálása és felszámolása,
- a terület rehabilitációja, a kitelepített lakosok visszatelepítése,
- a közigazgatás működési feltételeinek biztosítása,
- a közegészségügyi és járványügyi feladatok végrehajtási feltételeinek biztosítása.

A MŰSZAKI FELADATOK FAJTÁI, ÉRTELMEZÉSE, A MENTÉSI ÉS HELYREÁLLÍTÁSI FELADATOK MŰSZAKI TARTALMA, AZOK SAJÁTOSSÁGAI

A mindennapi balesetek, rendkívüli események során is előfordulnak műszaki jellegű feladatok, ezeket a mentőszervezetek és a szolgáltatók végzik el (elektromos művek, víz- és csatornázási művek stb.) A nagy kiterjedésű, összetett kárterületeken azonban minden probléma megoldásához szükséges valamilyen műszaki jellegű feladat végzése. A „műszaki" kifejezést a szervezetek, de még egy szervezeten belül is, gyakran eltérően használják és értelmezik.

A tűzoltóság tevékenységét szabályzó jogszabályok az általuk végrehajtandó műszaki mentési tevékenység alatt az alábbiakat értik:

„műszaki mentés: természeti csapás, baleset, káreset, rendellenes technológiai folyamat, műszaki meghibásodás, veszélyes anyag szabadba jutása vagy egyéb cselekmény által előidézett veszélyhelyzet során az emberélet, a testi épség és az anyagi javak védelme érdekében a tűzoltóság részéről - a rendelkezésére álló, illetőleg az általa igénybe vett eszközökkel - végzett elsődleges beavatkozói tevékenység." [43]

A polgári védelmi szervezetek műszaki egységeinek feladatai a jogszabályok szerint az alábbiak:

„a) a rendkívüli időjárási viszonyok következményeinek felszámolása,

b) a romosodott épületekben lévő személyek felkutatása, mentése,

c) közreműködés az épületekben, az üzemeltető szakmai útmutatása alapján a létfontosságú rendszerekben és létesítményekben keletkezett és egyéb műszaki károk felmérésének csökkentésében, felszámolásában, szükség szerinti helyreállításában,

d) közreműködés a lakosság és az anyagi javak megelőző műszaki védelmének végrehajtásában,

e) közreműködés a kulturális örökség védett elemei védelmében,

f) közreműködés védelmi célú építmények létesítésében, építésében,

g) közreműködés a vizek kártételei elleni védekezésben,

h) részvétel az üzemeltető szakmai útmutatása alapján a közműkárok és szolgáltatás kiesések felmérésében, valamint a szükség szerinti helyreállításában,

i) közreműködés a szükséggyógyintézetek, illetve járványügyi zárlat műszaki telepítésében, működtetésében, fenntartásában." [45; 24. § 7.]

A fentiekből is látható, hogy addig, amíg a tűzoltóság szervezetei értelmezésében a viszonylag kis kiterjedésű, intenzitású balesetek, katasztrófák esetén végrehajtandó feladatok ellátására koncentrálódik, addig a polgári védelmi szervezetek számára meghatározott feladatok nagyobb méretű kárterületen végrehajtandó feladatokat foglalnak magukba. Ezek a

feladatok feltételezik azt is, hogy nem egyedül, hanem másokkal együtt hajtják végre, azaz itt már előtérbe kerül az a követelmény, hogy a kárterületen működő szervezeteknek a munkájukat össze kell hangolniuk. Nagy kiterjedésű, és huzamosabb időn át tartó katasztrófáknál a műszaki feladatok ellátását a mentőerők és a szolgáltatók, valamint az állampolgári kötelezettség alapján létrehozott, vagy önkéntes alapú polgári védelmi szervezetek műszaki alegységei közösen hajtják végre.[16]

A fentieken túl, a műszaki feladatokat alapvetően két nagy csoportra kell bontani, ezek a mentés érdekében végrehajtandó műszaki feladatok, és a műszaki támogatási feladatokra.

A mentés érdekében végrehajtandó műszaki feladatok alatt az alábbi tevékenységeket kell érteni:

Mindazon tervezési, szervezési, koordinációs és végrehajtási feladatok összessége, amelyeket annak érdekében kell végrehajtani, hogy a kárterületen az emberi élet és az anyagi javak mentése gyorsan és hatékonyan valósuljon meg, a károk terjedését mérsékeljük, vagy megakadályozzuk, és biztosítsuk a mentőerők számára a mentéshez szükséges feltételeket. Ilyenek az utak megtisztítása, instabil, sérült épületszerkezetek rögzítése, közművek ideiglenes helyreállítása, romok alatt elzárt személyek kimentése stb.

A műszaki támogatási feladatok mindazon szervezési, koordinációs és végrehajtási feladatok összessége, amelyek célja, hogy a műszaki szakalegységek működési feltételeit biztosítja, továbbá a nem műszaki jellegű szervezetek tevékenységéhez és feladatainak végrehajtásához szükséges műszaki-szakmai tevékenységet igénylő feladatok végrehajtása és a feltételek biztosítása. Ilyen például a lakosság elhelyezéséhez szükséges épületek, közművek, energia biztosítása, táborok építése, vagy más szakalegységek számára a kárterületen a mozgás lehetőségének, a tüzek oltásához vízkivételi helyek kialakítása stb. A klasszikus értelemben vett műszaki alegységeknek legalább négy szakalegységére van/lehet szükség:

- a műszaki felderítők,
- a műszaki mentők,
- a közmű- és úthelyreállítók,
- a technikai szakalegységek.

A fentieken túl további speciális szakalegységeket is igénybe lehet venni, mint például a vasút-helyreállító, a robbantó, a búvár, a barlangi- és alpinista szakalegység stb.

A mentési és helyreállítási feladatok végrehajtásának folyamata alapvetően a kárterületen kialakult helyzettől, annak összetettségétől függ, amely meghatározza, hogy a mentésben milyen szervezeteknek, milyen felszereléssel kell részt venni, és milyen követelmények alapján kell a feladatokat végrehajtani.

A megfelelő védelmi vezetői döntések meghozatalához első, és fontos feladat *a kárterület-felderítés*[17], illetve ezen belül a károk jellemzőinek, nagyságának azonosítása, melynek feladatait egy korábbi kutatásban foglaltam össze [44], így ezt itt nem részletezem.

---

[16]Nem keverendő tehát össze a tűzoltók egy adott beavatkozás során végzendő műszaki mentési feladataival!

[17]„A műszaki felderítés során műszaki adatokat szereznek az épületek, utak, hidak, közművek, tárgyak, eszközök állapotáról, a rombolódásuk fokáról, jellegéről, a szükséges mentő-és helyreállítási munkákról, az ahhoz szükséges erőkről, eszközökről. Az épületek vizsgálata során elemzik a romtorlaszok határait, a romosodás módját, a romok alóli mentés lehetőségeit, vizsgálják a bennük rekedtek lehetséges számát, és az élet-esélyeiket". [44; 86. o.]

A műszaki károk felderítése a kárterület-felderítés speciális területét képezi. A felderítésnél a megfelelő mérések elvégzése, a felderítendő célpontok megközelítésének biztosítása, a mozgási útvonalak és irányok felderítése vagy menetvonalak kiépítése műszaki jellegű feladatok elvégzését is feltételezik. Szükségessé válhat a riasztó- és tájékoztató eszközök kiépítése és működtetése is. A következő fontos feladat, hogy a védekezés irányításához ki kell alakítani és meg kell teremteni *a vezetés alapvető feltételeit,* és végre kell hajtani az ezzel kapcsolatos műszaki feladatokat. Telepíteni kell a mozgó vezetési pontokat, ahhoz biztosítani kell az energia-ellátást, a munkafeltételeket, és szükség esetén olyan védelmi feltételeket kell kialakítani, amelyek lehetővé teszik a folyamatos vezetést a mentőerők számára.

A kárterületen végrehajtandó feladatok műszaki tartalmát alapvetően meghatározza, hogy a mentési szakaszban az életmentés mindenben elsőbbséget élvez. Kiemelt feladatot képez a mentés feltételeinek minden oldalú műszaki biztosítása. Az élőerők mentésének szempontjából szükség lehet a romos épületek alatt rekedtek mentése érdekében a beomlott, elzárt épület-részek feltárására, a romok alóli mentésre. Biztosítani kell a mentőerők felvonulási útvonalának megtisztítását, adott esetben ún. oszloputak és ideiglenes hidak építése válhat szükségessé. A tüzek terjedésének megakadályozása, tűzzáró sávok kialakítása is műszaki feladat, és feltételezi a műszaki eszközök, gépek, technológiák és a műszaki szakértelem meglétét.

További műszaki jellegű feladat a kimenekített, kitelepített lakosság elhelyezésével összefüggő feltételek biztosítása. Így például táborhelyek kialakítása, ideiglenes fürdők, illemhelyek kiépítése, az ivóvíz- és energiaellátás biztosítása. Elhúzódó mentési munkák esetén meg kell teremteni a mentőerők pihentetésének és elhelyezésének, valamint a technikai eszközök és anyagok tárolásának feltételeit is.

A mentési időszakban végrehajtandó feladatok után, a kárterület helyreállításánál is szükség van műszaki jellegű munkálatokra. Így például a mentesítési, fertőtlenítési feladatok végzéséhez szükséges feltételek biztosítása, a kárterület teljes rommentesítése a lakosság visszatelepítésével, az élet újraindításához szükséges feltételek biztosítása (közigazgatás, lakhatás, közlekedés stb.), valamint a környezeti károk felszámolása és a rekultiváció.

A műszaki tartalmú feladatok sajátossága, hogy összetett szakmai ismereteket igényelnek, hiszen a technikai ismereteken túl, tájékozottnak kell lenni a tereptani viszonyokban, az építészeti technológiákban, statikában, a hidrológiában, a balesetvédelemben és a munkaszervezésben stb. is. A feladatok végrehajtását a vezetés szempontjából is kettősség jellemzi. A tevékenység végzése a helyzetértékelésre épülő vezetői döntésen alapszik, minden szinten (kárhely-parancsnok, mentésvezető stb.) be kell tartani a vezetői döntéseket, és meghatározott rendszerben és szabályok betartása mellett kell végrehajtani azokat, ugyanakkor a kárterületi mélységben, a kármunkahelyen már a végrehajtók nagyfokú önállóságát igényli abban, hogy az adott helyzettől függően mit hogyan csinálnak, és mit nem tesznek (ennek is nagy jelentősége van).

Összességében megállapítható, hogy a kárterületen végrehajtandó kárelhárítás- és kárfelszámolás feladatainak alapja a katasztrófa-kárterület jellemzőinek ismerete. Ezek többnyire összetettek, a végzendő teendők ezért a kárterület-jellemzők felderítésével határozhatóak meg. A helyzet eszkalálódásának megakadályozása, a károk mérséklése, a

lakosság és az anyagi javak mentése érdekében műszaki jellegű feladatokat kell végrehajtani, amelyek célja a mentés és a mentés műszaki feltételeinek biztosítása.

A műszaki feladatoknál meg kell különböztetnünk a műszaki mentési feladatokat a mentési feladatok műszaki támogatásától, de mindkét tevékenységre elmondható, hogy speciális műszaki ismereteket és felkészültséget igényelnek, a végrehajtás során nagyfokú vezetési és irányítási fegyelmet, valamint a társszervekkel való szoros együttműködést és folyamatos információcserét.

A KATASZTRÓFAVÉDELEM RENDSZERSZEMLÉLETŰ, ÁTFOGÓ MEGKÖZELÍTÉSÉNEK SZÜKSÉGESSÉGE

A védelemben érintett szervek, szervezetek, személyek, stb. „reagálnak" a kialakult helyzetre, azaz, térben és időben olyan cselekvési sorozatot, vagy meghatározott feladatokat hajtanak végre, melyek csökkentik, vagy megakadályozzák a különböző veszélyek kialakulását, káros hatásainak érvényesülését. Szakpolitikai törekvés ebben is a jó minőség, megfelelő eredmény és a költséghatékonyság. A biztonság értelmezéséről és megteremtéséről, annak összetettsége miatt évek óta folyik a gondolkodás a szakemberek körében.

Abban egyetértenek, hogy az erők, eszközök, módszerek és elvek optimalizálása érdekében átfogóan, komplexitásában kell megközelíteni a kérdést. A Nemzeti Biztonsági Stratégia is ezt fogalmazza meg elvárásként.

„Korunk konfliktusainak megelőzése és kezelése globális szemléletet, valamint átfogó megközelítést igényel. A tartós, fenntartható biztonság és stabilitás megköveteli a válságkezelési – beleértve a fejlesztéspolitikai – eszközök átfogó, egymással összhangban lévő használatát, az integrált civil-katonai megközelítést és képességfejlesztést, valamint a nemzetközi szereplők együttműködésének erősítését. Az átfogó megközelítést nemzeti kormányzati szinten is alkalmazni kell". [32; I/4] Mit jelent az átfogó megközelítés?

A fogalom egyre inkább elterjedt, és napjainkban több értelmezése látott napvilágot. Kiemelhető a katonai védelmi oldalról történő értelmezés, mely szerint az átfogó, ***komprehenzív megközelítés:***

„… az összes szükséges nemzeti, illetve nemzetközi polgári és katonai elem, - beleértve a politikai, diplomáciai, gazdasági, pénzügyi, információs, szociális, gazdasági [….] stb. képességeket - együttes, koordinált alkalmazását jelenti a konfliktus megoldása érdekében. [47; 12. o.]

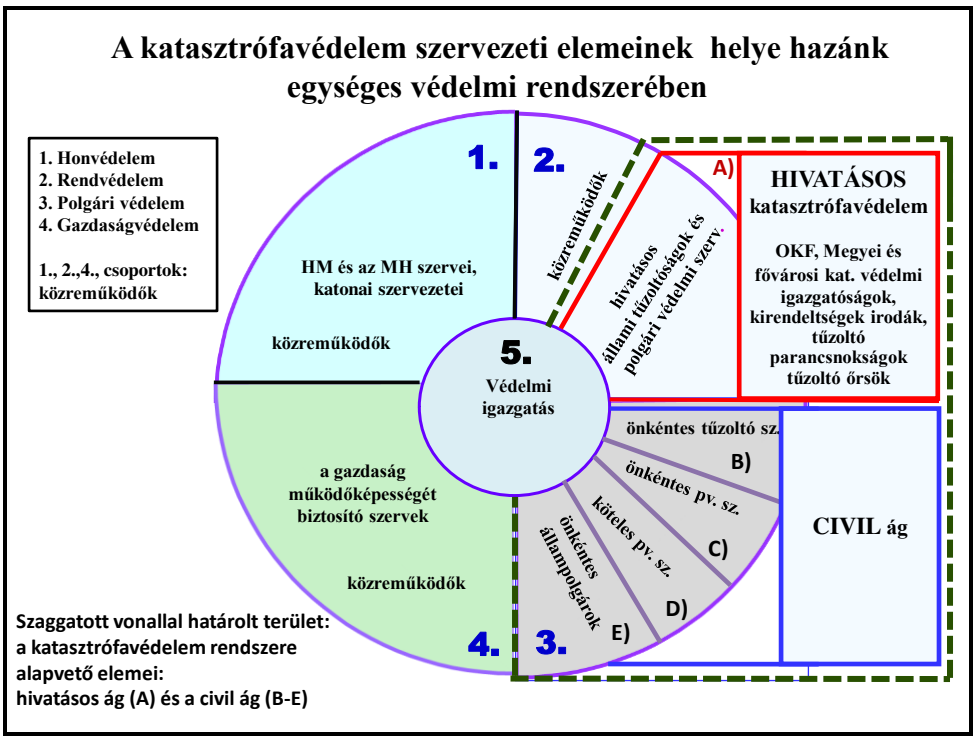
A védelem komplex rendszere és a katasztrófavédelem helye ebben a rendszerben

A biztonságot fenyegető veszélyek, az azok következtében kialakuló helyzetek megelőzésére, valamint a következmények felszámolására, és a lakosság védelmére hazánk minden kihívásra választ adó rendszert működtet, mely alapvetően a fegyveres védelem rendszeréből, valamint a polgári védekezés rendszeréből tevődik össze. Más megközelítésben a honvédelem, a gazdaságvédelem, a rendvédelem és a polgári védelem egysége adja. A rendvédelmi és polgári védelmi elemek bázisán, egy új szakterület jelent meg, a katasztrófavédelem, amely maga is egy önálló rendszert alkot.

A katasztrófavédelem rendszere három alrendszerből áll:

- a feladat-alrendszer,
- a szervezeti alrendszer,
- a végrehajtáshoz szükséges erőforrások alrendszere.

A katasztrófavédelem intézményi és szervezeti alrendszerét és azok elemeinek helyét hazánk egységes védelmi rendszerében a 4. sz. ábra mutatja. Az ábra jól tükrözi, hogy nemcsak hazánk egységes védelmi rendszere komplex, hanem a katasztrófavédelem is rendszere, mivel felöleli azokat a szervezeti és intézményi elemeket, amelyeket mind fegyveres küzdelem, mind katasztrófák esetén a védekezés alapját képezik. A védelmi rendszert ezért komplexen kell kezelni és értelmezni.



4. ábra A katasztrófavédelem szervezeti elemeinek helye hazánk egységes védelmi rendszerében.

Mára már nemcsak a katonai fenyegetés jelent komoly veszélyt, hanem a katasztrófák, környezeti veszélyek, a különböző természeti és civilizációs kihívások is, mint az éghajlatváltozás, migráció stb. Az utóbbi évtizedek kutatásai és a bekövetkezett katasztrófák, veszélyek felszámolása során szerzett tapasztalatok azt bizonyítják, hogy az ezekre történő felkészülés, a mentés, a következmények felszámolása összetett, komplex feladatrendszert képez. Ezeket átfogóan, minden részletre kiterjedően kell értelmezni, és a feladatok megoldásában minden résztvevő szervezet és az erőforrások összehangolt alkalmazására van szükség, hogy a szinergia-hatások érvényesüljenek. Vizsgáljuk meg a katasztrófavédelmi rendszer átfogó megközelítésének szükségességét!

Az átfogó megközelítés szükségessége a katasztrófavédelem területén

Az átfogó megközelítés szükségességének bizonyításához abból célszerű kiindulni, hogy a katasztrófavédelem három alrendszeréből áll, amelyeket összetettségük miatt, szintén átfogóan kell vizsgálni és értelmezni. Ezt az alábbiakban összegzem:

A katasztrófavédelem feladat-alrendszerének átfogó megközelítése

A kárterületi teendők összetettsége, valamint a védekezés és a kárelhárítás folyamatainak bonyolultsága maga után vonja, hogy a feladatokat az átfogó megközelítés szellemében kell meghatározni. Ezeknek ki kell terjedniük mind a megelőzés, a mentés és a helyreállítás feladataira, és tartalmukat tekintve pedig készülni kell mind a polgári védelmi, a tűzvédelmi, mind pedig az iparbiztonsági feladatok ellátására. Ezek jellemzője, hogy térben és időben

összefüggő rendszert alkotnak, amelynek okán a végrehajtóknak fontos együttműködés minden szintjének, irányának és feladatának a meghatározása.

A megelőzés feladatainak eredményes és hatékony végrehajtása hatással van, és alapvetően befolyásolja a katasztrófák kialakulását, pusztító hatásait, és ezáltal a mentés időszakában végrehajtandó feladatokat, azaz egymással szorosan összefüggnek. A mentés és a helyreállítás feladataira ugyanez érvényes. A mentés során végzett feladatok szintén hatással vannak a helyreállítási feladatokra, mert egy eredményes mentés és védekezés minimális helyreállítási feladatokat von maga után.

A védekezésben részvevő szervek, szervezetek alkalmazásának elveit, módszereit is átfogóan kell megközelíteni, össze kell hangolni a tevékenységeket, a módszereket és az alkalmazandó eszközöket. A katasztrófavédelemben korábban bemutatott hivatásos szervek és a közreműködők sokrétűsége megkívánja egymás rendszereinek ismeretét, a gyakorlati munka összehangolását, melyek egyik lehetséges útja a közös gyakorlatok és felkészítés szervezése.

A fentiek miatt a három időszak feladatait nem lehet egymástól elkülönítve kezelni, ezek együttes értelmezésével, vizsgálatával lehet csak helyes döntéseket hozni. A feladatrendszerek komprehenzív megközelítésével és ezek összefüggéseinek feltárásával lehet meghatározni a szükséges és elégséges védelmi szint eléréséhez szükséges feladatokat és azok végrehajtásának prioritásait.

A katasztrófavédelem szervezeti alrendszerének átfogó megközelítése

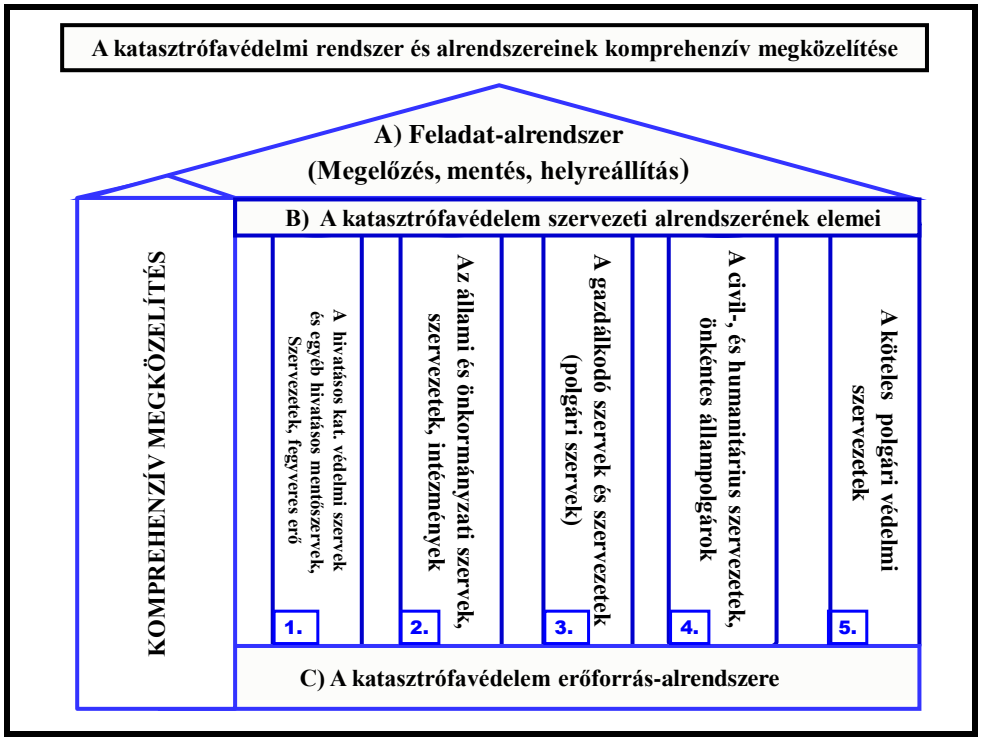
A védelem komplex rendszerének szervezeti elemeit az 4. ábra alapján vizsgálva megállapítható, hogy vannak a katasztrófavédelemben csak közreműködőként résztvevő szervezeti elemek (MH, rendvédelmi szervek, állami szervek intézmények stb.). A katasztrófavédelem szervezeti elemei pedig nemcsak a katasztrófavédelmi feladatok végrehajtásában vesznek részt, hanem közreműködnek az ország egyéb veszélyeztetettségével összefüggő feladatok végrehajtásában is. A katasztrófavédelem szervezeti elemei civil és hivatásos ágra oszthatóak, és különböző alaprendeltetésűek, ezért alkalmazhatóságukat, képességeiket egy feladat végrehajtása során komplexen kell áttekinteni, és a mentést úgy kell megszervezni, hogy ezek együttes vagy egymás utáni alkalmazásával a feladat a legoptimálisabban lehessen végrehajtható. Ezek vizsgálatát is átfogóan, komplexitásában kell megközelíteni, mert a mentés során helytelen döntéshez vezet az, ha a szervezeti elemeket nem összehangoltan, nem képesség szerint vetik be, és a tevékenységüket nem ennek megfelelően szervezik. Szem előtt kell tartani ezeknek a szervezeteknek az együttműködést, az összehangolt felkészítést, mert ez az eredményes végrehajtás záloga.

Ismerniük kell a veszélyeztető tényezőket, azok lehetséges következményeit, a kárterületek jellemzőit, valamint az ott végzendő feladatokat, másrészt a rendszert, amelyben adott esetben közreműködőként. Fontos eleme a feladat-végrehajtásnak a kommunikáció, ezért egymás információs rendjének, és eszközeinek ismerete is alapvető feltétele az eredményes együttműködésnek. A riasztási és alkalmazási rendek és egyéb, a közös munkára hatással lévő specialitások feltérképezése is nélkülözhetetlen. Ennek legjobb módja a közös gyakorlatok workshopok, konferenciák szervezése.

A katasztrófavédelem erőforrás alrendszerének átfogó megközelítése

A katasztrófák elleni védelem össztársadalmi feladat, melynek végrehajtásához egyetlen szervezet sem rendelkezik minden szükséges eszközzel és erővel, ami egy katasztrófa felszámolásához egyedül elégséges lenne. Az elmúlt időszak katasztrófa-eseményeit vizsgálva elmondható, hogy az ott alkalmazott erő-eszköz alrendszer több forrásból tevődik össze. A

munkálatoknál a mentőerők a saját eszközeiket, erőiket használták, valamint az adott település forrásait. Több esetben szükség volt a védekezésre elkülönített állami és önkormányzati alapok, eszközök, gépek stb. bevonására is. Ezen túlmenően az állampolgárok javai is bevonhatóak a védekezésbe. Sok esetben az állampolgárok és a civil szervezetek speciális eszközeit is igénybe kell venni, de érkezhetnek nemzetközi és hazai segélyek is. Ezen erőforrások elemek összehangolt felhasználását csak úgy lehet eredményesen és költséghatékonyan végrehajtani, ha az erőforrásokhoz való hozzájutást, annak költségvonzatát, a kárterületre való kijuttatását rendszerszemlélettel közelítik meg, és ennek megfelelően tervezik meg és hajtják végre. A katasztrófavédelmi alrendszereket (A-C) és azok átfogó megközelítésének szükségességét az 5. sz. ábra is jól szemlélteti.



5. ábra A katasztrófavédelmi rendszer és alrendszereinek átfogó (komprehenzív) megközelítése. (Készítette: a szerző.)

ÖSSZEGZETT KÖVETKEZTETÉSEK:

Az ország és a lakosság biztonságát fenyegető tényezők szerteágazóak, értelmezésükre, fogalmaikra és a csoportba sorolásukra sok kísérlet történt annak megfelelően, hogy milyen céllal vizsgálták a kutatók a problémakört, és milyen jellegű dokumentum készült a vizsgálatból. A védelmi rendszer működésére és szervezeti kialakítására, a jog- és igazgatás szabályzási hagyományaira, valamint a témával kapcsolatos kutatások eredményeire épülő szabályzókban, kockázatelemzésekben és egyéb dokumentumokban, a veszélyeztető tényezők a kihívások, kockázatok, fenyegetések, válságok és háborúk kategóriában jelentkeznek, azaz az intenzitás-alapú kategorizálásban, valamint a szektorális értelmezésen túl, a veszély jellegéből kiinduló értelmezésekkel találkozunk. A biztonság-értelmezéseket, és a biztonságot fenyegető tényezők körét, és az ellenük való védekezés lehetőségeit vizsgáló dokumentumok a biztonságpolitikai, szakpolitikai és szakmamódszertani kategóriába sorolhatóak. A szerzők a következtetéseikben mindannyian rámutattak a veszélyek sokrétűségére, és az állami és civil

szereplők felelősségére az ellenük való védekezésben. Az irodalmak a veszélyeztető tényezők megnevezésében és csoportosításában eltérőek és másként értelmezik a katasztrófákat is.

Bizonyítottam, hogy a katasztrófák önálló veszélytényezőként kell kezelni, és nem azok hatásaként értelmezendőek. A fent vázolt kockázatelemzéseket és a témához kapcsolódó irodalmakat vizsgálva megállapítható, hogy a természeti eredetű katasztrófák közül az ár- és belvizek, a rendkívüli időjárás, viharok, extrém esőzések és a természeti tüzek, a civilizációs veszélyek közül az ipari balesetek és a veszélyes anyagok gyártása, szállítása, felhasználása során kialakuló katasztrófákra kell készülni.

A katasztrófák következtében kialakult kárterületek összetettek, ezért mind a megelőzés, a mentés, a következményeik elhárítása, valamint a helyreállítási feladatok végrehajtása összehangolást és tervszerűséget igényel. Az alrendszerek összefüggéseinek vizsgálatával bizonyítható, hogy a katasztrófavédelem átfogó megközelítése elkerülhetetlen és szükséges. A feladatok típusa és fajtája eltérő, de túlnyomó többségükben műszaki jellegű tevékenységet igényelnek. Bemutattam, hogy ezek értelmezése és csoportosítása a végrehajtó szervezetek szemszögéből nem egyforma, valamint, hogy alapvetően két típusát különböztetjük meg, a műszaki mentési és a műszaki támogatási feladatokat. Bizonyítottam, hogy a katasztrófavédelem rendszerét és alrendszereit átfogóan kell értelmezni, mert ennek hiányában sem az ország védelem rendszere, sem a katasztrófák elleni védekezés nem lehet eredményes. Egy célorientált és költséghatékony rendszer kialakításához feltétlenül szükséges a „mit kell megoldani?” -kérdés megválaszolása, azaz azoknak a kárterület-jellemzőknek a megismerése, amelyek tükrében a szükséges feladatok, és erőforrások meghatározhatóak. A védekezés folyamatát komplexen kell kezelni, ezért a megoldásra hivatott rendszert, a működési elveket és a megoldási módokat mindig ehhez kell igazítani. A szervezeteket úgy kell működtetni, hogy a védekezésben résztvevők összehangoltan lássák el a feladataikat.

Ebben a cikkben részben feltártam a védelem és a katasztrófavédelem területén lévő szemléleti és megközelítési tendenciákat. A következtetésekre alapozva javaslom, hogy a további kutatások végzői, a jogszabályalkotók, és a védelmi szféra hivatásrendjei a gyakorlati munka során ezeket a kérdéseket a komprehenzív megközelítés szellemében vizsgálják, és erre alapozva tárják fel az összefüggéseket, valamint az esetleges hiátusokat.

FELHASZNÁLT IRODALOM

[1] 290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról

[2] KŐSZEGVÁRI T.: A nemzetközi biztonságot fenyegető új kihívások és kockázatok. egyetemi jegyzet, ZMNE, Budapest, 1999. 30. o.

[3] BOGNÁR K.: A háború fogalmának, tartalmának múltja, jelene és jövője. Új Honvédségi Szemle, 2005: sz. n. 1-25. o.

[4] Szerk.: KOÓS A.: Biztonságpolitikai prognózis 2015-ig. BHKKA, Budapest, 2010. 392 o.

[5] GAZDAG F.c: Biztonsági tanulmányok alapjai. NKE, Budapest: 2013. 232 o.

[6] CSIKI T., Tálas P.: Biztonságpolitikai kihívások. ín: Szerk.: Gazdag Ferenc: Biztonsági tanulmányok-biztonságpolitika. ZMNE, Budapest, 2011. 91-135. o.

[7] HUNTINGTON, S. P.: A civilizációk összecsapása és a világrend átalakulása. Európa Könyvkiadó, Budapest, 1999. 625 o.

[8] SZENES Z: A Katonai kihívások a 21. század elején, Hadtudomány, 2015. december, XV. évfolyam 4. szám, oldalszám n.

[9] BALOGH I., KAISER F., TÁLAS P. et al: A Globalizáció kihívásai. in: Szerk.: Gazdag Ferenc: Biztonsági tanulmányok-biztonságpolitika. ZMNE, Budapest, 2011. 137-189. o.

[10] ENDRESZ E.: A nemzetközi terrorizmus sajátosságai. in: Szerk. Dr. Vámosi Zoltán: A biztonságról fiataloknak. TIT HABE, Budapest, 2010. 73-89. o.

[11] MARJÁN A., ORBÁN A.: Az Európai Unió globális környezetének változása. In: Marján Attila (szerk.) Magyarország első évtizede az Európai Unióban 2004-2014. Budapest, 2014. Nemzeti Közszolgálati Egyetem, 2014. 215-238. o.

[12] PADÁNYI J.: Az éghajlatváltozás és a katonai erő viszonyrendszere a nemzetközi kutatások tükrében. Repüléstudományi Közlemények, (1997-től) 2012:(2), 111-118. o. Repüléstudományi Konferencia 2012. Szolnok, Magyarország: 2012.04.12

[13] NAGY K., HALÁSZ L.: Katasztrófavédelem. 2002. ZNME, Budapest, 147 o.

[14] POPELYÁK P., KÁTAI-URBÁN L.: Ipari biztonsági és katasztrófavédelmi kutatások az Európai Unióban. Munkavédelem és Biztonságtechnika, 2003. 25:(3) 49-52. o.

[15] ENDRŐDI I.: A katasztrófa-elhárításra felkészítő ismeretek. Budapest, Magyar Polgári Védelmi Szövetség, 2007. 122 o.

[16] HORNYACSEK J., Veres V.: Katasztrófák, sebezhetőség, biztonság. Hadtudomány, 17:(3) Paper 13. (2007), 101-113. o.

[17] VÁGVÖLGYI Z.: A vörösiszap katasztrófa környezeti hatásai, kárelhárítási folyamata, alkalmazott módszerei. Hadmérnök, 2011. VI. évfolyam, 1. szám, 261-275. o.

[18] TÓTH R.: A repülőeszközök alkalmazásának lehetséges területei és korlátai Repüléstudományi közlemények 2011/2 különszám, 2011. 1-23. o.

[19] HORNYACSEK J.: A felsőoktatási intézményeket veszélyeztető tényezők, és az ellenük való védelem lehetőségei. Műszaki Katonai Közlöny, 2011. december, 325-350. o.

[20] SZENES Z.: Tudomány és korszerű haderő. Magyar tudomány, 2015. február, 194-201. o.

[21] SZENES Z.: Válság vagy sodródás? A védelemgazdaság problémái Magyarországon. Hadtudomány: 2015. 25:(3-4) 91-108. o.

[22] MUHORAY Á.: A katasztrófavédelem aktuális feladatai. Hadtudomány, 2012. 1-2. sz. 1-17. o.

[23] FELHÁZI S., RUSZIN R.: A tüzérségi támogatás feladatrendszere az új kihívások tükrében. Hadtudomány, XVII. évfolyam, 2. sz. 2007. június, oldalszám n.

[24] TÁLAS P.: A terrorveszélyhelyzet-diskurzus margójára. Nemzet és Biztonság. Biztonságpolitikai Szemle, 2016: (1) 40-47. o.

[25] HORNYACSEK J.: A lakosság védelmének újszerű értelmezése és alkalmazási lehetőségei a New Orleans-i Katrina hurrikán eseményeinek tapasztalata alapján. Műszaki Katonai Közlöny, XXI. évfolyam, 1-4. sz. 2011. december, 370-396. o.

[26] HORNYACSEK J.: A Felsőoktatási Intézményeket veszélyeztető tényezők, és az ellenük való védelem lehetőségei. Műszaki Katonai Közlöny, XXI. évfolyam, 1-4. sz. 2011. december, 325-350. o.

[27] HAIG Zs.: Információ - Társadalom – Biztonság. Budapest: NKE Szolgáltató Kft., 2015. 291 o.

[28] FLEINER R., MUNK S.r: Közigazgatási adatbázisok összekapcsolásának biztonsági kérdései, Hadmérnök, 2012. VII.:(4) 119-127. o.

[29] KOVÁCS L., KRASZNAY Cs.: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és biztonság, 2010. 44-56. o.

[30] KIS N., BÁGER G., CSATH M. at al: Jó Állam Jelentés. NKE, Budapest, 2015. 136 o.

[31] A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2073/2004. (III.31.) Korm. határozat.

[32] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról.

[33] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

[34] Szerk.: Dr. GYENES Zs.: Nemzeti Katasztrófa Kockázat Értékelés – Magyarország, 2011., http://vmkatig.hu/KEK.pdf (letöltés: 2017. 01.10.)

[34 b] TÓTH F., HARMATI I., CSEH-SZAKÁL T.: Kockázatbecslési eljárás, településeink veszélyeztetettsége. https://mail.google.com/mail/u/0/#inbox/159b03eb14982dbf?projector=1 (letöltés ideje: 2016. 01.04.]

[35] Jelentés Magyarország nemzeti katasztrófakockázat-értékelési módszertanáról és annak eredményeiről. 2014. BM OKF, Budapest, 80 o.

[36] CSEH G.: Kockázatelemzési módszerek a veszélyes anyagokkal kapcsolatos súlyos baleseti veszélyek szabályozása területén. - doktori értekezés. ZMNE, Budapest, 2005.

[37] CIVPRO 0865R2 Project: Veszélyelemzési segédlet regionális veszélyelemzési jelentése. NFÜ 2012.

[38] 2384/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[39 a] Schadenerreignisse weltweit 2015. Prozentuale verteilung. https://www.munichre.com/site/corporate/get/documents_E-1153083917/mr/assetpool.shared/Documents/5_Touch/Natural%20Hazards/NatCatService/Annual%20Statistics/2015/2015_Torten_Kontinente_d.pdf (letöltés: 2017. 01.10.)

[39 b] Weltkarte der Naturkatastrophen. Gograpchische Übersicht. https://www.munichre.com/site/corporate/get/documents_E-885643431/mr/assetpool.shared/Documents/5_Touch/Natural%20Hazards/NatCatService/Annual%20Statistics/2015/2015_Weltkarte_d.pdf (letöltés: 2017. 01.10.)

[39 c] Schadenereignisseweltweit 2015. 10 teuerste Ereignisse für die Gesamtwirtschaft https://www.munichre.com/site/corporate/get/documents_E-654401102/mr/assetpool.shared/Documents/5_Touch/Natural%20Hazards/NatCatService/Annual%20Statistics/2015/2015_Tabellen_eco_d.pdf (letöltés ideje: 2015. 01. 07)

[40] Szerző nélkül: Veszélyhelyzet-kezelés. Katasztrófavédelmi Oktatási Központ, 2011. 89 o.

[41] NIKODÉM E: A lakosság és az anyagi javak hazai védelmének újszerű értelmezése, megvalósításának követelményei, lehetséges módszerei. –doktori értekezés NKE, Budapest, 2013. 272 o.

[42] Utasítás a polgári védelmi műszaki ezred műszaki alegységei mentési munkájának megszervezésére. PVOP, Budapest, 1987. 119 oldal

[43] Tűzoltás, műszaki mentés. http://www.katasztrofavedelem.hu/index2.php?pageid=tuzoltas_index

[44] HORNYACSEK J.: A katasztrófa-kárterület felderítésének elméleti és gyakorlati kérdései. Hadmérnök, VIII. évfolyam, 1. szám, 2013. március, 79-98. o.

[45] 62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól

[46] SZABÓ S.: A műszaki támogatás cél- és feladatrendszerének támogatása. http://193.224.76.2/downloads/konyvtar/digitgy/20012/eloadas/szabosa.html (2016. 01.04.)

[47] Szerk.: KESZELY L.: Az átfogó megközelítés és a védelmi igazgatás. Zrínyi Kiadó, 2013. 207 o.

[48] PADÁNYI J.: Az éghajlatváltozás hatása a biztonságra és a katonai erő alkalmazására. Stratégiai Védelmi Kutatóintézet, Budapest, 2010. 115 o.

[49] BODA J., BOLDIZSÁR G., KOVÁCS L. et al. : Fókusz és együttműködés. A hadtudomány kutatási feladatai. Honvédségi Szemle, 2016. 3. 3-19. o. (##)

[50] SIMICSKÓ I.: A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével. Hadtudomány, 26:(3-4) pp. 100-113. (2016)

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

CUT THE COSTS AND ENHANCE EFFICIENCY IN NUCLEAR SAFETY AND SECURITY CULTURE SELF-ASSESSMENTS: CONSIDERATIONS THAT SHOULD BE TAKEN TO MERGE NUCLEAR SAFETY AND SECURITY CULTURE ASSESSMENTS

KÖLTSÉGCSÖKKENTÉS ÉS HATÉKONYSÁGNÖVELÉS A NUKLEÁRIS BIZTONSÁGI ÉS VÉDETTSÉGI KULTÚRA FELMÉRÉSEKBEN: MEGFONTOLÁSOK AMELYEKHEZ TARTANUNK KELL MAGUNKAT, HA ÖSSZEVONJUK A NUKLEÁRIS BIZTONSÁGI ÉS VÉDETTSÉGI KULTÚRA FELMÉRÉSEKET

HORVÁTH Kristóf; SOLYMOSI Máté; VINCZE Árpád; VASS Gyula

(ORCID: 0000-0001-8979-9995); (ORCID: 0000-0002-6302-0370); (ORCID: 0000-0002-1197-2505); (ORCID: 0000-0002-1845-2027)

kristof.horvath.dr@gmail.com, mate.solymosi@somos.hu; vincze@oah.hu, gyula.vass@katved.gov.hu

Abstract

About the peaceful applications of atomic energy, there can be no doubt, that safety accidents have the greatest effect on the public opinion. Besides safety - culture -, the security incident of the recent years highlighted the importance of security and the culture for security, but it is still not a principal issue.
The topic of nuclear safety culture, the human factor within safety issues has been recognized as an important component of nuclear safety performance since Chernobyl.
How to make nuclear security as relevant as safety, how does nuclear security culture relate to safety (culture) and what and how can security culture assessments can benefit from the lot of results that nuclear safety culture has reached? This paper answers a specific part of the above-mentioned topics and provides important considerations about the combination of nuclear safety & security culture assessment.

Keywords: *Nuclear safety culture, nuclear security culture, culture assessment and combination*

Absztrakt

Az atomenergia békés alkalmazásait tekintve kétség sem merülhet fel afelől, hogy a biztonsági balesetek befolyásolják legnagyobb mértékben a közvéleményt. Azonban a biztonsági - kultúra – mellett az utóbbi évek védettségi eseményei felhívták a figyelmet a védettség és a védettségi kultúra fontosságára, amely ennek ellenére továbbra sem tekinthető elsődleges feladatbak.
A biztonsági kultúra témája, a biztonsági eseményekkel kapcsolatos emberi tényezők szerepe Csernobil óta ismeretes.
Hogyan tegyük a védettséget ugyanolyan fontos üggyé, mint a biztonság? Hogyan kapcsolódik a biztonsági és védettségi kultúra? Valamint a biztonsági kultúra által elért eredményeket hogyan tudja a védettségi kultúra felmérés kamatoztatni?
A cikk a fent említett kérdésekre ad választ, valamint fontos megfontolásokat tartalmaz a biztonsági és védettségi kultúra felmérések összevonásával kapcsolatban.

Kulcsszavak: *Nukleáris biztonsági kultúra, Nukleáris védettségi kultúra, kultúra felmérés és összevonás*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.16.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.02.28.

INTRODUCTION

About the peaceful applications of atomic energy, there can be no doubt, that safety accidents have the greatest (negative!) effect on the public opinion. One of the main reasons behind this is most likely the fact that because of security consideration safety incidents have received and in the future, will receive much more publicity, than the security incident. [1] Accordingly, nuclear safety is one of the "flagships" and probably the most important missions of the nuclear industry and this is reflected in regulations, decisions makings, communication and unfortunately in allocation of resources. The topic of Nuclear Safety Culture, the human factor within safety issues has been recognized as an important component of nuclear safety performance since Chernobyl. [2] Although beside the importance of safety culture well-known security incidents of the recent years in Pelindaba [3] and in Belgium [4] highlighted the value of security and the culture for security, it is still not a principal issue. What can be done to make nuclear security as relevant as safety? How does nuclear security culture relate to safety (culture)? What and how can security culture assessments can benefit from the lot of results that nuclear safety culture has reached? This paper answers a specific part of the above-mentioned questions and provides considerations about the combination of nuclear safety & security culture assessment that can be useful not just in NPPs or in nuclear installations, but in other radioactive material associated facilities in Hungary. [5]

ABOUT THE CULTURE FOR NUCLEAR SAFETY

Weaknesses in safety culture have contributed to significant accidents at the Three Mile Island Unit 2 and Chernobyl, and significant incidents at Davis-Besse, Vandellos II, Paks and Forsmark, among others. [6] the self-assessment of the nuclear safety culture is a requirement in the nuclear industry for several years and during these years several assessments were already successfully conducted. From these self-assessments a much larger amount of valuable independent data and information were born - besides trend and side analysis. The efficient and effective use of these data, methods and processes are essential for the assessments in the future too. but few years ago a new player appeared on the scene, the need for nuclear security culture.

THE BACKGROUND OF THE CULTURE FOR NUCLEAR SECURITY

The necessity for separate nuclear security culture was rooted in the terrorist attack on the 11th of September 2001. The first reply to that was a report by the International Atomic Energy Agency (IAEA) on "Measures to Improve the Security of Nuclear Materials and Other Radioactive Materials". [7] Besides the IAEA, States and the World Institute for Nuclear Security are working together to strengthen nuclear security culture by publishing guides and hosting (international) workshops. [8]

The basis of all IAEA nuclear security culture documents is NSS 07 Implementing Guide, which was published in 2008 and provides a model for nuclear security culture, identifies roles and responsibilities of various nuclear security stakeholders. In 2014 the IAEA released NST 026, a detailed technical guidance about nuclear security culture self-assessment, that describes the method and the process of nuclear security culture assessment, and a provides the necessary instructions for either nuclear safety culture or nuclear security culture assessment. Probably as the most significant innovation, it determines characteristics and indicators of nuclear security culture assessment and illustrates them with practical examples. Since then NST 027 technical guidance came into state of the "Member state comments",

which provides examples and case studies about the progresses of nuclear security culture enhancement. [1]

ABOUT THE INTEGRATION BETWEEN NUCLEAR SAFETY CULTURE AND NUCLEAR SECURITY CULTURE SELF-ASSESSMENT

Both safety and security awareness (and performance) are part of the culture of an organisation. They share the same goal to protect the individuals, the public and the environment from the harmful effects of ionizing radiation.

The IAEA's concept of shared objectives between nuclear security culture and nuclear safety culture is manifested also by the agency's organizational structure, which places the responsibility for both disciplines within an integrated IAEA Department of Nuclear Safety and Security. [7]

Several documents were published regarding the interface between nuclear safety and security. The latest one is TECDOC-1801 [9], the "Management of the Interface between Nuclear Safety and Security in Research Reactors" which emphasizes that the integration between the two disciplines is relevant.

However, the functional categories of the safety and security management systems are very similar[1], there are some differences both in the management processes[2] as well as in the approach of the culture too. Security deals with deliberate acts and demands that the sharing of information typically be restricted only to authorized trusted personnel on a valid "need-to-know" basis, to prevent sensitive information related to security measures or safety/security weaknesses at the facility from falling into the hands of adversaries. On the other hand, safety culture pursues transparency. It shares feedback on experience, thereby preventing repetitive occurrences of incidents or accidents and to disseminate information to prevent such occurrences from being repeated. In some cases, however, it may be necessary to withhold safety information for security reasons, such as information that might reveal a vulnerability which could be exploited by a person or persons having malicious intent. Therefore, the management needs to clearly identify not only safety and security as distinct processes to be managed, but also the interface between them, so that the areas of common ground and the areas of potential conflict between the two disciplines can be properly managed [9]

THE COMBINATION OF NUCLEAR SAFETY AND SECURITY CULTURE SELF-ASSESSMENT

Per my theory with necessary and appropriate preparation the determination of the overall culture through an integrated nuclear security culture and nuclear safety culture self-assessment, is more efficient and effective than separate assessments. There can be no doubt about the cost-efficiency of a merged assessment. However, in the following all the considerations will be described step by step that must be taken to reach the desired efficiency and effectiveness with the contraction. [10] [6]

---

[1] management responsibility, resource management, quality management, process implementation, performance assessment and improvement

[2] Typical processes for safety include the procedural management of safety analysis, fuel handling and core management, reactor operation, experiments, maintenance of systems and components important to safety and emergency preparedness. Typical security processes include personnel security, information security, computer security, access control, security training and exercises, system sustainability, security event reporting and management of the security organization and equipment.

The fundamental assumption is that self-assessment team needs to have a broad range of competencies and experience. At the first sight, the difference between integrated and separate assessments seems to be small… However, a separated team only has a delegate from the "other" team and the leading assumption is only either nuclear safety culture or nuclear security culture. On the other hand, an integrated team must have experts from both safety and security fields, and every member should have a comprehensive integrated approach from both nuclear safety culture and nuclear security culture, which makes an overall comprehensive approach of the assessment possible.

	Combined self-assessment	Separated self-assessments
Senior management workshop and commitment	With an integrated approach the management can cut the costs and enhance the efficiency.	During workshops and commitment, the integration is not part of the scope.
Self-assessment team composition	The Self-assessment team should contain experts from both safety and security fields and everyone must be aware of (culture for) safety and security as parts of the complete picture.	The fundamental role has either Nuclear Safety Culture or Nuclear Security Culture and according to that the scope is to assess and enhance only one of them.
Training on self-assessment	The training must handle culture as a whole.	The awareness of nuclear safety culture and nuclear security culture are separately handled.

Table 1. Prerequisite/general considerations: implementation of Action plan and Follow-up (made by the authors)

The preparation of the organisation in case of the assessment of the culture, is a very (if not the most) important activity. Without an appropriate establishment, it can go in a wrong direction, which is especially true if the organisation implements a combined self-assessment. It needs a comprehensive approach, and without it the campaign can do more harm than good. It may confuse the personnel without the possibility any reliably and valid result or enhancement. As it can be seen, there are several differences in the preparatory phase between merged and separated self-assessment.

	Combined self-assessment	Separated self-assessments
Allocation of the resources	To conduct one self-assessment is obviously the cost-efficient choice. But on the other hand the roles and responsibilities need to be harmonised.	Two separate self-assessments are more expensive, but the roles and responsibilities (safety or security divisions) are more clear.
Prepare the self-assessment team	The team put priority on safety and security approaches, but should handle the culture of the organisation as an integrated whole.	Prepare the team for a good organisational culture, but the focus is either on safety or security approach.
Prepare the Self-assessment plan	Integrated plan is needed to assess the complete whole of the culture and including nuclear security culture and nuclear safety culture and especially the interfaces between them.	A separate Self-assessment plan should contain all requirements (either safety or security (culture). *Simpler approach*.

	Integrated approach.	
Pre-launch	A harmonious and targeted campaign can reduce the costs, but without a strong communication and cooperation can do more harm than good.	There is no need for special integration. Two separate campaigns are more expensive, but it can clarify separate safety and security culture.

Table I. Preparatory Phase: Prepare the Organisation (made by the authors)

The main reason to conduct combined culture Self-assessment is that from technical aspects, that the prescribed recommendations of Nuclear Safety Culture and Nuclear Security Culture Self-assessment are very similar. In the conducting phase, there is no need for any special effort to pay attention on the interface. The processes and the methods [3]are appropriate to assess all and any type of culture, therefore by the combination of SAs the costs can be easily reduced.

Methods and Processes	All the methods and processes of Nuclear Safety Culture and Nuclear Security Culture Self-assessment can be merged without any difficulty.

Table II. Conduct Phase (made by the authors)

Several IAEA documents deal with the issue of the analysis of the assessments and the only difference between merged and separated ones is not the method, but the object of the analysis. During the analysis, attention must be paid to the overall culture of the organisation and/or as a part of it Nuclear Security Culture and Nuclear Safety Culture. The analysis method is very similar in every attitude assessment obviously, the variables and the connections to each other are different.

Communication of the results is similar from many aspects to the preparation campaign. With the help of an integrated communication the costs and redundancies will be reduced and a coherent enhancement of the organisational culture can be achieved.

	Combined self-assessment	Separated self-assessments
Analysis	The culture and the interface between Nuclear Safety Culture and Nuclear Security Culture must be analysed.	There is no need to pay special attention on the analysis of the interface between Nuclear Security Culture and Nuclear Safety Culture.
Prepare Assessment Report	The integrated Assessment Report handles the culture and as the leading segment the awareness of safety and security.	Prepare two separate Assessment Report. The focus is on the attitude of either safety or security. The integration does not play an important role.
Communication of the results	Like the pre-launch campaign, an integrated approach is essential.	Simpler messages in simpler campaigns, but separately for safety and security field.

Table III. Analysis & Communication Phase (made by the authors)

[3] interview, focus-group, survey, document review and observation

The communication is not a one-way traffic… It is preferable to communicate the results and then receive feedback from the management, but the employees must be involved in developing and finalizing the action plan too. Their involvement results in more commitment to successful implementation compared with top-down direction.

	Combined self-assessment	Separated self-assessment
Feedbacks	Feedbacks are related to the overall culture of the organisation.	Feedbacks are related only either to nuclear safety culture or nuclear security culture.
Engagement of the management	Both managements (safety and security) must be engaged besides the overall culture of the organisation.	The action plan consists information about the engagement of either safety or security culture.

Table 5. Preparation of the action plan: based on the feedback of the management and employees (made by the authors)

While the combined action plan takes the culture as a whole (and as its important parts the safety and security awareness) into considerations, the separated action plans concentrate on the analysis and the enhancement of either safety or security culture. Improvements require a long term strategy and plan in addition to ongoing promotion of continuous improvements. The process should be repeated within 6-18 month.

	Combined self-assessment	Separated self-assessment
Implement the action plan	The implementation is done with a strong cooperation by safety and security divisions through a holistic approach.	The focus of the implementation is either on safety or security, no need for a special link between the divisions.
Conduct a follow up	The follow-up information does not concentrate on one division, strong cooperation is necessary between them.	The process is handled by either safety or security division.

Table 6IV. Implementation of action plan and Follow-up (made by the authors)

CONCLUSION

It was already emphasized, that the integration between nuclear safety and security is an important issue. Important, because the consolidation of all the regulations, roles, responsibilities, decision making and the allocation of the resources would possess practical difficulties. But the culture is something different…

If we take a closer look on the attitude of safety and security (by the IAEA), apart from the approach to sensitive information and transparency, there are no significant difference between them. An overall comprehensive approach of organizational culture would be prefect, and safety and security awareness is "just" a segment of it.

Beside cost-efficiency, because of reliability and validity considerations one attitude measurement is always better then two separate ones. Overall, however, the integration can do more harm than good, but with preparation these disadvantages can be prevented.

The first challenge that should be solved is to create the image of an ideal organisational culture and fill all the requirements of the ideal safety and security attitudes within. Communicate the message successfully– the preparation before the assessment and the results and action plan after it -. One single message about the right organisational culture with the necessary safety and security approaches can reach the target easier.

The second challenge is to create a perfect collaboration between the different divisions, rules and responsibilities. In ideal circumstances the energies that were spared with the single merged nuclear security culture & nuclear safety culture campaign and assessment do not exceed the costs of the collaboration between the different divisions and the alignment of the management.

The third and easiest challenge is, to conduct the self-assessment successfully, that it is described by the IAEA in the either in nuclear security culture or nuclear safety culture guidance [10] [6] and during the whole process special attention must be paid on both safety and security approaches.

Without the integrated message and collaboration, a contraction just confuses the personnel and the management too. The IAEA had already clearly shaped the concept of safety and security culture and with and ill-considered "innovation" the assessments will lose that. Furthermore, it will be no use of the more effective integrated campaign, if the message and the concept about the organisational culture is hardly "digestible" and not deliberated.

REFERENCES

[1] SOLYMOSI M., HORVÁTH K. és SOLYMOSI J.: „Combine Nuclear Security and Safety Culture Self-Assessment, Fewer or More?," in *IAEA*, Wien, 2016.

[2] GULDENMUNd, F.: „Understanding and Exploring Safety Culture," Uitgeverij BOXPress, Oisterwijk, 2010.

[3] DOUGLAS BIRCH, R. J. S.: „The Center for Public Integrity: The assault on Pelindaba," 17 03 2015. [Online]. Available: https://www.publicintegrity.org/2015/03/14/16894/assault-pelindaba. [Hozzáférés dátuma: 15 02 2017].

[4] GREEN, J.: „Belgium's nuclear security scares," *Nuclear Monitor,* kötet4552, szám#822, 21 4 2016.

[5] KATAI-URBÁN, L.: „Establishment and operation of system for industrial safety within the Hungarian disaster management," *ECOTERRA: JOURNAL OF ENVIRONMENTAL RESEARCH AND PROTECTION,* kötet11, szám 2, pp. 27-45, 2014.

[6] IAEA, „No. 83: Performing Safety Culture Self-assessments," IAEA, WIEN, 2016.

[7] KUYKENDALL T., KHRIPUNOV, I.: „Examining the Interface Between Nuclear Security Culture and Nuclear Safety Culture," *1540 Compass,* szám8, pp. 34-37, 2015.

[8] BUNN, M., MALIN, M. B., ROTH, N., TOBEY, H. W.: Advancing Nuclear Security: Evaluating Progress and Setting New Goals, Cambridge: President and Fellows of Harvard College, 2014.

[9] IAEA, „Management of the Interface between Nuclear Safety and Security for Research Reactors," 2016.

[10] IAEA, „Self-Assessment of Nuclear Security Culture in Facilities and Activities that use Nuclear and/or Other Radioactive Material," IAEA, Wienna, 2014.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

SÚLYOS BALESETEK KÖVETKEZMÉNYEINEK, ÉS A VÉDELMI INTÉZKEDÉSEINEK RENDSZERBE FOGLALÁSA

SYSTEMATIZATION OF MAJOR ACCIDENT'S CONSEQUENCES AND LINES OF DEFENCE FOR RESPONSE

KÁTAI-URBÁN Irina

(ORCID: 0000-0001-5366-5565)

katai.irina@gmail.hu

Absztrakt

A hazai iparbiztonsági szabályozás egyik feladata az ipari katasztrófák következményeinek elhárítására történő felkészülés, a következmények felszámolásának hatékonyabb végrehajtása, valamint a lakosságvédelmi intézkedések eredményesebb bevezetése. Jelen cikkben a szerző értékelni és rendszerbe foglalja a veszélyes anyaggal kapcsolatos minta baleseti eseménysorainak kiváltó okait és következményeit. Ezt követően rendszerezi az ipari- és környezeti katasztrófák következményeinek elhárítására szolgáló műszaki és vezetési (irányítási) intézkedéseket.

"A mű a KÖFOP 2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Kulcsszavak: *ipari balesetek; lakosságvédelem; katasztrófavédelem, védelmi intézkedések, következmények felszámolása*

Abstract

One of the task of Hungarian industrial safety's regulation is the preparation for the elimination of the consequences of industrial disasters, more efficient implementation of these tasks and more effective introduction of measures related to population protection. The author introduce and summarise the preliminary results of her research activity related to the causes and consequences of reference major accident scenarios. The author of this article will also systematises the technical and control measures for the elimination of the consequences of major industrial and environment disasters (accidents).

Keywords: *industrial accidents; population protection; disaster management, lines of defence, elimination of consequences*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.02.27.

BEVEZETÉS

A globalizálódás és nemzetköziesedés eredményeként hazánk ipari veszélyeztetettsége emelkedő tendenciát mutat. A 2012-évben egységesült katasztrófavédelem - a lakosság élet- és vagyonbiztonságának növelése érdekében – iparbiztonsági jog-, intézmény, eljárás és eszközrendszert épített ki.

Az iparbiztonsági szabályozás keretében alkalmazott hatósági jogosítványok, önkormányzati és üzemeltetői feladatok eredményes teljesítése szükségessé teszi az ipari környezeti katasztrófák következményeinek elhárítására szolgáló felkészülési rendszer továbbfejlesztését.

A katasztrófavédelem iparbiztonsági hatóságai és polgári védelmi szervezetei jelentős előrelépéseket tettek a belső és külső védelmi tervezésével és tervek begyakorlásával kapcsolatos szakfeladatok teljesítésében. A feladatellátás gyakorlatának egységesítése érdekében szükség van azonban a joggyakorlat, az eljárásrend, a módszertan áttekintésére és egységesítésére. E feladat végrehajtásával vonhatók le azok a következtetések, amelyek a szabályozási területen történő felülvizsgálati intézkedések bevezetését teszik lehetővé. Célszerűnek tartom konkrét műszaki ajánlások kidolgozását az ipari katasztrófák következményeinek elhárítására történő felkészülését szolgáló jog-, intézmény-, eljárás és eszközrendszer, továbbá a katasztrófavédelmi feladatrendszer harmonizálására, további egységesítésére, optimalizálására és fejlesztésére.

Jelen cikkemben a Nemzeti Közszolgálati Egyetem (továbbiakban: NKE) kiválósági pályázata keretében végzett kutatásom első lépéseként a felkészülési jog-, intézmény-, eljárás és eszközrendszer értékeléséhez és tervezett optimalizálásához szükséges hatástanulmány bevezető elemzését készítem el.

A cikkben célkitűzésem

- áttekinteni, értékelni és rendszerbe foglalni a veszélyes anyaggal kapcsolatos minta baleseti eseménysorainak kiváltó okait és következményeit.
- rendszerezni az ipari- és környezeti katasztrófák következményeinek elhárítására szolgáló műszaki és vezetési (irányítási) intézkedéseket (benne nemzetközi kitekintés).

A célkitűzések eléréséhez felhasználható módszer a hazai és nemzetközi publikációk, jogi szabályozás, üzemi okmányrendszer, hatósági jogalkalmazás okmányainak értékelése, valamint nemzetközi és hazai összehasonlító elemzések készítése a rendszer optimalizálása érdekében.

A fenti két célkitűzés szerinti kutatás elvégzéséhez szükségesnek tartom a témakört érintő hazai és nemzetközi mértékadó szakirodalom rövid áttekintését.

A HAZAI ÉS NEMZETKÖZI MÉRTÉKADÓ SZAKIRODALOM ÁTTEKINTÉSE

A hazai katasztrófavédelem és azon belül az iparbiztonság fejlesztése összhangban van nemzetközi, európai uniós, valamint az azokra épülő hazai jogi szabályozással, kormányzati stratégiával és hatósági koncepciókkal.

A Kormány 2014-2020 közötti Közigazgatási- és Közszolgáltatás-fejlesztési Stratégiájának 3.8 fejezetében foglalkozik a Jó Állam közigazgatásának tisztességes és hatékony működésével. A dokumentum megfogalmazza, hogy *„Nemzeti érdek, hogy az állam folyamatosan érdemelje ki a polgárok bizalmát: védelmet és biztonságot szolgáltasson számukra.”* [1, 11] Az állam kiemelt kormányzati feladata tehát a lakosság biztonságának és biztonságérzetének növelése.

A kutatási témakör alapvető célja a jó állami működés és kormányzás alapjául, hátteréül és eszközéül szolgáló katasztrófavédelmi és azon belül iparbiztonsági ismeretanyagok és módszerek értékelése és tudományos kutatás útján történő fejlesztése. Ezzel összefüggésben a kutatás célkitűzése - az ipari és környezeti katasztrófák következményei elhárítására szolgáló felkészülési intézkedések eredményességének fokozása által - növelni a katasztrófavédelem iparbiztonsági szervezetrendszerének jogalkalmazási hatékonyságát, amelyhez szabályozási hatásvizsgálati, szervezési és fenntartható fejlődéshez kapcsolódó kutatások adnak keretet.

A kutatásaim összhangban vannak Magyarország Alaptörvénye [2] II. és a XXI. cikkében meghatározott alapjogokkal, és az állam 53. cikkében rögzített különleges jogrendben végzendő veszélyhelyzeti feladataival. Az emberi élet, az egészséges környezet és a vagyonbiztonság védelme érdekében a katasztrófák következményei elleni védekezés rendszerében vizsgálom az ipari- és környezeti katasztrófák káros hatásainak elhárítására szolgáló jog-, intézmény-, eljárás és eszközrendszert, valamint javaslatokat tervezek kidolgozni a rendszer működtetésének optimalizálására.

A kutatás az állam iparbiztonsági hatósági jogalkalmazási feladatai hatékony és egységes ellátásának fejlesztésére irányul. A témakör behatárolása céljából tisztáznunk kell az iparbiztonság fogalmát és feladatkörét. Az iparbiztonság fogalmát Kátai-Urbán Lajos fogalmazta meg, amely a következő: *„Mindazon veszélyes tevékenység (veszélyes üzem) specifikus jog – intézmény és feladatrendszer, eljárás és eszközrendszer, illetve módszertan, amely a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezéssel, a veszélyes áru szállítással, a nukleáris balesetek elhárításával, valamint a létfontosságú rendszerek és létesítmények biztonságával kapcsolatos üzemeltetői, hatósági és önkormányzati feladatok teljesítése útján a lakosság életének, és egészségének, a környezetnek és a létfenntartáshoz szükséges anyagi javaknak és szolgáltatásoknak a magas szintű védelmét szolgálja."* [3, 97]

A kutatásaim a fogalom-meghatározás egyik legfontosabb eleméhez a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezés következménycsökkentési jogintézményeinek alkalmazásához kapcsolódnak. A következménycsökkentési jogintézmények az ipari- és környezeti katasztrófák következményeinek elhárítására történő felkészülést szolgálják. A témakör legfontosabb hazai szabályai a *katasztrófavédelemről szóló 2011. évi CXXVIII. törvényben (továbbiakban: Kat.)* [4] és *a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendeletben (továbbiakban: Vhr.)* [5] találhatók meg. A két jogszabály együttesen alkotja az ún. veszélyes üzemi szabályozást (továbbiakban: veszélyes üzemi szabályozást)., amely a *veszélyes anyagokkal kapcsolatos súlyos baleseti veszélyek ellenőrzéséről szóló 2012/18/EU Tanácsi Irányelvvel* (SEVESO III.) irányelv [6] hazai teljesítését szolgálja.

Kutatási munkám megalapozását biztosította a kutatási témám (súlyos balesetek elleni védekezés felkészülési jogintézményeinek alkalmazása) nemzetközi és hazai írott joganyagának és szakirodalmának feldolgozása. A cikk bevezetőjében már beszámoltam a legfontosabb európai uniós és hazai iparbiztonsági szabályozásról, amelynek iparbiztonsági hatósági és műszaki jogalkalmazását szolgálja katasztrófavédelem „hatósági kódexe" *a katasztrófavédelem központi, területi és helyi szerveit érintő hatósági és szakhatósági tevékenység végzéséről szóló 17/2015. számú BM OKF főigazgatói intézkedés* [7]. Az intézkedés külön mellékletben foglalkozik a súlyos balesetek elleni védekezés iparbiztonsági hatósági és katasztrófavédelmi szakfeladatainak végrehajtási rendjével.

A veszélyes üzemi feladatellátás szabályait tartalmazza még *a katasztrófavédelmi bírság részletes szabályairól, a katasztrófavédelmi hozzájárulás befizetéséről és visszatérítéséről szóló 208/2011. (X. 12.) Korm. rendelet* [8] és *a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény* [9].

Az ipari baleseti nemzetközi és kétoldalú együttműködést alapozta meg az Ipari Balesetek Országhatáron Túli Hatásairól szóló, Helsinkiben, 1992. március 17-én kelt Egyesült Nemzetek Szervezetének Európai Bizottsága keretében létrejött Egyezmény, amelyet a 128/2001. (VII. 13.) Korm. rendelet hirdetett ki [10].

A nemzetközi szakirodalmat vizsgálva megállapítható, hogy a veszélyeztetettség elemzése szempontjából a holland Külső Védelmi Kutatóintézet által kiadott ún. színes könyvek [11] [12] [13] alkalmazása elkerülhetetlen. További eljárási és módszertani kutatási eredmények és adatbázisok találhatók az iparbiztonság alapműveiként is számon tartott külföldi könyvekben, mint a Vegyipari Biztonsági Központ mennyiségi kockázatelemzéséről szóló irányelveiben [14], a londoni kiadású Környezeti Kockázat Elemzés című szakkönyvben [15], a Feldolgozóipari Technológiák Veszteség elemzése [16] című három kötetes munkában.

Az Európai Unió Közös Kutatási Központ olaszországi Isprában lévő Súlyos Baleseti Veszélyek Irodája kiadásában több módszertani útmutató jelent meg, amelyek beépültek a hazai szakmai kiadványokba és útmutatókba. Ilyen útmutató a biztonsági jelentéssel szemben támasztott követelményeket [17] [18] tartalmazó, vagy a hatósági felügyelet szabályait taglaló útmutató [19]. Sajnálatos módon a tagállami jogalkalmazást segítő az üzemi és települési védelmi tervezés végrehajtására vonatkozó uniós módszertani segédlet nem készült.

Az NKE iparbiztonsági tankönyve a veszélyes anyagokkal kapcsolatos súlyos ipari balesetek üzemeltetői és hatósági feladatai végrehajtásához ad eljárási és módszertani útmutatót [20]. A katasztrófavédelem súlyos balesetek elleni területi és helyi feladatainak végrehajtásáról szól - a módszertani értelemben még mindig alkalmazható és a védelmi tervezés szabályait magyarázó - *Módszertani segédlet a veszélyes anyagokkal kapcsolatos súlyos ipari balesetek elleni védekezés területi és helyi feladatainak ellátásához* [21]. Az NKE és jogelődje a Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola szervezésében összesen 15 db iparbiztonsági témájú doktori értekezés és 3 db habilitációs tézisfüzet készült, amelyek szintén iránymutatásul szolgálhatnak kutatómunkám végrehajtásában.

A cikk következő részeiben a nemzetközi és hazai szakirodalmi áttekintést már a konkrét kutatási célkitűzést érintően fogom elvégezni.

A VESZÉLYES ANYAGGAL KAPCSOLATOS BALESETEK KIVÁLTÓ OKAINAK ÉS KÖVETKEZMÉNYEINEK ÁTTEKINTENTÉSE ÉS ÉRTÉKELÉSE

A veszélyes anyagokkal kapcsolatos súlyos balesetek kiváltó okainak és következményeinek értékelését megelőzően fogalmi elhatárolást kell végeznünk, amely kiterjed a katasztrófa, a veszélyes anyagokkal kapcsolatos súlyos baleset és üzemzavar fogalmának részletes értékelésére

Ipari- és környezeti katasztrófák fogalmi értékelése

Az ipari- és környezeti katasztrófák legautentikusabb fogalmi meghatározása kapcsán a katasztrófavédelmi törvény megfogalmazásait hívhatjuk segítségül. A katasztrófavédelmi törvény fogalom-meghatározása szerint a „*Katasztrófa: a veszélyhelyzet kihirdetésére alkalmas, illetve e helyzet kihirdetését el nem érő mértékű olyan állapot vagy helyzet, amely emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit, és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli.”* [4. 3.§ 5.].

A fogalom-meghatározás alapvető jellemzője, hogy az esemény szintjét olyan állapothoz (helyzethez) kapcsolja, amely meghaladja a védekező szervezetek lehetőségeit és különleges intézkedések bevezetését, esetlegesen nemzetközi segítség igénybevételét igényli.

A katasztrófa esemény (törvényi megfogalmazásban helyzet) mértékét a jogalkotó nem határozta meg veszélyforrásonként, ezért az ipari- és környezeti katasztrófa fogalmának értelmezéséhez tovább kell lépnünk a Kat. veszélyes anyagokkal kapcsolatos súlyos baleseti definíciójához.

A Kat. a veszélyes anyagokkal kapcsolatos súlyos baleset fogalma alatt az alábbi szövegezést adja meg: *„Veszélyes anyagokkal kapcsolatos súlyos baleset: olyan mértékű veszélyes anyag kibocsátásával, tűzzel vagy robbanással járó, veszélyes anyagokkal kapcsolatos üzemzavar, amely a veszélyes anyagokkal foglalkozó üzem, küszöbérték alatti üzem működése során befolyásolhatatlan folyamatként megy végbe, és amely az üzemen belül vagy azon kívül közvetlenül vagy lassan hatóan súlyosan veszélyezteti vagy károsítja az emberi egészséget, illetve a környezetet.* [4. 3.§ 29.]

Az előző törvényi fogalom-meghatározásban megadott veszélyes anyag kibocsátásával, tűzzel vagy robbanással járó, veszélyes anyagokkal kapcsolatos üzemzavar súlyos baleseti szintet akkor éri el, ha - a Seveso III. Irányelvi szabályozás szerint - az üzemzavar következményének súlyossága a jelentési küszöböt meghaladja.

A veszélyes anyagokkal foglalkozó üzemeknél különös figyelmet kell fordítani - az eseménynek az Európai Bizottság felé történő jelentési kötelezettség szempontjából – a Vhr. 11. mellékletében megadott mennyiségi és minőségi szempontrendszerre. A törvényi szabályozás teljes mértékben megegyezik a Seveso III. Irányelvben foglaltakkal. A Vhr-ben megadott minőségi és mennyiségi szempontok olyan magas értékeket tartalmaznak, hogy azokat az Európai Unióban a 28 tagállamának több mint 10000 veszélyes üzeme esetében is évente csak 20-30 közötti baleseti eseménynél alkalmazzák. Magyarországon a 270 körüli veszélyes anyaggal foglalkozó üzemet figyelembe véve nagyon ritkán következik be EU jelentési kategóriát elérő szintű esemény, ezért a veszélyes baleseti tapasztalatok rendelkezésre állása érdekében egy alacsonyabb jelentési küszöbre volt szükség.

A Kat. IV. fejezetének hatálya alá tartozó veszélyes tevékenységek jelentési kötelezettségeinek szabályozásához szükség volt az „üzemzavar” szintjének szakmai megállapítására.

Az üzemzavar fogalmát ugyancsak a Kat. tartalmazza, amely szerint a „*veszélyes anyagokkal kapcsolatos üzemzavar: veszélyes anyagokkal foglalkozó üzemben, küszöbérték alatti üzemben a rendeltetésszerű működés során vagy a technológiai folyamatokban bekövetkező olyan nem várt esemény, amely azonnali beavatkozást igényel és az alábbi következmények egyikével jár:*

a) veszélyes anyaggal kapcsolatos tűz,

b) veszélyes anyaggal kapcsolatos robbanás,

c) mérgező, rákkeltő tulajdonságú veszélyes anyag kibocsátása,

d) oxidáló, tűz- vagy környezetre veszélyes tulajdonságú folyadék halmazállapotú veszélyes anyag kikerülése legalább 1000 kg mennyiségben,

e) egyéb veszélyes anyag kikerülése legalább a felső küszöbérték 0,1%-át elérő mennyiségben” [4. 3.§ 30.]

A fogalom-meghatározás kutatásom szempontjából lényegi elemét a rendeltetésszerű működés során vagy a technológiai folyamatokban bekövetkező ún. *„nem várt eseménynek”* a minősítése jelentette. A Kat. 4. 3.§ 30. pontjában jellemzett üzemzavari szintet elérő „nem várt esemény” és a *„súlyos baleset”* szintje közé besorolt valamennyi baleseti esemény jelentéskötelesnek minősül.

A harmadik eseménykategória az ún. *nem sorolt esemény*, amely nem minősül veszélyes anyagokkal kapcsolatos üzemzavarnak, így veszélyes anyagokkal kapcsolatos súlyos balesetnek sem.
Az ilyen események lehetnek az ún. *nem jelentésköteles események* (például a környezetbe került tűzveszélyes folyékony anyag mennyisége nem éri el az 1000 kg-ot; vagy olyan esemény, ami azonnali beavatkozást igényel, veszélyes anyag kibocsátásával nem jár, azonban a veszélyes anyagokkal foglalkozó létesítmény működését korlátozni szükséges. Ide sorolhatóak az egyéb üzemi események is, mint például a munkahelyi baleset, vagy a nem veszélyes anyag jelenlétében bekövetkezett esemény.

Ez utóbbi baleseti minősítési kategória részletes leírását a „hatósági kódex" [7] az iparbiztonsági káreseti helyszíni szemlék eljárási rendjét szabályozó 6. mellékletében találhatjuk meg.

A következő táblázatban összefoglalom az ipari és környezeti katasztrófákkal kapcsolatos végzett fogalmi értékelésem eredményeit:

Megnevezés	Jogforrás	A minősítés fogalmi szempontjai	A minősítés értékelése
Ipari- és környezeti **katasztrófa**	Kat. 3.§ 5.	Minőségi szempontból - olyan **állapot vagy helyzet**, - amely többek között az emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket **olyan módon vagy mértékben veszélyezteti, károsítja**, - hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek védekezési lehetőségeit, - és **különleges intézkedések bevezetését**, - az önkormányzatok és az állami szervek folyamatos és szigorúan **összehangolt együttműködését**, - illetve **nemzetközi segítség igénybevételét igényli**.	A minősítés műszaki paramétereit jogszabály nem tartalmazza. A minősítés szubjektív és széles teret ad a jogalkalmazóknak a veszélyhelyzeti szintű állapot (helyzet) azonosítására. Veszély-forrásonként különböző szempontrendszert lehet alkalmazni.
Veszélyes anyagokkal kapcsolatos **súlyos baleset**	Kat. 3.§ 29. Vhr. 11. melléklet (a Seveso III. alapján)	Minőségi szempontból: - olyan mértékű veszélyes anyag kibocsátásával, tűzzel vagy robbanással járó, veszélyes anyagokkal kapcsolatos **üzemzavar**, - amely a veszélyes anyagokkal foglalkozó üzem, küszöbérték alatti üzem működése során **befolyásolhatatlan folyamatként megy végbe**, - és amely az üzemen belül vagy azon kívül közvetlenül vagy lassan hatóan **súlyosan veszélyezteti vagy károsítja az emberi egészséget, illetve a környezetet**. Mennyiségi szempontokat a Vhr. 11. mellékletében megadott részletes határértékek tartalmazzák.	A veszélyes üzemi szabályozás részletes műszaki paramétereket tartalmaz. A szempontok objektívek, azonban igen jelentős a károsodás mértékét megjelenít határértékek nagysága.
Veszélyes anyagokkal kapcsolatos **üzemzavar**	Kat. 3.§ 30.	Minőségi szempontból: - veszélyes anyagokkal foglalkozó üzemben, küszöbérték alatti üzemben - a rendeltetésszerű működés során vagy a technológiai folyamatokban bekövetkező olyan **nem várt esemény**, - amely **azonnali beavatkozást igényel.** Mennyiségi szempontból: „és az alábbi következmények egyikével jár: a) veszélyes anyaggal kapcsolatos tűz, b) veszélyes anyaggal kapcsolatos robbanás, c) mérgező, rákkeltő veszélyes anyag kibocsátása, d) oxidáló, tűz- vagy környezetre veszélyes folyadék halmazállapotú veszélyes anyag kikerülése legalább 1000 kg mennyiségben,	Mennyiségi és minőségi szempontok konkrétan megállapításra kerültek a magyar veszélyes üzemi szabályozás szerint.

		e) egyéb veszélyes anyag kikerülése legalább a felső küszöbérték 0,1%-át elérő mennyiségben”	
Nem jelentésköteles egyéb üzemi esemény	17/2015. BM OKF főig. int. 6. melléklete	Minőségi szempontok - **nem jelentésköteles események**; - vagy **egyéb üzemi esemény** (például: munkahelyi baleset, nem veszélyes anyag jelenlétében bekövetkezett esemény).	A BM OKF belső szabályozójában megadott szempontok szerinti eseménytípus. Üzemeltetőt jelentési kötelezettség nem terheli.

1. táblázat: ipari és környezeti katasztrófákkal kapcsolatos végzett fogalmi értékelés, saját készítés

A táblázat további értékelésének eredményeként megállapíthatjuk, hogy a Kat. IV. fejezetének hatálya alá tartozó üzemben veszélyes anyaggal kapcsolaton nem várt üzemi esemény akkor minősül „üzemzavarnak”, ha azonnali beavatkozást igényel, és különböző következményekkel jár (tűz, robbanás, veszélyes anyag kibocsájtása és kikerülése).

Az „üzemzavar” súlyos balesetnek minősítéséhez szükséges, hogy az esemény befolyásolhatatlan folyamat eredménye legyen és a baleset az egészséget, a környezetet, illetve az anyagi javakat súlyosan veszélyezteti, vagy károsítja.

A „súlyos baleset” fogalmi elemei közül jelen kutatás szempontjából lényeges kiemelni a *„súlyos veszélyeztetés”* meghatározását, amelyet a következő hatások szerint tudunk jellemezni:

- emberi életet- és egészséget veszélyeztető lehetséges veszélyes üzemen belüli, vagy kívüli következmények;
- az emberi életet- és egészséget veszélyeztető lehetséges következmények és emberek csoportját érintő társadalmi zavar;
- a környezeti elemeket (a levegőt, a felszíni- és felszín alatti vizeket, a talajt) jelentős mértékben károsító lehetséges következmények;
- az anyagi javak (épített környezet) üzemen belül vagy kívül történő súlyos károsodása.

A veszélyes anyagokkal kapcsolatos baleset vagy üzemzavar bekövetkezésénél *az esemény jellemzőinél* figyelembe kell még venni következőket:

- a kialakult tűznek, vagy robbanásnak a veszélyes anyaggal kapcsolatos érintettségét,
- a kikerült veszélyes anyag mennyiségét és halmazállapotát,
- a kikerült veszélyes anyag tulajdonságát (mérgező, rákkeltő, oxidáló, tűz- vagy környezetre veszélyes, sugárzás fajtája és veszélyességi kategóriája),
- az emberi életben és anyagiakban, illetve a természeti elemekben (talaj, víz) okozott kár, valamint a munkavállalók, a lakosság és a környezet sugárterhelésének becsült mértékét.

Az *esemény minőségi és mennyiségi értékeléséhez* a szükséges mértékben ismerni kell továbbá:

- az eseményben érintett veszélyes létesítmény, üzemi technológia, vagy berendezés kialakítását, működését, technológiai paramétereit (hőmérséklet, nyomás, stb.) és karbantartottságát,
- az esemény feltételezett kiindulási helyzetét és az esemény kialakulásának folyamatát, az esemény kezelése során tett üzemeltetői intézkedéseket,
- az eseményt előidéző okokat, az esemény kialakulását befolyásoló tényezőket, az eseményben érintett veszélyes anyagok fizikai és kémiai jellemzőit,

- az esemény következményeinek és hatásainak (személyi sérülés/halál, anyagi kár, környezetszennyezés, belső, vagy külső dominóhatás, stb.) részletes leírását,
- a normál üzemtől való eltérés, illetve esetlegesen az arra való visszaállás tényét, befolyásoló körülményeit.

A következőkben a súlyos balesetek kiváltó okainak és következményeinek értékelését fogom elvégezni.

Súlyos balesetek kiváltó okainak, baleseti eseménysorainak és következményeinek átfogó értékelése és rendszerezése

A korszerű fejlett államokra jellemző veszélyes üzemi szabályozás a veszélyes üzemek biztonságos üzemeltetése, valamint a veszélyes üzem környezetében élő lakosság és közvetlen környezetének magas szintű védelme érdekében a veszélyes tevékenységet üzemeltető gazdálkodó szervezet feladatává teszi, az általa üzemeltetett veszélyes tevékenységet végző telephely iparbiztonsági hatósági engedélyezését.

A veszélyes üzemi szabályozás alapján az iparbiztonsági hatóság - építési és veszélyes tevékenység megkezdési hatósági eljárás keretében - az üzemeltető által benyújtott biztonsági dokumentáció valóságtartalmát vizsgálja. Az adott üzem státusza alapján előírt biztonsági dokumentáció (biztonsági jelentés és elemzés, súlyos káresemény-elhárítási terv) üzemeltető általi elkészítésének célja többek között bemutatni és bizonyítani azt, hogy az üzemeltető

- azonosította (elemezte és minősítette) a veszélyes üzem által okozott súlyos baleseti veszélyeztetettséget, valamint
- bevezetett minden védelmi intézkedést, amely a súlyos balesetek megelőzése, és azok emberi életre és egészségre, a környezeti elemekre és az anyagi javakra gyakorolt káros következményeinek csökkentése érdekében szükséges.

Az üzemeltető - a súlyos baleseti veszélyeztetettség elemzésére alapozva - elkészíti és alkalmazza a veszélyes üzem belső védelmi tervét, amely a külső települési védelmi tervezéshez szükséges információt is tartalmazza.

A veszélyes üzemi *veszélyeztetettség elemzésnek* ki kell térnie a következő fontos elemekre:

- a lehetséges súlyos baleseti eseménysorok belső és külső kialakulási feltételeinek (okainak) és bekövetkezési valószínűségének részletes leírása;
- az azonosított súlyos baleseti veszélyek súlyosságának és lehetséges következményeinek értékelése;
- a veszélyes létesítmények biztonságos üzemeltetéséhez szükséges műszaki feltételek és alkalmazott eszközök leírása;
- a súlyos baleseti események következményeinek csökkentéséhez szükséges védelmi intézkedések.

A veszélyes üzem *belső védelmi tervének* az alábbi tartalmi feltételeknek kell megfelelni:

- a súlyos balesetek következményeinek csökkentését szolgáló eszközök és felszerelés rendelkezésre állásának leírása;
- a riasztás és a beavatkozási intézkedések kialakításával kapcsolatos információ;
- a belső és a külső felhasználható erőknek és eszközöknek a leírása.

Papadakisnak és Amendolának a Seveso II. Irányelv teljesítését szolgáló biztonsági jelentés elkészítési útmutatóban [17] megadott eljárási lépései valamennyi nemzetközileg alkalmazott veszélyeztetettség elemzési eljárásnál megtalálható, amely magában foglalja

- veszélyazonosítást;

- a baleseti eseménysorok azonosítását;
- az eseménysorok bekövetkezési valószínűségének értékelését;
- az eseménysorok következményének értékelését;
- a kockázatok rangsorolását;
- a biztonsági rendszerek megbízhatóságának és alkalmazhatóságának elemzését.

A *veszélyazonosítási módszerek* számos fajtáját ismerjük, amelyek alkalmazását a veszélyazonosítás célja, az elemzés várható eredményeinek rendeltetése, rendelkezésre álló információ, az elemzett eljárások sajátosságai, a felhasználható személyi és technikai erőforrások megléte határoz meg. Ilyen módszer lehet például az ellenőrző jegyzék; a relatív osztályozás (relative ranking) módszere, az előzetes kockázatelemzés, a veszély és működőképesség elemzés - HAZOP, a hibamód és hatás elemzés - FMEA elemzés, a hibafa elemzés, az eseményfa elemzés, valamint az ok- és következményelemzés.

Súlyos baleseti eseménysorok azonosítása a veszélyazonosítás és a kockázatelemzés közötti kapcsolatot hozza létre többségében minta baleseti eseménysorok formájában. A minta súlyos baleseti eseménysorokat alkalmazhatjuk a védelmi intézkedések (barriers – védelmi zárak) megfelelősségének vizsgálatára, a védelmi tervek és településrendezési tervek kidolgozásához egyaránt.

Az üzemeltetőnek a lehetséges súlyos baleseti eseménysorok és azok kezdeti eseményeinek (okok) módszeres meghatározásával bizonyítania kell a megtett védelmi intézkedések megfelelőségét. Az eseménysorok általában a veszélyes anyag kibocsátással járó események feltételezésén alapulnak.

A biztonsági jelentésben szerepeltetendő súlyos baleseti eseménysor rendszerint leírja a veszélyes anyag kiszabadulásának módját (műszaki jellegét), amely lehet tartálytörés; csővezeték-törés; veszélyes anyag tároló edény kilyukadása. Megadja továbbá a kiváltott esemény hatását is, így a tüzet; a robbanást és a veszélyes anyagok kibocsátását (szabadba kerülését).

A súlyos baleseti eseménysorok és kiváltó okainak jellemzésére széleskörűen elterjedt módszer az ún. *csokornyakkendő ábra*. Az ábra közepe jelöli a készülékből való veszélyes anyag kibocsájtás eseményét az ún. csúcseseményt. A csokornyakkendő ábra bal oldala ábrázolja a csúcsesemények bekövetkezéséhez vezető lehetséges okok teljes körét. A hibafa veszélyazonosítási módszerhez kapcsolódnak az ún. megelőzési kockázatcsökkentő intézkedések. A csokornyakkendő ábra jobb oldala a csúcseseményből kiinduló lehetséges végesemények kialakulását mutatja. Az eseményfa módszerrel állapíthatjuk meg a lehetséges súlyos baleseti eseménysorok következményeit, azok emberi egészségre káros hatásait, valamint a következmények csökkentésére szolgáló intézkedéseket.

A mértékadó szakirodalmi hivatkozások [11] [15] [20] összevetése alapján *a veszélyes anyag kibocsájtásával járó baleseti eseménysorok* fajtái az alábbiak:

- tócsatűz (pool fire);
- villanótűz (flash fire);
- tartálytűz;
- szúróláng;
- VCE (párolgó gőz/gázfelhő-robbanás);
- mérgező felhő terjedése;
- BLEVE (forrásban levő folyadék táguló párarobbanása);
- talaj-, levegő- és víz szennyezés.

A fenti események általában a technológiai egységeknél; a tároló berendezéseknél; a csővezetékeknél; a töltő és lefejtő létesítményeknél; a veszélyes anyagok üzemen belüli szállítása során következnek be.

A lehetséges balesetek kiváltó okainak egy lehetséges csoportosítási lehetőségét a következő felsorolásban mutatom be:

- *Az üzemeltetésre visszavezethető okok* lehetnek a fizikai és a kémiai folyamatok jellemzőinek határértékei; az adott üzemmódból (indítás vagy leállítás) következő veszélyek; a veszélyes anyagnak a készülékből való kiszabadulásának lehetősége; a berendezések és a rendszerek rendellenes működése és műszaki meghibásodásai; a létesítmények közötti belső eszkalációs hatás; a kiszolgálórendszerek meghibásodása; az üzemeltetéssel és a karbantartással összefüggő emberi tényezők; a kémiai összeférhetetlenség és szennyeződés; a gyújtóforrások jelenléte.
- *A belső okok* között tartjuk számon a veszélyes létesítményekben bekövetkező tüzek, robbanások vagy veszélyes anyagok szabadba kerülésével járó kezdeti eseményeket, amelyek normál üzemmenetére is káros hatással lehet.
- A *külső okok* közül főleg a következőket veszik figyelembe:
    - dominóhatással érintett veszélyes üzemek súlyos baleseteinek hatásai (tűz, robbanások, toxikus anyag szabadba jutása), vagy más nem veszélyes tevékenységek és a szállítási hálózatok fizikai hatásai;
    - a veszélyes anyagok telephelyen kívüli szállítása, mint például közutak, vasutak, csővezetékes szállítás, vízi szállítási útvonalak, olaj- vagy gázátadó állomások, légi szállítási útvonalak, stb.);
    - szomszédos üzembeli tevékenységekhez tartozó létesítményektől való funkcionális, kölcsönös függés, mint például veszélyes áru szállítási csővezetékek vagy más közös szolgáltatások (gőzszolgáltatás);
    - természeti veszélyforrások, mint a (rendkívüli) csapadék (eső, hó, jégeső), szél, szélviharok, villámcsapás, árvizek, fölcsuszamlások, szeizmikus aktivitás, stb. (Natural Hazard Triggering Technological Disasters - NATECH);
    - *Egyéb baleseti okok* eredhetnek a tervezésből, az építésből és a biztonsági irányítási rendszer működéséből, amelyek kapcsolódhatnak az üzemi életciklushoz, az üzembe helyezéshez, a leállításhoz, a berendezések vagy a termelési folyamat átalakításához, a karbantartáshoz, stb. [15]

A veszélyes üzemi *következményelemzés* célja a műszaki, illetőleg vezetési és szervezési jellegű intézkedések kidolgozása és bevezetése a súlyos baleseti események kialakulásának megakadályozása és/vagy a baleseti következmények csökkentése, továbbá a következménycsökkentő intézkedések hatékonyságának és megfelelőségének értékelése érdekében. A következményelemzés információt szolgáltat a külső védelmi tervezéshez és a településrendezési tervezéshez is. Az értékelés eredményeit „térképek, képek és leírások” formájában kell bemutatni.

A súlyos baleset következményeinek modellezéséhez általában bemeneti adatokra van szükség, mint például a veszélyes anyagok fizikai és kémiai tulajdonságai (tűzveszélyesség, toxicitás, stb.); emissziós potenciál (hősugárzás, túlnyomás); szabadba jutási jellemzők (mennyiség, halmazállapot, stb.) és az időjárási körülmények. E modellszámítás eredményeit a (potenciális) hatás súlyosságának függvényében adják meg. A biztonsági jelentéseknél a potenciális hatást általában az emberi egészségkárosodás függvényében fejezik ki, bár relatív anyagi vagy környezeti károkat is meg lehet adni.

A hatás súlyosságának mérésére használatos a károsodási probit görbe; és a rögzített károsodási küszöbértékek.

AZ IPARI- ÉS KÖRNYEZETI KATASZTRÓFÁK KÖVETKEZMÉNYEINEK ELHÁRÍTÁSÁRA SZOLGÁLÓ VÉDELMI INTÉZKEDÉSEK RENDSZEREZÉSE

Jelen fejezet célja a tanulmány bevezetőjének alapján rendszerezni az ipari- és környezeti katasztrófák következményeinek elhárítására szolgáló műszaki és vezetési (irányítási) intézkedéseket (összefoglalóan védelmi intézkedéseket).

A veszélyes anyag kibocsájtásával járó események *következményeinek csökkentésére szolgáló intézkedéseket* céljuk szerint három csoportba oszthatjuk:

- a környezetbe kibocsájtott veszélyes anyag mennyiségének csökkenése, amely függ a veszélyes anyag és a kibocsájtás fajtájától (például: vészhelyzeti leállító rendszerek, vízfüggönyök, tócsaméret csökkentés és habtakarás);
- az esemény kiterjedésének megakadályozása, amelyet főként a tűz- és robbanásveszélyes anyagok eseményeinél alkalmazhatunk;
- az esemény környezetében lévő emberek és infrastruktúra védelmére az elzárkózási vagy a kimenekítési intézkedés szolgálhat, amely a rendelkezésre álló időtartamtól függ.

Az Európai Bizottság Közös Kutatási Központ által készített útmutató [18] alapján a veszélyes létesítményben a megelőzéssel, az irányítással és a káros hatások csökkentésével kapcsolatos intézkedések lehetnek:

- folyamatirányító rendszer, beleértve a tartalékrendszereket is;
- tűz- és robbanásvédelmi rendszerek;
- a véletlenszerű kibocsátások mértékét korlátozó berendezések, mint például mosórendszerek, sprinklerek;
- gőzszűrők, vészhelyzeti leválasztó-edények, illetőleg gyűjtőedények, és vészhelyzeti elzáró-szelepek;
- riasztórendszerek, beleértve a gázérzékelőket is;
- automatikus leállító rendszerek;
- inertizáló rendszerek;
- meghibásodás-biztos műszerezés;
- vészhelyzeti szellőztetés, beleértve a robbanásra nyíló felületeket is;
- gyorsleállítás és egyéb vészhelyzeti eljárások;
- a berendezésnek a nem engedélyezett tevékenységek elleni védelmével kapcsolatos speciális megelőzési rendszabályok.

A felsorolás nem kimerítő jellegű, továbbá nem tartalmazza a megelőzési és következménycsökkentési intézkedések megfelelő elhatárolását.

A veszélyeztetettség elemzés szempontjából figyelembe veendő *védelmi intézkedéseket* típusuk szerint az alábbi csoportokra oszthatjuk:

- a *passzív* intézkedésekre, amelyek a technológiai folyamat állapotától független, állandóan hatást kifejtő intézkedéseknek minősülnek, valamint
- az *aktív* intézkedésekre, amelyek tovább bonthatók
    - a folyamatot megszakító beavatkozásokra (a műveletek végrehajtását akadályozó reteszrendszerek, mint például biztonságos technológiai üzemeltetési előírások) vagy
    - beindítanak egy vagy több védelmi tevékenységet, mint például nyomáscsökkentő szelep kinyitása, vagy a vészleállítás.

A kockázatcsökkentő (védelmi) intézkedések részletes csoportosítását a következő táblázat mutatja be.

Az intézkedés típusa		Az intézkedések jellemzése
Műszaki intézkedések	Passzív műszaki intézkedések	Nincs szükség a biztonsági funkciót működtető mechanizmusra. Például a tartály körüli kármentő, melyet a teljes anyagmennyiség befogadására terveztek. Viszonylag nagy megbízhatósággal üzemeltethetők.
	Aktív műszaki intézkedések	Külső energiaforrást igényelnek a biztonsági funkciójuk ellátásához, azonban emberi beavatkozás nélkül üzemelnek (például: automatikus leállítás, vészhűtő-rendszerek)
Üzemi magatartási rendszabályok	Passzív magatartási rendszabályok	A meghatározott üzemi területek esetében rezsimszabályokat léptetnek életbe. A rendszabály önmagában alkotja az intézkedést, anélkül, hogy bármilyen műszaki intézkedést igénybe vennének (például védőtávolságok, üzemi elzárt területek, nyílt lángot kizáró terület)
	Aktív magatartási rendszabályok	A veszélyes létesítményrészen követendő kötelező magatartási szabályokat határozza meg. (Például kiürítési intézkedés mérgezésveszély- vagy tűzriadó esetén vagy a vegyszerek kezelésénél előírt munkavédelmi vagy tűzvédelmi előírások).
Vegyes intézkedések		Műszaki intézkedések és magatartási rendszabályok kombinációja. Az aktív intézkedések kombinációja a legfontosabb, mert azok kölcsönhatásban vannak (például riasztásira történő üzemleállítási eljárások)

2. táblázat védelmi intézkedések (lines of dedence), készítette a szerző, forrás: [18]

A *kockázatcsökkentő intézkedéseket* Hoffmann Imre PhD értekezésében [22] három osztályba sorolta, amelyekre jellemző információt a következő táblázat foglal össze és pontosít:

Intézkedés célja	Intézkedés típusa	Példák bemutatása
A súlyos ipari baleset bekövetkezési gyakoriságát csökkentő intézkedések.	Technológiai rendszer módosítását igénylő intézkedések.	Ilyenek lehetnek például a technológia váltás; biztonsági szerelvények beépítése; flexibilis vezeték cseréje nem flexibilisre, kármentő létesítése. átmeneti tartályok kivétele a rendszerből.
	Szervezési intézkedések.	Például egyes szerelvények fokozott ellenőrzése; veszélyes anyagok mennyiségének racionalizálása; logisztikai folyamatok racionalizálása; oktatás, képzés.
	Humán intézkedések.	Például: létszámbővítés; szakértők alkalmazása.
A súlyos ipari baleset következményeit (hatásait) csökkentő intézkedések A szabadba kerülő veszélyes anyagok mennyisége, terjedési távolsága, illetve káros hatása csökkenthető.	Technológiai rendszer módosítását igénylő intézkedések.	Ilyenek lehetnek például: veszélyes anyag mennyiségének csökkentése az adott rendszerben; technológiai paraméterek – nyomás, hőmérséklet – változtatása.
	Szervezési és humán intézkedések.	Például: létesítményi tűzoltóság működtetése; egyéb védelmi szervezet létrehozása; kiszakaszolási tervek kidolgozása; oktatás, képzés; létszámpótlási terv kidolgozása.
	Védelmi tervezés.	Hatékony védelmi tervezés az adott rendszerre vonatkozóan, erő-eszköz kidolgozása; védelmi tervezés a kockázatok által érintett helyre (vizsgálati pontra) vonatkozóan, erő-eszköz kidolgozása.
	Beavatkozás.	Stabil védelmi rendszer kiépítése; monitoring rendszer kiépítése; speciális, a kiválasztott eseménysor következményeit csökkentő védelmi eszközök beszerzése és alkalmazása; közös gyakorlatok, rendszeres üzemi szintű gyakorlatok.
Egyéb intézkedések	Az egyéb intézkedések kategóriájába sorolhatunk minden olyan intézkedést, amely a másik két kategóriába nem illetve mindkettőbe egyaránt besorolható.	Néhány példa: veszélyes anyagok mennyiségének küszöbérték alá való csökkentése; veszélyes technológia zárt helységbe való betelepítése.

3. táblázat kockázatcsökkentő intézkedések rendszere, készítette a szerző, forrás: [22]

Hasonló csoportosítást találhatunk Grafjódi István PhD doktori értekezésében [23] is, ahol a szerző a kockázatcsökkentési intézkedéseket szakértői elemzések (eredmények) és a nemzetközi szakirodalomi hivatkozások [11, 14] tanulmányozása alapján három osztályba sorolta be:

- kockázat (veszély) kizárása vagy csökkentése (tervezési biztonság, inherent safety);
- a következmények csökkentése;
- és a gyakoriság (bekövetkezési valószínűség) csökkentése.

Az intézkedések lehetnek passzív, aktív, eljárási vagy tervezési jellegűek.

A tervezési biztonság (az angol terminológia szerint: inherent safety) szabálya szerint az ipari tevékenységek (létesítmények) egyszerűvé, felhasználó baráttá és alapvetően alacsony kockázatúvá tételével kell a veszélyeket kiküszöbölni és a kockázatot csökkenteni. A kockázatcsökkentés lehetséges módszere lehet az

- intenzifikálás: a veszélyes berendezések számának csökkentése;
- helyettesítés: veszélyes anyagok helyettesítése kevésbé veszélyesekkel;
- a baleseti hatás csökkentése: a veszélyes anyagok vagy folyamatok potenciális veszélyének behatárolása mellett történő alkalmazása (például a veszélyes anyag biztonságos oldószerben oldva, alacsony hőmérsékleten és nyomáson tárolva);
- egyszerűsítés: az üzem és a folyamatok egyszerű tervezése, kivitelezése és működtetése, így kevesebb felszerelés, ellenőrzés és emberi hiba várható.

A nemzetközi szakirodalom elemezése alapján a következménycsökkentő intézkedések közé sorolhatjuk azokat az intézkedéseket, amelyek akkor alkalmazhatók, ha egy veszélyforrás pénzügyi, folyamatirányítási vagy egyéb okokból nem küszöbölhető ki. Ebben az esetben megoldást jelenthet a következmények súlyosságának csökkentése. Ilyen intézkedés például: távirányítású szelepek alkalmazása; csőátmérő csökkentése; technológiai jellemzők csökkentése; a vészlefúvató biztonsági rendszerek; a tűz oltására vagy lehatárolására az elárasztó rendszerek és habágyúk; gőz- vagy vízfüggönyök mérgező gázok kimosására; tűzálló építmények; robbanásálló falak; együttárulási szabályok alkalmazása; zárt üzemépületek kialakítása. Ezek az intézkedések a csokornyakkendő ábra jobb eseményfa oldalán működhetnek.

A baleseti események bekövetkezési gyakoriságát csökkentő intézkedések lehetnek például a korrozív hatású anyagok alkalmazásának csökkentése; karimás csatlakozások mennyiségének minimalizálása; szilárdsági méretezések fémszerkezeteknél; nem korrodáló anyagok alkalmazása; megerősített védelem egyes berendezéseknek (dupla falú csővezetékek vagy szelepek alkalmazása); vészleállító rendszerek alkalmazása; tartalék védelmi rendszer beépítése; gáz érzékelők beépítése mérgező vagy tűzveszélyes anyagok monitoringozására; hatékony biztonsági irányítási rendszer alkalmazása. Az utóbb csoporthoz tartozó intézkedések a csokornyakkendő ábra bal oldalához tartoznak. [23]

KÖVETKEZTETÉSEK

A cikk első felében áttekintettem és rendszerbe foglaltam a veszélyes anyaggal kapcsolatos minta baleseti eseménysorainak kiváltó okait és következményeit. Erre alapozva a cikk második felében rendszereztem ipari- és környezeti katasztrófák (súlyos balesetek) következményeinek elhárítására szolgáló műszaki és vezetési (irányítási) intézkedéseket. A munkám során a vizsgált témában mértékadónak számító hazai és nemzetközi szakirodalmat áttekintettem és értékeltem.

A kutatás első elemének végrehajtását követően az egyes fejezeteknél bemutatott részeredményeken túl, az alábbi általános következetésekre jutottam:

- megállapítható, hogy az ipari- és környezeti katasztrófák, illetve a súlyos balesetek fogalmi meghatározásai alapján a súlyos baleseti események minősítéséhez részletes minőségi és mennyiségi értékelési szempontok állnak a hatóságok rendelkezésre;
- a súlyos balesetek kiváltó okait a súlyos baleseti minta eseménysorok kapcsolják össze a súlyos baleseti következményekkel, valamint azok emberre és környezetre veszélyes hatásaival;
- a súlyos baleseti minta eseménysorok belső védelmi tervezéshez történő alkalmazásához szükséges azok mennyiségi és minőségi jellemzésére, amely további kutatás tárgyát képezi;
- a súlyos baleseti védelmi intézkedések az ún. csokornyakkendő ábra alapján hiba- és eseményfa modellek alkalmazásával szemléltethetők;
- a súlyos baleseti védelmi intézkedések létesítmény- és berendezés specifikus jellemzőket tartalmaznak, ezért általános rendszerezési eljárások alkalmazhatók.

A kutatás eredményei felhasználhatók az NKE KVI katasztrófavédelmi alap- és mesterképzés ipari és környezeti katasztrófák elhárítására történő felkészülés - védelmi tervezési és balesetelhárítási szakfeladatokkal foglalkozó - iparbiztonsági tantárgyai tananyagának fejlesztéséhez.

FELHASZNÁLT IRODALOM

[1] A Kormány 2014-2020 közötti Közigazgatási- és Közszolgáltatás-fejlesztési Stratégiája. http://www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf (letöltve: 2016.12.28.)

[2] Magyarország alaptörvénye. (2011. április 25.). https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100425.ATV. (letöltve: 2016.08.08.)

[3] KÁTAI-URBÁN Lajos: Súlyos ipari balesetek megelőzését és a felkészülést célzó jogintézmények egységes rendszerbe foglalása. Hadmérnök IX. 4. (2014). 94-105. o.

[4] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[5] 219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

[6] 2012/18/EU (Seveso III.) Irányelv az Európai Parlament és a Tanács a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről

[7] A katasztrófavédelem központi, területi és helyi szerveit érintő hatósági és szakhatósági tevékenység végzéséről szóló 17/2015. számú BM OKF főigazgatói intézkedés

[8] 208/2011. (X. 12.) Korm. rendelet a katasztrófavédelmi bírság részletes szabályairól, a katasztrófavédelmi hozzájárulás befizetéséről és visszatérítéséről

[9] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

[10] 128/2001. (VII. 13.) Korm. rendelet az Ipari Balesetek Országhatáron Túli Hatásairól szóló, Helsinkiben, 1992. március 17-én kelt Egyesült Nemzetek Szervezetének Európai Bizottsága keretében létrejött Egyezmény kihirdetéséről

[11] Committee for the Prevention of Disasters. CPR 18E. Guidelines for Quantitative Risk Assessment. The Director-General of Labour, The Netherlands, TNO (1999, Purple Book).

[12] Committee for the Prevention of Disasters. CPR 16E, Methods for the Determination of Possible Damage, 3 rd edition. The Director-General of Labour, The Netherlands, TNO (1989, Green Book).

[13] Committee for the Prevention of Disasters. CPR 14E, Methods for the Calculation of Physical Effects., 3 rd edition. The Director-General of Labour, The Netherlands, TNO (1997, Yellow Book).

[14] Center for Chemical Process Safety: Guidelines for Chemical Process Quantitative Risk Analysis. A.I.Ch.E., NY. ISBN 0-8169-0402-2.; (CCPS) Center for Chemical Process Safety (1989).

[15] FAIRMAN; MEAD; WILLIEMS: Environmental Risk Assessment. Monitoring and Assessment Research Centre, King's College London; ISBN 92-9167-080-4

[16] LEES, F. P., Loss Prevention in the process Industries, Second Edition, Butterworth-Heinemann, London. ISBN 0-7506-1547-8. (1996).

[17] PAPADAKIS G. A.; AMENDONA A,: Guidance on the preparation of a safety report to meet the requirements of Council Directive 96/82/EC (SEVESO II) JRC EC, Ispra Italy, 1997.

[18] FABBRI L., STRUCKL M. és WOOD M.: Guidance on the preparation of a Safety Report to meet the requirements of Directive 96/82/EC as amended by Directive 2003/105/EC (SEVESO II). Ispra, 2005. ISBN 92-79-01301-7

[19] GEORGIOS A. PAPADAKIS G. A., PORTER S. (ed.): Guidance on Inspections as required by article 18 of the council directive 96/82/ec (seveso ii). Luxembourg, 1999. ISBN 92-828-5898-7

[20] BOGNÁR B. at. all: Iparbiztonságtan I, Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 564 p.

[21] BÍRÓNÉ ŐSZ J. at. all.: Módszertani segédlet a veszélyes anyagokkal kapcsolatos súlyos ipari balesetek elleni védekezés területi és helyi feladatainak ellátásához. Budapest: Akaprint Kft., 2005. 116 p. (ISBN:963 218 561 7)

[22] HOFFMANN I.: A védelmi tervezés és a kockázatcsökkentés jelentőségének kutatása a súlyos ipari balesetek elleni védekezésben. PhD értekezés, ZMNE, Budapest 2007.

[23] GRAFJÓDI I.: A súlyos ipari balesetek megelőzését és következményeinek csökkentését szolgáló műszaki és gazdasági eszközök és eljárások kutatása-fejlesztése. PhD értekezés, ZMNE, Budapest 2007.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

BESONDERE WASSERNEBELLÖSCHER

SPECIAL WATER MIST EXTINGUISHING SYSTEMS

KUTI Rajmund

(ORCID: 0000-0001-7715-0814)

kuti.rajmund@sze.hu

Absztrakt

Nachdem die Aspekte des Umwelt- und Sicherheitsbewusstseins in den Vordergrund geraten sind, kann man sowohl bei der Prüfung von Brandfällen als auch bei Verkehrs- und Industrieunfällen feststellen, dass diese sowohl für die Luft, den Boden, die Gewässer als auch für die gebaute humane Umwelt erhebliche verschmutzende Wirkung haben können. Die Bestrebungen auf die Forschung, Entwicklung und praktische Einführung von neuen Löschtechnologien sowie auf die Minimierung der Umweltschäden des Brandlöschens sind ununterbrochen. Die schnelle, wirksame und umweltfreundliche Brandbekämpfung mit optimierter Löschmittelverwendung ist also von besonderem Belang. Das Wasser, als umweltfreundliches Löschmittel wurde wieder in den Vordergrund gestellt: die Forscher haben mehrere Löschgeräte optimiert, die auf einer speziellen Anwendung von Wasser, nämlich auf der Herstellung von Wassernebel basieren. Anlagen dieser Art sind zum Beispiel die turboreaktiven Löscher, in deren Entwicklung sich die ungarischen Ingenieure unschätzbare Verdienste erworben haben: der erfolgreiche Einsatz dieser Anlagen hat die Aufmerksamkeit der Welt auf Ungarn gelenkt. Ziel des vorliegenden Aufsatzes ist es, diese Anlagen vorzustellen und die Wichtigkeit der ungarischen Entwicklungen zu betonen. Ferner werden die Vorteile der Anwendung von Wassernebel in der Brandbekämpfung vorgestellt

Schlüsselwörter: *Brandbekämpfung, Wassernebel, Löschwirkung, Löscheffizienz, Turbolöscher*

Abstract

Investigating either fires, transportation or industrial accidents with the privilege of environment and safety consciousness it is statable that they can have serious contamination consequences to air, soil, water and also the artificial human environment. The efforts are continuous to research, develop and implement new technologies and to decrease environmental damages of fire-fighting. Environmental friendly fire-fighting solutions are very important with the use of quick, effective materials having beneficial effects. Use of water as an environmental friendly fire-fighting material have been reemerged recently, several fire extinguishers have been improved using a special feature of water, making or generating water fog. Examples for this equipment are the so called turbo reactive extinguishers, where Hungarian engineers had been gathered such amount of credits in development and successful applications that had been driven the attention of the World to our country. I introduce these instruments in my paper emphasizing the importance of the Hungarian R&D activities. In addition, I describe the benefits of using water fogs for fire-fighting.

Keywords: *fire-fighting, water fog, extinguishing effect, fire-fighting efficiency, turbo reactive extinguisher*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.22.

EINLEITUNG

Im XX. Jahrhundert hat die Entwicklung der chemischen Industrie die Erforschung und die Anwendung neuer Löschmittel (Löschschaum, Löschpulver) gefördert. Infolge dessen wurde Weiterentwicklung des Löschens mit Wasser in den Hintergrund gedrängt, obwohl es absehbar war, dass dieses Verfahren noch viel Potenzial bergen würde.

Nach dem Beitritt Ungarns in die EU mussten die nationalen Umweltvorschriften verschärft werden [1], wodurch die Anwendung von Wasser wieder in den Vordergrund gestellt wurde. [2] Es wurde eine Reihe von Brandbekämpfungsversuche mit Wasser angefangen. Die chemischen Eigenschaften von Wasser, nämlich dass es sich gegenüber anderen Stoffen (mit wenigen Ausnahmen) neutral verhält und nicht giftig ist, sprechen ebenfalls für seine Anwendung. Es wurde nachgewiesen, dass je nach Anwendungsart ungefähr die Hälfte des Löschwassers bei der Brandbekämpfung abfließt und Sekundärschäden anrichtet.

Bezüglich der Entwicklungsrichtung kristallisierten sich im Zuge der Versuche zwei Probleme aus:

- Erhöhung der Löscheffizienz, Minimierung des abfließenden Löschwassers
- Aufnahme, Reinigung und Wiederverwendung des abfließenden Wassers

Die Steigerung der Löscheffizienz bietet eine Lösung auch für die Aufnahme des Löschwassers, die Forschungen wurden daher in diese Richtung vorangetrieben. Die Löscheffizienz kann durch Zerstäuben des Wassers erhöht werden [3]. Die perfekteste Zerstäubung kann durch Anwendung von Wassernebel-Löschsysteme erreicht werden. Die Forschungen wurden primär im Hinblick auf die Brandbekämpfung geführt, aber aufgrund der positiven Erfahrungen wurde die Anwendbarkeit von Wassernebel später auch in anderen Gebieten, in breiten Kreisen geprüft.

HERSTELLUNG UND ANWENDUNG VON WASSERNEBEL

Mit verschiedenen Düsensystemen kann man schon seit langem einen feinen, nebelartigen Wasserstaub herstellen, wobei die Tropfengröße schon entsprechend, die kinetische Energie aber noch gering war zum Einlangen des Wasserstaubs in den Brandraum.

Die kleinen Wassertropfen können durch die nach oben strebende heiße Gasströmung mitgerissen bzw. durch die strahlende Wärme bereits an der Brandperipherie abgedämpft werden. Der entsprechende Wassernebel kann durch eine hochgradige Zerstäubung des Wassers hergestellt werden.

Zur Erklärung siehe folgendes Bild:

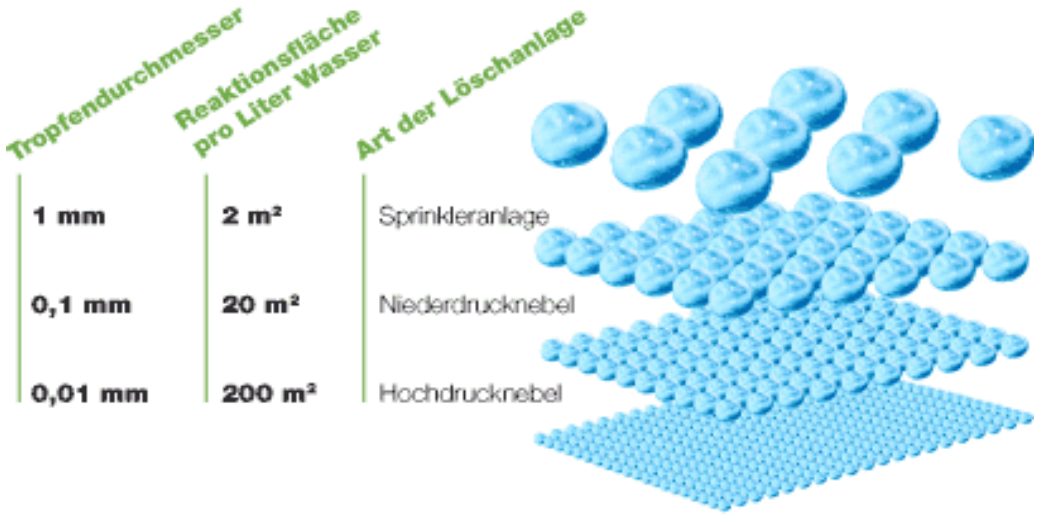


Bild 1.: Die Größe der Wassertropfen [4]

Ziel des Wassernebellöschens ist eine Brandbekämpfung mit geringster Wasserverwendung und höchster Effizienz. Dazu müssen schnell abdämpfende, kleine Wassertropfen mit entsprechender Größe und großer kinetischer Energie in der erzeugten Wasserneben-Aerosolwolke in großer Anzahl anwesend sein. Zum Erreichen einer entsprechenden kinetischen Energie bei den Tropfen mit kleiner Größe und Masse muss ihre Geschwindigkeit erhöht werden. In der Praxis wird dies durch die Düsenköpfe im Wassernebellöschsystem erreicht, die den Tropfen die notwendige Energie zum Einlangen in den Brandraum im Wege der Hochdruckzerstäubung verleihen [5].

Das für die Brandbekämpfung geeignete Wassernebel kann am einfachsten mit der Methode des Strömens von ein oder zwei Stoffen hergestellt werden. Beim Strömen von einem Stoff funktioniert die Herstellung von Wassernebel in den am häufigsten verwendeten Spezialdüsen nach dem Prinzip der Zentrifugalzerstäubung. Bei der Anwendung der Zweistoffmethode wird zur Herstellung des Wassernebels ein Wasserstrahl im Niedrigdruckbereich zu einem Gasstrahl von oben oder in Strahlrichtung in einem bestimmten Winkel von den zwei Seiten entlang des Gasstrahls zugeführt [6].

Der Wasserstrahl zerstäubt sich im Gasstrom auf kleine Tropfen, die vom Gasstrom gleichzeitig zur Zerstäubung mitgerissen werden. Der Zerstäubungsgrad hängt vom Gasdruck ab. Von der Strömungsgeschwindigkeit des Gases abhängig gelangen die Wassertropfen mit einer relativ hohen kinetischen Energie in den Brandraum. Daraus folgt, dass die Wirksamkeit des Wassernebel-Aerosollöschens in der Steigerung der Zerstäubung und der kinetischen Energie der Wassertropfen und in ihren plötzlichen Abdämpfung in der Flammenzone liegt, wodurch sich die Sauerstoffkonzentration in der Nähe des Brandes bei einer Kühlwirkung an der Oberfläche des brennenden Stoffes reduziert. Parallel dazu ist zufolge der homogenen/heterogenen Inhibition ein Abbruch der Kettenreaktion im Brandvorgang zu beobachten [6].

Wassernebel kann grundsätzlich zum Löschen sämtlicher brennbaren Stoffe angewendet werden, bei denen das Wasserlöschen zulässig ist, wobei die Frostgefahr beim Winterbetrieb berücksichtigt werden muss. Die Versuche haben nachgewiesen, dass Wassernebel mit entsprechendem Hochdruck auch bei der Brandbekämpfung von Anlagen unter Spannung eingesetzt werden kann. Zur Ablösung von Halon wurden auch in elektrischen Schalt- und Steuerräumen, digitalen Serverräumen und Telefonzentralen eingebaute Wassernebel-Löschsysteme errichtet [7].

Einer der Nachteile der Anwendung von Wassernebel in der Brandbekämpfung ist, dass es Stoffe gibt, die in chemischer Reaktion mit Wasser sogar zu Explosion führen können. So

sind einige Alkalimetalle und Erdalkalimetalle, Natrium, Kalium usw. sowie die Karbide und Hybride dieser. Eine andere gefährliche Charakteristik von Wassernebel ist, dass er bei hoher Temperatur zur thermischen Dissoziation neigt, so zum Beispiel beim Löschen von Metallbränden. Durch die hohe Temperatur wird das Wasser in seine Komponenten, in Wasserstoff und Sauerstoff geteilt, wodurch Knallgas (H2 + O2) entsteht, das sich explosionsartig wieder als Wasser vereinigt. Durch die Anwendung von Wassernebel kann im Vergleich zu den herkömmlichen Methoden unter Benutzung von erheblich weniger Wasser eine bessere Effizienz ohne Sekundärschäden erzielt werden. Dank der komplexen Löschwirkung von Wassernebel verringern sich die Umweltschäden in erheblichem Maße [7].

Der zur Brandbekämpfung geeignete Wassernebel kann durch spezifische Strahlköpfe, Wassernebeldüsen sowie Turbolöscher hergestellt werden, die keine einfache technische Herausforderung darstellen.

Es lässt sich also feststellen, dass dank den neuen Forschungen und Entwicklungen die Anwendung der entsprechenden Technologie eine außerordentlich schnelle und wirksame Brandbekämpfung mit Wassernebel aus herkömmlichem Wasser ermöglicht.

CHARAKTERISTIK UND ANWENDUNGSMÖGLICHKEITEN DER TURBOLÖSCHERN

In der Entwicklung und Optimierung der Turbolöschern haben sich die ungarischen Ingenieure unschätzbare Verdienste erworben: der erfolgreiche Einsatz dieser Anlagen hat die Aufmerksamkeit der Welt auf Ungarn gerichtet. Die ungarischen Entwicklungen wurden nur auf den Einsatz im Freien (Feuerlöschen von Gas- und Ölbrunnenausbrüchen) fokussiert, zum Testen des Einsatzes der Anlage zur Brandbekämpfung bei Industriebränden sowie auf spezifischen Gebieten, wie z.B. bei Tunnelbränden wurden und werden zur Zeit in Ungarn keine Versuche durchgeführt. Für den Industrieeinsatz wurden in Deutschland aufgrund des ungarischen Musters Turbolöscher entwickelt.

Nach dem Zweiten Weltkrieg wurde die Erdöl- und Erdgasgewinnung immer mehr gesteigert. Die großen Ölstaaten und -konzerne kämpften häufig gegen die Fackelfeuer beim Ausbruch von Gas- und Erdölbrunnen. In den 60-er Jahren wurden in der ehemaligen Sowjetunion Versuche mit dem Einsatz von Strahltriebwerken von Luftfahrzeugen zur Brandbekämpfung durchgeführt. Die Fachmänner in Novosibirsk waren bemüht, eine speziell zum Löschen von Fackelfeuern geeignete Anlage zu bauen. Das Strahltriebwerk des Luftfahrzeuges wurde auf einen LKW montiert, wodurch die Anlage mobilisiert werden konnte. Als der Löscher auch in der Praxis getestet wurde, wurden sie vor dem Problem gestellt, dass ein Teil der aus dem Strahltriebwerk ausströmenden Gase auch brennbare Stoffe enthält, die die Löscheffizienz verringern. Das Problem wurde dadurch gelöst, dass dem aus dem Triebwerk austretenden Gasstrahl Wasser zugeführt wurde, das sich in Reaktion mit dem ausströmenden Gas zerstäubt hat. So wurde Wassernebel erzeugt. Durch die Zugabe von Wasser konnte die Löscheffizienz gesteigert werden. Später haben sich auch ungarische Entwicklungsingenieure den Forschungen angeschlossen, und haben eine optimierte Version des russischen Turbolöschers gebaut [8].

Dabei wurde das Radialkompressor-Strahltriebwerk des Typs Klimow VK-107 eines MIG-15 Düsenjägers auf einen Zil-157 Gelände-LKW montiert. Auf die Auslaufseite des Strahltriebwerks wurden drei feste Wasserstrahlen in gleichem Abstand montiert, deren Einlaufstutzen an zwei Seiten des Fahrzeugs angebracht waren. Das Fahrzeug, wovon nur zwei Exemplaren gebaut wurden, ist am folgenden Bild zu sehen:

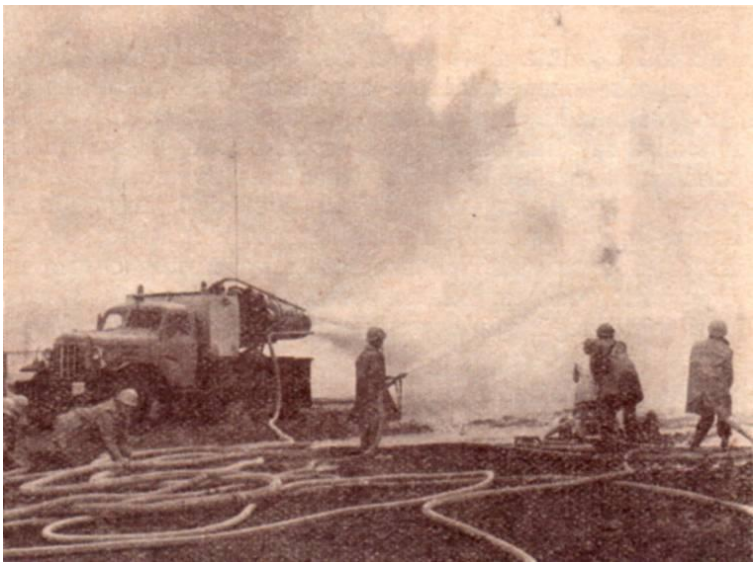


Bild 2. Zil 157 Turbolöscher [9]

Das Funktionsprinzip des Turbolöschers: Die Gasturbine hat großen Luftbedarf. Nach Anlauf des Triebwerks wird der Luftdruck durch den Radialverdichter (Kompressor) vervielfacht. Die Luft tritt aus dem Verdichter – dank der Bauart des Drehwerks des Verdichters - radial aus und gelangt durch die Einlauföffnung in den Mehrrohrbrennkammer. Hier wird der Luft Kraftstoff (Kerosin) zugeführt. Nach Zündung des Gemisches kommt es zu einer kontinuierlichen Verbrennung bei konstantem Druck. Die aufgeheizten und ausgedehnten Gase drehen die Turbine. Die Turbine treibt den Verdichter über die gemeinsame Welle, das Speisesystem des Triebwerks und die Hilfseinrichtungen an. Die gasförmigen Verbrennungsprodukte und die Inertgase gelangen ins Düsenrohr der Turbine. Diese Anlage wandelt die thermische Energie in kinetische Energie um: die Gase werden parallel zur Senkung der Temperatur beschleunigt. Der Gasstrahl tritt mit einer Geschwindigkeit von ca. 2000 km/h ins Freie aus, seine Temperatur liegt bei 500-600 °C [10].

Dem mit hoher Geschwindigkeit ausströmenden Verbrennungsprodukt-Gasstrom des Strahltriebwerks wird direkt beim Austritt durch drei Strahlrohre ungefähr 6000 Liter/Minute Wasser als gebundener Strahl zugeführt. Durch die hohe Geschwindigkeit des Gasstromes werden die Wasserstrahlen zerstäubt, während das Gas durch das Wasser gekühlt und ein Teil davon in Dampf umgewandelt wird. Das weiterströmende Gemisch und das dispergierte Wasser bilden ein besonderes Gemisch (Gemisch aus Inertgas und Dampf), das eine katalytische Kühl- und Löschwirkung ausüben kann, die zur Brandbekämpfung erforderlich ist. Der entstehende Löschstrahl mit großer Durchschlagskraft hat eine Länge von 35-40 Metern und einen Durchmesser von 10-15 Metern. Die beste Löschwirkung kann in einem 15-20 Meter großen Umkreis der Anlage erzielt werden. Der Löschmechanismus des Turbolöschers basiert auf der Durchschlagskraft, die zufolge der großen Geschwindigkeitsenergie entsteht. Der enthaltene Wassernebel wandelt sich mit gutem Wirkungsgrad in Dampf um und übt seine kühlende Wirkung aus. Die entstehende Dampfwolke und die als Trägergas benutzten inerten Abgase haben eine erhebliche Erstickungswirkung, die den Sauerstoff aus dem Brandraum verdrängt. In der Brandbekämpfung spielt auch der sog. negative Wandeffekt der Wassernebel- und Dampfkörnchen als homogene und heterogene Inhibition eine Rolle. Diese Löschwirkungen wirken gleichzeitig, einander ergänzend und zusammen

Regeln für das Löschen mit Turbolöschern [11]:

- Die Betriebsrichtung des Löschstrahls muss so festgelegt werden, dass keine Lebewesen gefährdet werden.
- Über die eigene Kühlung hinaus muss die Anlage mit mindestens zwei weiteren „C"-Strahlen ausgelegt werden.
- Ein genügend fester Angriffsweg muss zur Anlage ausgebaut werden, der durch keine Schläuche gekreuzt wird.
- In begründetem Fall (häufiger Wechsel der Windrichtung) muss auch ein alternativer Weg ausgebaut werden.
- Zum Schleppen des Löschers eine Kraftmaschine bereit halten.
- Zur Bewegung der Speiseleitungen genügendes Personal vor Ort bereitstellen.
- Beim Löschen mit mehreren Löschern die Maschinen entlang eines 90-Grad-Kreisbogens aufstellen.
- Der Winkel zwischen der Windrichtung und dem Löschstrahl soll bis einer Windstärke von 5 m/s nicht höher als 90°, bei einer Windstärke von 5-10 m/s nicht höher als 15°, bei einer Windstärke über 10 m/s nicht höher als 10 °sein.
- Die Löschzeit soll weniger als 15 Minuten betragen.

Die Anlagen wurden bei der Brandbekämpfung des Erdgasausbruchs in Algyő im Jahre 1969 von der Feuerwehr mit Erfolg angewendet. In den darauffolgenden Jahren wurden die Anlagen optimiert: die Trägermaschinen wurden auf den Typ Zil-131 umgestellt, auch die Position der Wasserstrahlen am Triebwerk wurde für einen besseren Wirkungsgrad geändert. Die Fahrzeuge an den folgenden Bildern werden in Szeged bis heute eingesetzt.

Bild 3. Zil 131 Turbolöscher [12]

Die Brände des Gasausbruchs bei Zsana im Jahre 1979 wurden schon mit diesen, auf Zil-131 LKW-Fahrgestellen gebauten Turbolöschern bekämpft. Die Beseitigung des Schadensfalls dauerte beinahe ein Monat lang und auch das Löschen wurde nur nach mehreren Versuchen erfolgreich. Während der Arbeiten wurde klar, dass zu einem wirksameren Löschen der ähnlichen Brandfälle notwendig ist, eine Anlage mit dem bisherigen Funktionsprinzip aber höherer Löschleistung zu bauen und einzusetzen. Die Erfahrungen der Beseitigung von mehreren kleineren Gasbrunnenausbrüchen, unter anderem 1984 bei Sávoly trugen dazu bei, dass die Führungsorgane noch im selben Jahr für den Bau einer neuen Hochleistungs-Turbolöschers entschieden haben [13]. Unter Berücksichtigung der wirtschaftlichen Faktoren wurden zwei, unabhängig betriebs- und steuerungsfähige Strahltriebwerke des Typs R-11F300, ursprünglich angewendet in MIG-21

Überschall-Abfangjägern auf ein umgebautes T-34 Kampfwagenfahrgestell montiert. Es wurde eine in der ganzen Welt eigenartige Löschanlage geboren. Das Gewicht des Löschers beträgt 38.000 kg. Was seine Leistung betrifft, er ist zur Erzeugung von bis zu 80-100 m Löschstrahls fähig. Mit äußerer Einspeisung kann je Triebwerk 6000 l/min Löschwasser, 3200 l/min Schwerschaum, 800 l/min Mittelschaum und 40 kg/sec Löschpulver dem Gasstrom zugeführt werden. Gleichzeitig können je Strahlwerk unterschiedliche Löschmittel angewendet werden, die Maschine eignet sich dadurch zum kombinierten Löschen [14].

Die Anlage hat ihre außerordentliche Wirksamkeit bei der Brandbekämpfung der im ersten Golfkrieg in Brand gesetzten Ölbrunnen in Kuwait bewiesen. Die Feuerwehrmänner der unterschiedlicher Länder, die an der Brandbekämpfung teilgenommen haben, staunten die Maschine bewundern an und gaben ihr den Namen „Big Wind“. Diese phantastische Leistung lenkte die Aufmerksamkeit der Welt auf die Genialität des ungarischen Erfindergeistes. Die Anlage wurde 1996 renoviert und ist bis heute betriebsbereit.

Bild 4. Big Wind Turbolöscher, [14]

SCHLUSSFOLGERUNGEN

Ich bin zur Schlussfolgerung gekommen, dass durch die Anwendung von Wassernebellöschern messbar weniger Löschwasser zu einer effizienten Brandbekämpfung genügt, wodurch auch die Sekundärschäden minimiert werden. Dank der Zusammensetzung des Wassernebels ergibt sich eine bessere Löscheffizienz. Aufgrund der geringen verwendeten Wassermenge entstehen keine Sekundärschäden. Dank der komplexen Löschwirkung von Wassernebel verringern sich die Umweltschäden in erheblichem Maße.

ZUSAMMENFASSUNG

Nimmt man die Änderungen in der Sicherheit der Welt unter die Lupe, lässt sich feststellen, dass Wasser, das auch an sich als Sicherheitsfaktor gilt, für die Lebens- und Vermögenssicherheit von besonderem Belang ist. Die umwelt- und sicherheitsbewusste Anwendung von Wasser zur Brandbekämpfung bedarf immer mehr Umsicht. Die turboreaktiven Löscher sind besondere Wassernebellöscher, die über die Erstickung der klassischen Erdgas- und Ölbrunnenausbrüche hinaus auch zur Brandbekämpfung in verschiedenen Industrieanlagen sowie zum Niederschlagen von giftigen Gasen, zur intensiven Kühlung mit Wassernebel sowie zum Einsatz als Ventilator mit Positivdruck geeignet. Die sicheren Grundlagen zur Verbreitung und erfolgreichen Anwendung der auch

heute als besonders geltenden turboreaktiven Löschtechnik wurden durch die ungarischen Entwicklungen geschaffen.

LITERATURVERZEICHNIS

[1] FÖLDI L., HALÁSZ L.: Környezetbiztonság, Complex Kiadó Budapest 2009

[2] PADÁNYI J.: Vízkonflikzusok, Hadtudomány, A Magyar Hadtudományi Társaság Folyóirata, 25. szám, pp. 272-284. 2015

[3] KUTI R.: Vízköddel oltó berendezések speciális felhasználási lehetőségei és hatékonyságuk vizsgálata a tűzoltás és kárfelszámolás területén, PhD doktori értekezés, ZMNE, 2009. URL: http://193.224.76.4/download/konyvtar/digitgy/phd/2009/kuti_rajmund.pdf

[4] Wassernebel-Löschanlagen mit Hochdrucktechnik bis 120 bar – für optimalen Schutz, G und S Sprinkleranlagen, URL: http://www.gs-brandschutz.de/15-hochdruck-feinsprueh-loeschanlagen.html (heruntergeladen: 12. 01. 2017.)

[5] KUTI R.: Miben rejlik a vízköd tűzoltási hatékonysága? Védelem Online: Tűz-és Katasztrófavédelmi Szakkönyvtár, 501, pp. 1-7. 2014, URL cím: http://www.vedelem.hu/letoltes/tanulmany/tan501.pdf

[6] KUTI R., FÖLDI L.: A beépített vízköddel oltó rendszerek újabb alkalmazási lehetőségeinek feltárása, Hadmérnök on-line, a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar és a Katonai Műszaki Doktori Iskola on-line tudományos folyóirata, III. Évfolyam 2. szám 60-66. o., 2008. június. ISSN 1788 1919. URL: http://www.hadmernok.hu/archivum/2008/2/2008_2_kuti.pdf

[7] KUTI R.: A víz tűzoltói felhasználhatóságának lehetőségei, korlátai, Védelem Online: Tűz-és Katasztrófavédelmi Szakkönyvtár, 536, pp. 1-7. URL: http://www.vedelem.hu/letoltes/anyagok/536-a-viz-tuzoltoi-felhasznalhatosaganak-lehetosegei-korlatai.pdf

[8] KUTI R.: Vízköddel oltás speciális alkalmazási lehetőségei, turboreaktív oltóberendezések I. Védelem Online: Tűz-és Katasztrófavédelmi Szakkönyvtár, 496, pp. 1-7. 2014, URL cím: http://www.vedelem.hu/letoltes/tanulmany/tan496.pdf

[9] KUNCZ I.: A tűz és oltóanyagai, BM Könyvkiadó Budapest, 1972

[10] BICZÓ I.: Különleges tűzoltó gépjárművek és felszerelések, BM Könyvkiadó Budapest, 1977

[11] BLESZITY J. – ZELENÁK M.: A tűzoltás taktikája, BM könyvkiadó Budapest, 1989

[12] FireTrucks, Internetes Tűzoltótechnikai Adatbázis, URL: http://tuzoltoautok.hu/szertar/spec/zil_131_turboreaktiv_olto/ (heruntergeladen: 12. 01. 2017.)

[13] BUDA E.: A Sávoly-18 kúton keletkezett gázkitörés és a kitörés elhárításának menete, Kőolaj és gázipari biztonságtechnikai közlemények, 15. évfolyam, 3-4. szám, 1984

[14] GALAMBOS S.: Birodalmi lépegető, negyedszázada készült a magyar csodafegyver http://www.honvedelem.hu/cikk/42634 (heruntergeladen: 12. 01. 2017.)

KÜLÖNLEGES VÍZKÖDDEL OLTÓ BERENDEZÉSEK

Absztrakt

A környezet és biztonságtudatos szemlélet előtérbe kerülésével akár a tűzeseteket, akár a különféle közlekedési, ipari baleseteket vizsgálva megállapítható, hogy azok mind a levegőre, a talajra, mind a vízre, valamint az épített humán környezetre komoly szennyező hatással lehetnek. Folyamatos a törekvés az új tűzoltási technológiák kutatására, fejlesztésére és gyakorlati bevezetésére, valamint a tűzoltással járó környezeti károk csökkentésére. Fontos tehát a gyors, hatékony, kedvező oltóanyag felhasználású környezetbarát tűzoltás. A víznek, mint környezetbarát oltóanyagnak a felhasználása ismét előtérbe került, több oltóeszközt tökéletesítettek a kutatók, melyek a víz speciális felhasználására, vízköd előállítására épülnek. Ilyen eszközök például a turboreaktív oltógépek, melyek fejlesztésében elévülhetetlen érdemeket szereztek a magyar mérnökök, sikeres alkalmazásuk hazánkra irányította a világ figyelmét. Ezeket az eszközöket mutatom be írásomban, kiemelve a magyar fejlesztések fontosságát. Rávilágítok továbbá a vízködök tűzoltási alkalmazásainak előnyeire.

Kulcsszavak: *tűzoltás, vízköd, oltóhatás, oltási hatékonyság, turboreaktív oltógép,*

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

IRÁNYÍTÁSI RENDSZEREK ADAPTÁLÁSA A KÜSZÖBÉRTÉK ALATTI ÜZEMEKBEN

ADAPTATION OF SAFETY MANAGEMENT SYSTEMS IN UNDER TIER ESTABLISHMENTS

MESICS Zoltán

(ORCID: 0000-0002-0196-6021)

zoltan.mesics@katved.gov.hu

Absztrakt

A biztonsági irányítási rendszerek eredményes és hatékony működtetése a súlyos balesetek megelőzésének egyik legfontosabb eszköze. A küszöbérték alatti üzemek a jelen lévő veszélyes anyagok mennyisége alapján alacsonyabb veszélyeztetési szintet képviselnek. Jelen cikkben a szerző áttekinti az iparbiztonsági hatóságok ellenőrzési tevékenységének tapasztalatait és az irányítási rendszerekre vonatkozó szabályozás végrehajtási lehetőségeit a küszöbérték alatti üzemek esetében. A hatósági tapasztalatok alapján javaslatot tesz az irányítási rendszerekhez kapcsolódó jogi szabályozás fejlesztésére, konkrétan a biztonsági irányítási rendszerekre vonatkozó követelmények kiterjesztésére az alsó küszöbértékű és a küszöbérték alatti üzemekben működtetett irányítási rendszerekre. *"A mű a KÖFOP 2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."*

Kulcsszavak: *súlyos baleset, iparbiztonság, veszélyes üzem, biztonsági irányítási rendszer, küszöbérték alatti üzem*

Abstract

One of the most important instrument for preventing the major accidents involving dangerous substances is the effective and efficient operation of the safety management system. The under tier establishments pose a lower endangering level and according to this fact the operators expect proportional legal obligations. In this article the author review the authorial experiences of the regular inspections and the enforcement opportunities associated with implementing the provisions of national legislation on the management systems in case of under tier plants. On the basis of the authorial experiences he propose the further improvement of the management system related legal framework. One way of this improvement could be the extension of the safety management system to the lower tier and under tier establishments.

Keywords: *major accident, industrial safety, hazardous plant, safety management system, under tier plant.*

A kézirat benyújtásának dátuma (Date of the submission): (2017.02.10.
A kézirat elfogadásának dátuma (Date of the acceptance): (2017.02.30.

BEVEZETÉS

Az olyan üzemektől, amelyek veszélyes anyagokkal kapcsolatos súlyos balesetek okozói lehetnek, más üzemeknél nagyobb mértékben várható el, hogy magas szintű védelmet legyenek képesek nyújtani. Ez azt jelenti, hogy rendelkezniük kell hatékony baleset-megelőzési célkitűzésekkel és a célkitűzések hatékony végrehajtását biztosító irányítási rendszerrel. [1] [2]

A veszélyes üzemek üzemeltetői részére a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény (Kat.) IV. fejezete az üzem státuszától függően biztonsági irányítási rendszer vagy irányítási rendszer működtetését írja elő. Mindkét típusú rendszer működtetésének célja az üzemeltető súlyos balesetek megelőzésére és a kockázatok csökkentésére irányuló biztonsági politikájának végrehajtása. [3]

A biztonsági irányítási rendszer olyan nem önkéntes vállaláson – hanem jogszabályi kötelezettség teljesítésén – alapuló „minőségirányítási" rendszer [4], amelynek működtetésével a súlyos balesetekkel szembeni megfelelő biztonság elérhető és fenntartható.

A biztonsági irányítási rendszer elsődleges célja a vállalat tevékenységének formális szabályozása az üzemeltetés biztonságának kialakítása, fenntartása, a biztonsági teljesítmény folyamatos fejlesztése, valamint a pozitív biztonsági kultúra támogatása érdekében. A biztonsági irányítási rendszer strukturált megközelítést nyújt mindazon vállalaton belüli szervezési intézkedések megtételére, amelyek a kívánatos biztonsági teljesítmény eléréséhez szükségesek. Gyakorlatilag a biztonsági irányítási rendszer hivatott az üzemeltető súlyos balesetek megelőzésére vonatkozó célkitűzéseinek megvalósítására. [5] Az alsó küszöbértékű és küszöbérték alatti üzemekben működtetett irányítási rendszer (IR) a célját, felépítését és főbb elemeit tekintve megegyezik a felső küszöbértékű üzemekben előírt biztonsági irányítási rendszerrel (BIR), azonban az IR esetén a rendszer egyes elemeinek tartalmát és dokumentáltságát tekintve a Kat. végrehajtására kiadott, *a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X.20.) Kormányrendelet (R.)* kevésbé részletes előírásokat határoz meg. [6]

Tekintve, hogy az Európai Bizottság Közösségi Kutatási Központban működő Súlyos Baleseti Veszélyek Iroda elemzései [7] azt bizonyították, hogy a balesetek 85 %-a emberi mulasztásra, illetve a biztonsági irányítási rendszer hiányosságaira vezethető vissza, megállapítható, hogy az eredményesen és hatékonyan működtetett biztonsági irányítási rendszer - melynek középpontjában az üzemeltető, a munkavállalói, alvállalkozók és egyéb közreműködők biztonsággal kapcsolatos tevékenységének részletekbe menő szabályozása áll - a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzésének egyik legfontosabb eszköze. [8]

Az Európai Parlament és a Tanács 2012/18/EU számú, a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről szóló Irányelve (Seveso III. Irányelv) követelményeivel összhangban az üzemeltető által kialakított biztonsági irányítási rendszernek foglalkoznia kell az alábbi tartalmi elemekkel.

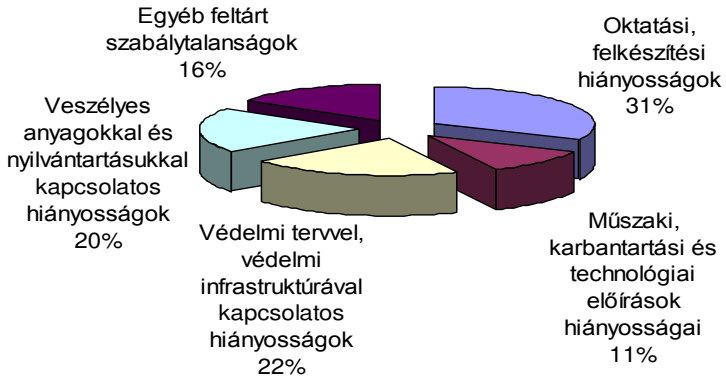
- szervezet és személyzet,
- súlyos baleseti veszélyek azonosítása és értékelése,
- üzemeltetési normarendszer,
- változások kezelése,
- védelmi tervezés,
- teljesítményértékelés (monitoring),
- audit és átvizsgálás. [9]

Az iparbiztonsági hatóságok az R. 14. §-ában foglaltaknak megfelelően a felső küszöbértékű veszélyes anyagokkal foglalkozó üzemeket legalább évente, az alsó küszöbértékű veszélyes anyagokkal foglalkozó üzemeket legalább háromévente egyszer a biztonsági irányítási rendszerre vagy az irányítási rendszerre is kiterjedően ellenőrzik (a továbbiakban: időszakos hatósági ellenőrzés). Az R. 39. § értelmében a hatóságok a küszöbérték alatti üzemeket legalább háromévente egyszer az irányítási rendszerre is kiterjedően ellenőrzik.

Az időszakos hatósági ellenőrzések tapasztalatainak elemzésével lehetővé válik a küszöbérték alatti üzemekben feltárt biztonsági hiányosságok és az irányítási rendszerek nem megfelelő működtetése közötti összefüggések azonosítása. Ennek tükrében hatékonyabban kialakíthatóak és továbbfejleszthetőek a küszöbérték alatti üzemekben alkalmazott irányítási rendszerek, a jogszabályban foglalt valamennyi tartalmi elem vonatkozásában.

A 2016. ÉVI IDŐSZAKOS HATÓSÁGI ELLENŐRZÉSEK TAPASZTALATAI

Az iparbiztonsági hatóságok 2016. december 15-ig lefolytatott időszakos hatósági ellenőrzéseik során 116 hiányosságok tártak fel. A hiányosságok jelentős részét (42%) küszöbérték alatti üzemek telephelyein, további mintegy harmadát (32%) az alsó küszöbértékű veszélyes anyagokkal foglalkozó üzemekben, a fennmaradó részt (26%) pedig a felső küszöbértékű üzemekben tárták fel. A hiányosságok főbb kategóriánkénti megoszlását a következő ábra szemlélteti.



1. ábra Hatósági ellenőrzéseken feltárt hiányosságok megoszlása (saját szerkesztés)

Az oktatási, felkészítési hiányosságok közül kiemelhető a veszélyes üzemek területén állandó vagy eseti megbízással tevékenységet végző alvállalkozók súlyos baleseti veszélyekről és az esetlegesen bekövetkező súlyos baleset esetén követendő magatartási szabályokról való tájékoztatásának elmulasztása, valamint a társadalmi kockázat számítás során a szomszédos gazdálkodó szervezetek figyelmen kívül hagyhatóságára vonatkozó feltételek be nem tartása. Egyes üzemeltetők nem részesítették védelmi terv oktatásban valamennyi saját munkavállalójukat, valamint a hosszabb távú együttműködés keretében foglalkoztatott alvállalkozókat, továbbá elmulasztották bevonni az üzem területén folyamatos megbízással tevékenykedő alvállalkozókat a védelmi tervek kidolgozásába.

A veszélyes anyagok nyilvántartásával kapcsolatos hiányosságok alapvetően a nyilvántartások naprakészségével, valamint a telephelyen előforduló a főtevékenységhez közvetlenül nem kapcsolódó veszélyes anyagok figyelembevételével kapcsolatban merültek fel.

A védelmi tervvel és infrastruktúrával kapcsolatos hiányosságok közül kiemelhető a robbanásbiztos kivitelű berendezések (például mobil szivattyú) vonatkozó tanúsítványának hiánya, valamint a soros felülvizsgálat során nem megfelelő minősítést kapott villámvédelmi

rendszer javításának elmulasztása. Előfordult, hogy az üzemeltető az egyéni védőeszközöket nem a tervezett felhasználás helyén (a védelmi tervezés során meghatározott munkahelyen) tárolta, a veszélyhelyzeti gyülekezési hely nem volt megfelelően kijelölve, a portaszolgálatnál elhelyezett értesítési lista nem volt aktuális vagy a portaszolgálat személyzete nem tartózkodott a szolgálati helyén.

A műszaki, karbantartási és technológiai előírások tekintetében kiemelhetőek az alvállalkozói tevékenységek kezelésével kapcsolatos eljárások (például munkaterület átadás-átvétel és a kapcsolódó kiszakaszolási, veszélyes anyag mentesítési feladatok) hiányosságai, amelyek az idei évben is okoztak személyi sérüléssel járó üzemzavart. Az igazgatóságok eltéréseket tártak fel a veszélyes anyagok tárolási rendjétől, valamint szabálytalanságokat tapasztaltak a csomagolóanyagok jelölése és épsége tekintetében. Számos igazgatóság jelezte a biztonság szempontjából kritikus berendezések karbantartásával, időszakos felülvizsgálatával kapcsolatos hiányosságok fennállását is.

Az egyéb feltárt szabálytalanságok között elsősorban a biztonsági dokumentációk valóságtartalmát érintő eltérések, valamint a nem közvetlenül a veszélyes üzemi szakterülethez tartozó hiányosságok (például tűzvédelmi vagy a veszélyes áru szállítással kapcsolatos szabálytalanságok) kerültek jelentésre.

A 2016. évi időszakos hatósági ellenőrzések kiemelt vizsgálati területei az alábbiak voltak:

- a veszélyes anyagok nyilvántartási rendszerének, naprakészen tartásának, nyomon követhetőségének, irányítási rendszerben való dokumentáltságának vizsgálata, valamint
- a veszélyes anyagokkal kapcsolatos üzemzavarok, súlyos balesetek dokumentálása, a kapcsolódó vizsgálati és dokumentálási kötelezettségek teljesítésének ellenőrzése.

Az iparbiztonsági hatósági tapasztalatok azt mutatják, hogy a jelen lévő veszélyes anyagok nyilvántartását az üzemeltetők döntő többsége az R. 13. § (6) bekezdésében foglalt követelményeknek megfelelően naprakészen vezeti és annak elérhetőségét a hatóság által ellenőrizhető formában a telephelyen biztosítja.

A nyilvántartások legtöbbször elektronikus formában, naplózott és visszakereshető módon kerültek kialakításra, az üzemeltetők a nyilvántartás vezetésének szabályait beépítették az üzemi irányítási rendszerbe. Az üzemeltetők a nyilvántartásokhoz kapcsolódóan gyakran az üzem besorolása és tevékenységének jellege miatt indokolt szoftveres küszöbérték figyelő alkalmazásokat is működtetnek. Az ammónia hűtőközeget használó hűtőházak üzemeltetői a nyilvántartást a hűtőközeg utánpótlásához kapcsolódó szállítási dokumentumok és a rendszer nyomás és térfogat viszonyai alapján számításokkal határozzák meg, azonban a nyilvántartások még ezen üzemek esetében is többnyire elektronikus formában vezetettek.

A veszélyes anyagokkal kapcsolatos üzemzavarok kivizsgálása tekintetében rendelkezésre álló tapasztalatok sokkal árnyaltabb képet mutatnak.

A biztonság iránt tudatos, megfelelő anyagi, személyi és pénzügyi erőforrásokkal rendelkező, elsősorban felső küszöbértékű veszélyes anyagokkal foglalkozó üzemek üzemeltetői a nem várt események bekövetkezését követően külső és belső szakértők megbízásával megfelelő mélységű kivizsgálást végeznek, a megállapított biztonságnövelő ajánlásokat vezetői szinten jóváhagyott és nyomon követett formában végrehajtják. Az iparbiztonsági hatóságok tapasztalatai alapján amennyiben az adott létesítmény biztonságos működésének helyreállítása az üzemeltető gazdasági érdekeihez közvetlenül kapcsolódik, akkor a kivizsgálás és a szükséges intézkedések megtétele haladéktalanul megtörténik, egyéb esetekben azonban a bonyolult szervezeti felépítés és a szerteágazó adminisztratív és költségvetési folyamatok miatt az események kivizsgálása indokolatlanul elhúzódhat.

A biztonság iránt kevésbé elkötelezett üzemeltetők nem minden esetben fektettek kellő hangsúlyt a kivizsgálásra és a megfelelő megelőző intézkedések megtételére, azonban

hatósági kötelezés hatására kellő erőforrást és megfelelő szakértelmet biztosítottak a kivizsgálás lefolytatásához és a megelőző intézkedések (például karbantartási rend módosítása, a berendezés gyártójával egyeztetések annak módosítására) megtételéhez.

Valódi problémát az alacsony biztonsági kultúrával rendelkező üzemeltetők jelentenek, amelyek a kivizsgálásokat a lehető legminimálisabb erőforrás és szakértelem hozzárendelésével hajtják végre. Az ezen üzemeltetők által elvégzett kivizsgálások gyakran nem az események feltételezhető alap okainak (például a karbantartásra vonatkozó üzemi szabályok enyhítése a közelmúltban) feltárásáig, hanem kizárólag a közvetlen kiváltó ok (például szelep tömörtelensége) azonosításáig terjednek. A kivizsgálás eredményként kizárólag az adott műszaki meghibásodás megjavítására intézkednek (például ammóniás hűtőrendszer esetében kizárólag a sérült csőszakasz cseréje), azonban rendszerszintű műszaki vagy szervezési vonatkozású megelőző (például a teljes csővezetékrendszer falvastagságának műszeres átvizsgálása vagy a karbantartási ciklusidők felülvizsgálata) és biztonságnövelő (például gázérzékelők elhelyezése) intézkedéseket nem tesznek.

A 2016. évi időszakos hatósági ellenőrzési tapasztalatokat tekintve összességében elmondható, hogy a feltárt biztonsági hiányosságok döntő többsége (például oktatási hiányosságok, alvállalkozói tevékenységek kezelése, karbantartási rendszerek működtetése, üzemzavarok kivizsgálása) a biztonsági irányítási rendszerek és irányítási rendszerek nem megfelelő kialakítására, működtetésére visszavezethető. Megállapítható továbbá, hogy a hiányosságok túlnyomó része (74%) az alsó küszöbértékű veszélyes anyagokkal foglalkozó és a küszöbérték alatti üzemekben működtetett, a vonatkozó jogszabályi környezetben kevésbé részletesen szabályozott irányítási rendszerekhez köthető. Iránymutatások biztosítása indokolt az érintett üzemeltetői kör számára az irányítási rendszerek hatékony és eredményes kialakítása érdekében.

AZ IRÁNYÍTÁSI RENDSZEREK KIALAKÍTÁSÁNAK LEHETŐSÉGEI A KÜSZÖBÉRTÉK ALATTI ÜZEMEKBEN

A jelen fejezetben a szerző az irányítási rendszerek kialakítása és működtetése során felmerülő, elsősorban a küszöbérték alatti üzemek esetében jellemző sajátosságokat, kapcsolódó kihívásokat elemzi, amelyek tapasztalatai szerint jelentős mértékben hozzájárulhatnak az irányítási rendszerek nem megfelelő kialakításához, működtetéséhez.

A biztonsági irányítást valamennyi vállalatnak az általános vállalatirányítás részeként célszerű kezelnie [10], tekintve, hogy egyértelmű összefüggés áll fenn a biztonságosan üzemelő vállalatok és a jól irányított üzemeltetés között. A biztonsági irányítási rendszernek a biztonsági politikán kell alapulnia, és meg kell határoznia olyan szintű célkitűzéseket, amelyet a vállalat megfelelőnek tart üzleti tevékenységéhez, továbbá a biztonsági megfontolásoknak és követelményeknek illeszkedniük kell a vállalat létesítményeihez. [11]

A biztonsági irányítási rendszer elsődleges célja a vállalat tevékenységének formális szabályozása az üzemeltetés biztonságának kialakítása, fenntartása és a biztonsági teljesítmény folyamatos fejlesztése, valamint a pozitív biztonsági kultúra támogatása érdekében. A biztonsági irányítási rendszer struktúrált megközelítést nyújt mindazon vállalaton belüli szervezési intézkedések megtételére, amelyek a kívánatos biztonsági teljesítmény eléréséhez szükségesek.

Jelenleg nem létezik nemzetközi szabvány a súlyos balesetek megelőzését szolgáló irányítási rendszerekre vonatkozóan. Az üzemek többsége azonban rendelkezik környezet-, minőség- és egyéb ágazatspecifikus (például gyógyszeriparban a Good Manufacturing Practice - GMP) irányítási rendszerekkel, amelyek sok értékes elemet tartalmaznak a súlyos balesetek megelőzése tekintetében. A súlyos balesetek megelőzését és hatásaik elleni

védekezést szolgáló irányítási rendszerek kifejlesztése lehetséges ezen irányítási rendszerek céljának kibővítésével, ebben az esetben az integrációt kell megvalósítani.

Az MSZ 28001 „A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR). Követelmények" vagy az ISO 14001 „Környezetközpontú irányítási rendszerek. Követelmények és alkalmazási irányelvek" című szabványokban foglaltaknak megfelelően kialakított és működtetett irányítási rendszerek – annak ellenére, hogy szerkezeti felépítését és célját tekintve különösen az előbbi közel áll a biztonsági irányítási rendszerekhez – önmagában nem elegendőek a vonatkozó jogszabályi követelmények teljesítésére, mivel az említett szabványok előírásai nem kifejezetten a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzését és elhárítását szolgálják. Nem terjednek ki például a telephely környezetében élő lakosságot érintő kockázatok szisztematikus felmérésére, értékelésére, valamint a csökkentésük érdekében végrehajtandó intézkedésekre.

A több telephelyet üzemeltető (gyakran multinacionális) vállalatok esetében a biztonsági irányítási rendszer többszintűen kerülhet kialakításra. Egyes elemek – például a biztonsági politika és a biztonsági célkitűzések egy része központilag, mások – például a változtatások kezelésére, a karbantartásokra, a munkaengedélyezésre, vagy a nem várt események kivizsgálására vonatkozó eljárások csoportszinten, míg továbbiak – például a kockázatelemzés eredményeként a helyi biztonsági követelmények meghatározására és teljesítésére irányuló eljárások, a munkavállalók képzésével kapcsolatos egyes szabályok és nyilvántartások telephelyi szinten jelenhetnek meg.

Az előzőekben foglaltaknak kiemelkedő jelentősége van a hazánk területén több – a Kat. IV. fejezet hatálya alá tartozó – telephelyet alacsony személyi létszámmal üzemeltető (például egyes veszélyes áru raktár-logisztikával foglalkozó) vállalatok esetében. Előfordulhat, hogy kizárólag a vállalat központi telephelyén áll(nak) rendelkezésre az EHS (Egészség, Biztonság, Környezetvédelem) területért felelős szakember(ek), és az egyes fióktelepeken csupán 2-3 fő anyagmozgatási, valamint adminisztratív feladatokat ellátó munkavállaló van jelen. Ilyen esetben kulcsfontosságú a biztonsági irányítási rendszer főbb eljárásait vállalati szinten kialakítani, és a végrehajtásukhoz kapcsolódó feladatokat például munkaköri leírások, munkautasítások formájában delegálni az érintett munkavállalók részére. Természetesen nem lehetséges a teljes biztonsági irányítási rendszer központi szinten történő egységes kialakítása, mivel az eljárásokban figyelembe kell venni az egyes fióktelepek sajátosságait (például a jelen lévő anyagok eltérő veszélyprofilját, az egyes anyagokhoz kapcsolódó sajátos tárolási szabályokat, a belső védelmi tervezés telephelyi sajátosságait).

A biztonsági dokumentációban (biztonsági jelentés, biztonsági elemzés, súlyos káresemény elhárítási terv) a biztonsági irányítási rendszer bemutatásakor nem szükséges a rendszer teljes dokumentációját (valamennyi folyamat, utasítás stb.) maradéktalanul megjeleníteni. Elegendő átfogó leírás formájában utalni az egyes jogszabályban foglalt tartalmi elemekhez kapcsolódó szervezeti-személyi feltételek, eljárások, utasítások, intézkedések meglétére, továbbá egyértelmű hivatkozások alkalmazásával lehetővé kell tenni a további részletszabályozók azonosíthatóságát.

Előfordulhat, hogy egyes vállalatoknál az említett átfogó leíráson túlmenően a biztonsággal kapcsolatos egyes eljárások nem kellő mértékben szabályozottak (írott formában nem leképezettek), sokkal inkább ösztönösen, a jól bevált szokásokat fenntartva működnek. Ekkor azonban fennáll a veszélye a jelenlegi tapasztalt vezetők, munkavállalók áthelyezése/távozása esetén – az írásban szabályozott irányítás hiánya miatt – a biztonság átmeneti csökkenésének.

A felső küszöbértékű veszélyes anyagokkal foglalkozó üzemekben működtetett biztonsági irányítási rendszerek, valamint az alsó küszöbértékű veszélyes anyagokkal foglalkozó és a küszöbérték alatti üzemekben működtetett irányítási rendszerek célja egyaránt a veszélyes anyagokkal kapcsolatos súlyos balesetek hatékony megelőzésének és elhárításának

biztosítása. Tekintettel a rendszerek fenntartási céljának azonosságára, a vonatkozó jogi szabályozás értelmében a főbb tartalmi elemek mindkét típusú rendszer esetében megegyeznek, azonban a jogalkotó a biztonsági irányítási rendszerek részletekbe menő szabályozásával ellentétben az irányítási rendszerekre vonatkozóan kevesebb dokumentálási követelményt határozott meg. Ezáltal lényeges különbség kizárólag a rendszerek dokumentálásának szintjén jelentkezik. Ezen előírások összhangban vannak a Seveso III. irányelv 8. cikk (5) bekezdésében foglaltakkal, amely szerint az alsó küszöbértékű üzemekben a súlyos balesetek megelőzésére vonatkozó terv (MAPP) végrehajtásának eszköze nem kizárólag a biztonsági irányítási rendszer alkalmazása lehet, hanem egyéb - az irányelv III. mellékletével összhangban lévő - a súlyos baleset veszélyeivel arányban álló más megfelelő eszköz, struktúra, irányítási rendszer működtetése is megoldást jelenthet.

A gyakorlatban az egyes tartalmi elemekhez tartozó szervezeti-személyi feltételeknek, eljárásoknak, utasításoknak, intézkedéseknek mindkét típusú rendszer esetében kialakítottnak kell lennie, a biztonsági irányítási rendszert azonban a vonatkozó jogi szabályozás részletesebb követelményeinek megfelelően szükséges dokumentálni. Célszerű mindezt egységes szerkezetű biztonsági irányítási kézikönyv formájában megtenni, amely biztosítja a gyors, rendszerszintű áttekinthetőséget, ugyanakkor közvetlen hivatkozásokat is tartalmaz az egyes szabályozókra vonatkozóan. Az alsó küszöbértékű veszélyes anyagokkal foglalkozó és a küszöbérték alatti üzemekben – mivel az R. 3. melléklet 1.8. pontjában foglalt részletes dokumentálási követelmények ezen üzemeltetőkre nem vonatkoznak – elegendő az R. 3. melléklet 1.1. pontjában foglaltaknak megfelelően kialakított irányítási rendszert a meglévő üzemi szabályozás eljárásaiban, dokumentumaiban megjeleníteni (például a munkaköri leírásokat kiegészíteni a biztonsággal kapcsolatos feladatokkal, a munkautasításokban hangsúlyosan szerepeltetni a biztonságos üzemeltetés feltételeit, felülvizsgálni az egyéb sajátos utasításokat – például ammónium-nitrát raktár-logisztikai tevékenység esetében célszerű a telephelyi tárolási utasításokat a gyártó által közzétett, a biztonságos tárolásra vonatkozó ajánlások alapján felülvizsgálni, vagy például egyéb telephelyeken a veszélyes anyagok/keverékek biztonsági adatapján szereplő információkat figyelembe venni a kezelési, tárolási utasítások kialakításakor).

Mind az üzemeltető, mind a szerződött felek munkavállalóinak folyamatbiztonsági kérdésekkel kapcsolatos tudatossága döntő jelentőségű, emellett az üzemeltetőknek nyomon kell követniük szervezési eljárásaik, az alkalmazottaik képzésének és az alvállalkozói tevékenység szervezésének működését. Minden személynek, aki felelős a biztonság szempontjából kritikus műveletekért, beleértve a karbantartási tevékenységet, (belső munkavállalók, vagy vállalkozók és alvállalkozók alkalmazottai, vagy bárki aki terméket és szolgáltatást nyújt) részesülnie kell megfelelő képzésben és információkban a kockázatokról, a követendő helyes eljárásokról, és a munkaengedélyezés követelményeiről azok teljesítése érdekében. Különleges tevékenységek esetében, amelyekhez a nemzeti jogi szabályozás sajátos követelményeket támaszt (például elektromos munka, ATEX berendezések karbantartása, szűk/zárt térben végzett munka, gépek biztonságos kialakítása - kockázatfelmérés) az üzemeltetőnek speciális eljárásokat kell kidolgoznia, figyelembe véve azokat az előírásokat mind a saját munkavállalói (speciális minősítésen keresztül), mind a vállalkozók alkalmazottai (a minősítések ellenőrzése külső munkavállalóknál) számára. Ezen eljárásoknak biztosítania kell azt, hogy a speciális képzettséget igénylő munkák (például hegesztés) kizárólag az arra minősített szakember által kerülhessenek kivitelezésre. A munkaengedélyek kiadásával kapcsolatos felelősségeknek tartalmaznia kell a kockázatelemzést és a balesetek kezelését a kockázati tudatosság és a tevékenységben rejlő sajátos veszélyek ismeretének kialakítása érdekében. Más üzemeltetési szempontból, a munkavállalókat be kell vonni biztonságos munkavégzés eljárásainak kidolgozásába.

A biztonsági normák folyamatos tökéletesítése érdekében szükséges bevonni az adott berendezés/veszélyes anyagokkal foglalkozó létesítmény üzemeltetésében nagy tapasztalattal rendelkező munkavállalókat is. Az irányítási rendszer kialakításában és folyamatos fejlesztésében a közvetlen munkavállalókon túlmenően fontos szerepet játszanak a külső felek szakemberei (például szakszervizek, szaktanácsadók, műszaki felülvizsgálatot végzők stb.) is. Az általuk megállapított problémák, hiányosságok, negatív tendenciák értékelése jelentősen javíthatja a biztonság szempontjából kritikus elemek biztonságát, hozzájárulhat az irányítási rendszer eredményes tökéletesítéséhez. A hatóságok által tett megállapítások, kötelezések, javaslatok (például a védelmi terv gyakorlatok, ellenőrzések alkalmával stb.) szintén hozzájárulhatnak az irányítási rendszer folyamatos fejlesztéséhez.

A veszélyforrás-elemzés keretében a veszélyes anyagokhoz kapcsolódó gyártási-, tárolási- és egyéb folyamatok közül kiszűrésre kerülnek a biztonság szempontjából kritikus műveletek. Az üzemeltetési normarendszer kialakításakor az említett folyamatok technológiai utasításait ki kell egészíteni a biztonságos üzemeltetés feltételeivel.

Az üzemeltetési normarendszerben a technológiai veszélyhelyzetek üzemen belüli jelzésének és kezelésének lehetséges módjait a kapcsolódó erőforrások megjelenítésével együtt szerepeltetni szükséges. Természetesen a Kat. 3. § 29. és 30. alpontja szerinti minősített szintek valamelyikét (veszélyes anyagokkal kapcsolatos üzemzavar vagy súlyos baleset) elérő nem várt üzemállapotok jelentésére vonatkozó eljárásrendet és a kapcsolódó erőforrások bemutatását is tartalmaznia kell a normarendszernek.

Ezen túlmenően az üzemeltetőnek célszerű eljárásokat kialakítania az alvállalkozói tevékenységekkel kapcsolatosan, amelyek többek között az alvállalkozók kiválasztási folyamatát (beleértve a kiválasztási kritériumokat), a munkaengedélyezési, a felügyeleti tevékenységeket foglalhatják magukban, továbbá kiterjedhetnek a munkaterület átadás-átvétel, a munkavégzést követő ellenőrzési-jóváhagyás, valamint az alvállalkozók és külső partnerek biztonsági teljesítmény értékelésének szabályozására.

A normarendszer kialakításakor külön figyelmet kell fordítani az üzem területén állandó megbízással tevékenységet végző alvállalkozókra, mint például az őrzés-védelmi, vagy éppen takarítási feladatokat ellátó külső felekre. Egyes telephelyek esetében - különösen munkaidőn kívül - az őrzés-védelmi feladatokat ellátó személyek kulcsfontosságú szerepet töltenek be a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzésében és következményeik csökkentésében a kialakulásukhoz vezető nem várt események (például kezdeti tüzek, egyéb rendellenes állapotok) észlelésén, az első beavatkozói tevékenység megkezdésén, valamint az érintett külső beavatkozók és veszélyeztetettek riasztásán keresztül. Emiatt a vonatkozó utasítások (például őrutasítás) kiegészítése szükséges a biztonság szempontjából fontos információkkal (például a veszélyes létesítmények/veszélyes anyagok elhelyezkedése a telephelyen belül, lehetséges súlyos baleseti eseménysorok és azok bekövetkezésére utaló jelek, követendő magatartási szabályok, aktualizált riasztási-értesítési rend).

Természetesen az irányítási rendszerek kialakítása során a jogszabályban foglalt valamennyi tartalmi elemmel foglalkozni szükséges, azonban az egyes elemeken belül lehetőség van az arányosság elvének érvényesítésére a vállalati sajátosságok figyelembe vétele érdekében.

Az integrált irányítási rendszerek kialakítása során kiemelt figyelmet érdemes fordítani arra, hogy az egyesítendő alrendszerek, azaz a vállalatirányítás és a biztonság különböző területeit lefedő egyes irányítási rendszerek megfelelő szakmai mélységben kerüljenek kialakításra, és ezt követően történjen meg azok integrációja a lehetséges kapcsolódási pontok mentén. Az üzemeltetőnek nem szabad azt a hibát elkövetnie, hogy horizontálisan ugyan minden előírást lefed a szakértő/szolgáltató cégek segítségével kialakított integrált irányítási rendszereken keresztül, azonban a rendszer mögött vertikálisan lévő megfelelően mély szakmai tartalom hiánya miatt az eredményesség megkérdőjelezhetővé válik.

Fontos továbbá kiemelni, hogy az irányítási rendszerek valódi értéke, biztonságnövelő hatása – a vertikális szakmai mélységen túlmenően – egyenesen arányos a szigorú, következetes végrehajtásuk, betartásuk mértékével.

Az előzőekből következik, hogy a biztonság különböző területeivel foglakozó, megfelelő szakmai képesítésű szakember(ek) állandó, teljes munkaidőben történő alkalmazásának mellőzése – különösen a több telephelyet működtető vállaltok esetében – igen nagy kockázatot jelent az irányítási rendszer hatékony és eredményes végrehajtása szempontjából.

A veszélyes anyagokkal kapcsolatos súlyos balesetekkel szembeni biztonság szempontjából kritikus technológiai berendezések állapotának nyomon követésére és ellenőrzésére szolgáló stratégia és módszertan kidolgozása kulcsfontosságú. Az üzemeltetőnek megfelelő figyelmet kell fordítania az utókövetési intézkedések és az esetlegesen szükséges ellenintézkedések megtételére. Gyakorlati végrehajtási lehetőségként alkalmazható például a műszaki biztonsági fenntarthatósági célkitűzések meghatározása és a kapcsolódó eljárások kijelölése a tárgyi berendezések időszakos ellenőrzésével, műszaki biztonsági felülvizsgálatával, kalibrálásával és karbantartásával kapcsolatos tevékenységek szabályozására, valamint ezen feladatok elvégzéséhez a szükséges erőforrások biztosítása.

Az üzem biztonsági teljesítménye fejlesztésének egyik legfontosabb eszköze az irányítási rendszer zavaraira visszavezethető nem várt események (különösen a veszélyes anyagokkal kapcsolatos üzemzavarok és súlyos balesetek) kivizsgálása eredményeként levont következtetések tükrében az irányítási rendszer érintett elemeinek felülvizsgálata és a szükségesként azonosított módosítások megtétele. A vonatkozó jogi szabályozási környezetben korábban is szerepeltek kapcsolódó előírások, amelyek a jelen rendeleti módosítás eredményként még egyértelműbben kötelezővé teszik az előzőekben említett eljárások lefolytatását. A nemzetközi hatósági tapasztalatok azt mutatják, hogy a nem várt eseményekből levont tanulságokat az üzemeltetők nem minden esetben építik be az üzemi irányítási rendszerbe, illetve az esetlegesen tervezett változtatások nem jelennek meg a gyakorlati végrehajtás szintjén. A jogszabályi módosítás célja ezen tevékenység előmozdítása.

A dinamikusan működő, erős végrehajtással rendelkező irányítási rendszernek nem csupán követnie kell a vállalat fejlődését, hanem a tervezéshez, a fejlesztési irányok meghatározásához kiindulási információkkal kell szolgálnia. A szervezeti és műszaki fejlesztések következtében szükségessé válhat az irányítási rendszer egyes elemeinek módosítása. Az R. 11. § (2) bekezdése szabályozza a biztonsági dokumentáció felülvizsgálatának eseteit. Amennyiben a biztonsági irányítási rendszer módosítása kapcsán a nevezett jogszabályhelyen felsorolt feltételek valamelyike fennáll, úgy az üzemeltető köteles a biztonsági dokumentáció soron kívüli felülvizsgálatára irányuló eljárást kezdeményezni.

Összességében elmondható tehát, hogy a küszöbérték alatti üzemek gyakran több telephelyet működtető multinacionális vállalatok fióktelepeként, alacsony személyi létszámmal végzik tevékenységüket. A telephelyeken az alacsony humán erőforrás meglehetősen nagy mértékű kihasználtsága miatt kevés erőforrás áll rendelkezésre a biztonsággal kapcsolatos kérdések kezelésére és szabályozására annak ellenére, hogy ezen kérdések jelentős része helyi szinten, a telephelyi sajátosságokra visszavezethetően jelentkezik. Az iparbiztonsági hatósági ellenőrzések tükrében az irányítási rendszerekhez kapcsolódó jogi szabályozási környezet további fejlesztése indokolt, amely fejlesztés során figyelemmel kell lenni ezen üzemek szervezeti és technológiai sajátosságaira.

AZ IRÁNYÍTÁSI RENDSZEREKRE VONATKOZÓ JOGI SZABÁLYOZÁS FEJLESZTÉSE

A Seveso III. Irányelv szerint a tagállamoknak elő kell írni az üzemeltetők számára, hogy olyan dokumentumot dolgozzanak ki, amely meghatározza a súlyos balesetek megelőzésére

vonatkozó célkitűzéseit (MAPP), és gondoskodik ezek megfelelő végrehajtásáról. A súlyos balesetek megelőzésére kidolgozott üzemeltetői célkitűzések olyanok legyenek, hogy megfelelő eszközökkel, szervezetekkel és irányítási rendszerekkel garantálják az ember és a környezet magas szintű védelmét. [12] Egy lehetséges meghatározás szerint [13] az irányítási rendszer olyan eszközrendszer, amely révén biztosítható az, hogy amit meg kell tenni, azt megfelelően és a kellő időben tegyük meg. Legfontosabb alrendszerei a következők: emberek; intézkedések; eljárások; képzés és felkészítés. Az R. 3. melléklet 1.8. pontja a Seveso III. Irányelvvel összhangban részletesen tartalmazza a biztonsági irányítási rendszerekre vonatkozó előírásokat.

A felső küszöbértékű veszélyes anyagokkal foglalkozó üzemek esetében a jogi szabályozás tartalmazza azon követelményeket, amelyek teljesítésével hatékonyan megelőzhetőek a veszélyes anyagokkal kapcsolatos súlyos balesetek, üzemzavarok.

Ilyenek például a veszélyes anyagokkal kapcsolatos súlyos baleseti eseménysorokhoz rendelhető technológiai berendezések elhasználódásával és a korróziójával járó kockázatok kezelése és ellenőrzése, ezen technológiai berendezések állapotának nyomon követésére és ellenőrzésére szolgáló stratégia és módszertan kialakítása, a megfelelő utókövetési intézkedések és az esetlegesen szükséges ellenintézkedések megtétele, az alvállalkozói rendszerben végzett tevékenységek szabályozása és a műszaki-, szervezeti és személyi változtatások kezelése.

Ezzel szemben az alsó küszöbértékű és a küszöbérték alatti üzemekben működtetett irányítási rendszerek vonatkozásában az R. eltérő követelményeket fogalmaz meg. Az R. 3. melléklet 1.1. pontja kizárólag a tartalmi elemek felsorolását tartalmazza, az egyes elemek részletes tartalmát azonban már nem.

A jogalkotói szándék szerint ezen enyhítés kizárólag a dokumentálási követelményeket érinti, célja az üzemeltetők adminisztratív terheinek csökkentése. A hatósági tapasztalatok azt mutatják, hogy az alsó küszöbértékű veszélyes anyagokkal foglalkozó és a küszöbérték alatti üzemek üzemeltetőinek jelentős része a jogszabályi követelményekben lévő enyhítést nem kizárólag a dokumentálás, hanem a végrehajtás szintjén is értelmezi, ennek következtében az irányítási rendszerét esetenként igen csekély szakmai tartalommal alakítja ki. Ezáltal a veszélyes anyagokkal kapcsolatos üzemzavarok és súlyos balesetek megelőzésére szolgáló alapvető folyamatok és eljárások, beleértve a veszélyes anyagokkal kapcsolatos üzemzavarok és súlyos balesetek kivizsgálására és a megfelelő megelőző intézkedések megtételére vonatkozó eljárásokat is, ezen üzemekben maradéktalanul nem kerülnek végrehajtásra, továbbá ezek hatóság általi előírása is nehézségekbe ütközik.

A BM OKF útmutatót adott ki [14] az egységes jogértelmezés elősegítésére, azonban az igazgatóságok visszajelzései alapján az abban foglaltakat az alacsony biztonsági kultúrával rendelkező üzemeltetők figyelmen kívül hagyják.

A témakört érintően indokolt a jogi szabályozás módosítása, az R. 3. mellékelt 1.8. pontjában megfogalmazott követelmények jogszabályi szinten történő kiterjesztése az alsó küszöbértékű és a küszöbérték alatti üzemekben működtetett irányítási rendszerekre. A tárgyi jogszabályhely meghatározza a biztonsági irányítási rendszerek legfontosabb tartalmi elemeit és az azokon belül szabályozandó főbb területeket, azonban az egyes területekkel kapcsolatban nem támaszt részletes követelményrendszert. Ezáltal a szabályozás jelentős szabadságot biztosít az üzemeltetőknek a biztonsági irányítási rendszerek kialakítása során, lehetővé teszi a szervezeti, szervezési, technológiai és egyéb vállalati sajátosságok figyelembe vételét. A szabályozás alsó küszöbértékű és küszöbérték alatti üzemekre történő kiterjesztésével az irányítási rendszer egyes elemein belül lehetőség marad az arányosság elvének érvényesítésére. Ezáltal az alacsony biztonsági kultúrával rendelkező üzemeltetők esetében is biztosíthatóvá válik a súlyos balesetekkel szembeni eredményes megelőzési és védekezési intézkedések, eljárások kialakítása és folyamatos működtetése. A tárgyi üzemek –

az ott jelen lévő veszélyes anyagok mennyisége alapján – alacsonyabb veszélyeztetési szintet képviselnek, mellyel összefüggésben az ipari szereplők általános elvárása, hogy a jogszabályi követelmények arányosak legyenek a fennálló veszélyeztetés szintjével.

Ezen fejlesztési irány összhangban áll a Seveso III. Irányelv 8. cikkének (5) bekezdésében megfogalmazott alapelvvel, amely szerint az alsó küszöbértékű üzemekben a súlyos baleset-megelőzési politikát a biztonsági irányítási rendszerre és az üzem szervezetére az Irányelv III. mellékletében meghatározott elvekre figyelemmel, a súlyos baleset veszélyével arányban álló más megfelelő eszközök, struktúrák és irányítási rendszerek révén is teljesíteni lehet.

Az irányítási rendszerekre vonatkozó jogi szabályozás ilyen irányú fejlesztése az üzemeltetői biztonsági kultúra kialakítását, erősítését, az irányítási rendszer megfelelő színvonalú működtetéséhez szükséges feltételek rendelkezésre állását eredményezheti azon üzemekben is, melyekben a leginkább indokolt a biztonságos működés feltételeinek biztosítása, az önkéntes jogkövetés és az üzemeltetői elkötelezettség erősítése, ezáltal is hozzájárulva a közbiztonság növeléséhez.

KÖVETKEZTETÉSEK

A SEVESO III. irányelv bevezetésével megújult a biztonsági irányítási rendszerekre vonatkozó hazai jogi szabályozás. Az egyes tartalmi elemeket érintően megjelent legfontosabb új követelmények áttekintését követően meghatározásra és gyakorlati példákon keresztül szemléltetésre kerültek azon kapcsolódó végrehajtási lehetőségek, amelyek a biztonsági irányítási rendszerek eredményes és hatékony kialakításához és működtetéséhez elengedhetetlenek.

Az üzemeltetői, valamint az iparbiztonsági hatósági tapasztalatok rávilágítottak az üzemeltetők biztonság tökéletesítésére irányuló tevékenysége további fejlesztésének szükségességére. A hatóságok által feltárt hiányosságok túlnyomó része az alsó küszöbértékű veszélyes anyagokkal foglalkozó és a küszöbérték alatti üzemekben működtetett irányítási rendszerek hiányosságaira volt visszavezethető, amely indokolttá tette a terület mélyreható vizsgálatát és olyan végrehajtási javaslatok kidolgozását, amelyek figyelembe veszik ezen üzemeltetők – döntő többségében kis- és középvállalkozások – szervezeti, munkaszervezési sajátosságait, anyagi-, humán-, valamint pénzügyi lehetőségeit. A megfogalmazott ajánlások valódi segítséget jelentenek az érintett vegyipari vállalatok számára a biztonság tökéletesítésére irányuló tevékenységük végzése során.

Az iparbiztonsági hatósági tapasztalatok rávilágítottak továbbá az irányítási rendszerekhez kapcsolódó jogi szabályozási környezet további fejlesztésének szükségességére. E tekintetben megoldást jelenthet a biztonsági irányítási rendszerekre vonatkozó követelmények jogszabályi szinten történő kiterjesztése az alsó küszöbértékű és a küszöbérték alatti üzemekben működtetett irányítási rendszerekre. A területtel kapcsolatos jogi szabályozás továbbfejlesztése, ezáltal a magas szintű üzemeltetői biztonsági kultúra kialakulásának elősegítése nemzeti érdekünk. A társadalmunk élvezi és egyben támaszkodik azon hatalmas előnyökre, amelyeket a vegyi anyagok elterjedése, valamint elsősorban az olaj- és a gázipari szektorok fejlődése tett elérhetővé napjainkban. A veszélyek ellenőrzött körülmények között tartása érdekében szükséges intézkedések összetettek és esetenként nem magától értetődőek. A veszélyes anyagokkal kapcsolatos súlyos baleseteknek jelentős hatása lehet a telephely környezetében élő lakosság életére, egészségére, a természeti környezetre, valamint a vállalatok kereskedelmi tevékenységére, esetenként hazánk nemzetgazdaságára a fellépő üzleti zavaron és befektetői bizalom csökkenésén keresztül. Az utóbbi időben társadalmunk egyre kevésbé toleráns az elkerülhető balesetekkel szemben, különösen abban az esetben, ha a katasztrófa a kockázatok nem megfelelő kezelése vagy figyelmen kívül hagyása miatt következett be. Éppen ezért a legfontosabb cél egyensúlyt teremteni a kockázatok eredményes

kezelése és a pénzügyi haszon növelésére irányuló törekvések között azáltal, hogy az ipari szektor veszélyes üzemeket működtető felsővezetőinek figyelmét a magas színvonalú vállalati vezetés szükségességére irányítjuk.

FELHASZNÁLT IRODALOM

[1] VARGA I.: A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezési tevékenység rendszere, PhD értekezés, ZMNE, Budapest, p. 128, 2005.

[2] KÁTAI-URBÁN L.; Vass Gy.: Kátai-Urbán L. (szerk.). Kézikönyv: Veszélyes üzemek, tevékenységek és technológiák az iparban. Budapest: Nemzeti Közszolgálati Egyetem, 2014. 119 p. (ISBN 978-615-5491-74-0)

[3] SZAKÁL B., CIMER Zs., KÁTAI-URBÁN L., SÁROSI Gy., VASS Gy.: Veszélyes anyagokkal kapcsolatos balesetek elleni védekezés I.: módszertani szakkönyv veszélyes anyagok és súlyos baleseteik az iparban és a közlekedésben. Budapest: Korytrade, 2015. 120 p. (ISBN:978-963-12-3502-9)

[4] MESICS Z., KÁTAI-URBÁN L.: Biztonsági irányítási rendszerek értékelése. Hadmérnök X. évfolyam 1. szám – 2015. március, 8. old.

[5] Safety Report Assessment Manual V2. Control of Major Accident Hazards Regulations URL.: www.hse.gov.uk/comah/sram/index.htm – Health & Safety Executive, 2007.

[6] DR. VASS Gy., MESICS Z., KOVÁCS B.: ÚTMUTATÓ a biztonsági irányítási rendszerekkel kapcsolatban a Seveso III. irányelv hazai bevezetésével módosuló jogszabályi előírások végrehajtásához, közzétéve a BM OKF hivatalos honlapján, 2016. március

[7] Guidance on Developing Safety Performance related to Chemical Accident Prevention, Preparedness, and Response, Organisation for Co-operation and Developement, 2008

[8] VASS Gy., HALASZ L.: Assessment of the Land-use Planning Practices Applied in the Vicinity of EU Seveso Establishments. *ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE* 6:(1) *pp. 77-88.* (2007)

[9] BOGNÁR B., KÁTAI-URBÁN L., KOSSA Gy., KOZMA S., SZAKÁL B., VASS Gy., KÁTAI-URBÁN L. (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)

[10] SOLYMOSI J, TATÁR A, SZAKÁL B, KÁTAI-URBÁN L: A súlyos ipari balesetek általi veszélyeztetettséggel kapcsolatos értékelési eljárások összehasonlító vizsgálata, Katasztrófavédelmi Szemle, IV. évfolyam 2. szám, pp. 32-57. 2001.

[11] KÁTAI-URBÁN L.: Veszélyes üzemekkel kapcsolatos iparbiztonsági jog-, intézmény és eszközrendszer fejlesztése Magyarországon, Budapest: Nemzeti Közszolgálati Egyetem, 89 p.

[12] VASS Gy., HALÁSZ L., SOLYMOSI J.: A veszélyes ipari üzemekkel kapcsolatos hazai településrendezési szabályozás értékelése. *TUDOMÁNYOS KÖZLEMÉNYEK SZENT ISTVÁN EGYETEM YBL MIKLÓS MŰSZAKI FŐISKOLAI KAR* 3:(1) *pp. 72-81.* (2006)

[13] HAWKSLEY, J.L.: Implementing an effective safety management system (SMS). In: Workshop on Community legislation for the control of Major Accident Hazards. – Warsaw, EPSC, pp. 48-56. 2000.

[14] DR. VASS Gy., MESICS Z., KOVÁCS B-: ÚTMUTATÓ a biztonsági irányítási rendszerekkel kapcsolatban a Seveso III. irányelv hazai bevezetésével módosuló jogszabályi előírások végrehajtásához, közzétéve a BM OKF hivatalos honlapján, 2016. március

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

KUTATÁSI ALAPOK A KATASZTRÓFÁK ELLENI VÉDEKEZÉS TECHNIKAI FEJLESZTÉSÉHEZ

RESEARCH BASIS FOR TECHNICAL DEVELOPMENT OF PROTECTION AGAINST DISASTERS

PÁNTYA PÉTER

(ORCID: 0000-0003-2732-2766)

pantya.peter@uni-nke.hu

Absztrakt

A katasztrófavédelem szervezete és az azon belül működő tűzoltóságok a lakosság, a Magyarország területén tartózkodók élet és vagyonbiztonságát hivatottak szolgálni többek között a tűzoltás, műszaki mentés, tűzmegelőzés területén. A tűzoltói beavatkozó tevékenység igen sokrétű, jól szabályozott és technikai eszközökkel jelentős mértékben ellátott. A fenti tevékenység minél hatékonyabb ellátásának vizsgálata, az elérhető fejlesztési módszerek kutatása indokolt, melyhez kapcsolódóan készült jelen mű.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Zrínyi Miklós Habilitációs Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *katasztrófavédelem, tűzoltóság, kutatás*

Abstract

The organisation of disaster management and fire departments operating within it are dedicated to ensuring the safety of life and property of Hungarian residents by means of firefighting, technical rescue and fire prevention, among others. Fire service interventions are diverse, well-regulated and technically well-equipped. Examining the means of increased effectiveness of the above activity and studying available development methods are justified, which is in the focus of this paper.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the Miklós Zrínyi Habilitation Program.

Keywords: *disaster management, fire service, research*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.13.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.14.

BEVEZETÉS

Az élet és vagyonmentés, ezek védelmének biztosítása az egész világon ősidők óta jelenlévő feladat. Fellelt iratok, tárgyak, eszközök, létesítmények bizonyítják, hogy az ember társadalomban élve a közösség által is megpróbálja a megelőző és a beavatkozó tevékenységet ellátni a tűzesetek és egyéb káresetek ellen. Magyarországon már a római korból van fellelt tűzoltólaktanya maradványunk és a híres debreceni diáktűzoltóságról valamint az általuk használt gerundiumokról[1] sokan hallhattak. A magyarországi szervezett, akár hivatásosnak is tekinthető tűzoltóság megalapítója, gróf Széchenyi Ödön nemcsak hazánkban, hanem nemzetközi szinten is elismerést kapott. Hozzá köthető nemcsak a magyar, hanem a törökországi tűzoltósági szervezet létrehozása, fejlesztése is.

Elmondható tehát, hogy a jelen írás témája - katasztrófavédelem és tűzoltóság Magyarországon és nemzetközi szinten – ősidők óta folyamatosan ellátott társadalmi és egyben kiemelten fontos feladat.

Az alaptételek a tevékenységekre vonatkozóan:

- tűzmegelőzés: csökkenteni a tüzek kialakulását, továbbterjedését, károsító hatásainak méretét mind technológiai folyamatokban, mind pedig az épített környezetben
- tűzoltás: a már kialakult tűzeset - amely veszélyt jelent az emberi életre, a testi épségre és az anyagi javakra – lehető leghamarabb való eloltása figyelemmel a lehető legkisebb másodlagos károkozásra, a beavatkozói biztonságra, az esetleges életmentésre
- műszaki mentés:[2] a bekövetkező technikai-műszaki jellegű káresetnél az életveszélybe kerültek, sérültek mentése, a további kárnövekedés megállítása, a közvetlen életveszély elhárítása a helyszínen

„Fontos, hogy az állampolgárok minél szélesebb köre legyen képes értelmezni a rendszer működését, ezért helyénvaló, hogy az új rendszer részletesen bemutatásra kerüljön mind a kárhelyszínre vonuló állomány nagyságrendje, mind az erő -, eszköz rendszer tekintetében.” [6]

A tűzoltóságok beavatkozói, tehát jellemzően a tűzoltási, műszaki mentési (élet és vagyonmentési) tevékenysége a feladatból és annak környezetéből adódóan igen fontos, pontosan és hatékonyan végzendő szerep. A hatékonyság növelésének, további lehetőségeinek vizsgálata, a kutatás és különösen a tudományos kutatás folyamatos igénybevétele elsőrendű és közvetlen várható haszonnal kecsegtet a várhatóan kevesebb és kisebb mértékű személyi sérülés, és a minél nagyobb megmenthető vagyonérték területén.

A tűzoltói beavatkozói hatékonyság növelésére szolgáló egyik kutatás alapjairól szól jelen cikk is. A teljes kutatás várható eredményei során a hazai lehetőségek is megvizsgálásra kerülnek az elérhető jobbítási lehetőségek palettájával valamint a nemzetközi jó példák számbavételével.

---

[1] A debreceni tanulók nagyméretű botja. A tüzesetek alkalmával magukkal hordták, hogy a tűz terjedését megakadályozzák az égő épületszerkezetek igen nagy fizikai erőt kívánó szétverésével. Esetenként a gerundiumok felületét különböző jelmondatokkal láttak el a Bibliából idézve.

[2] a pontos megfogalmazás szerint természeti csapás, baleset, káreset, rendellenes technológiai folyamat, műszaki meghibásodás, veszélyes anyag szabadba jutása vagy egyéb cselekmény által előidézett veszélyhelyzet során az emberélet, a testi épség és az anyagi javak védelme érdekében a tűzoltóság részéről - a rendelkezésére álló, illetőleg az általa igénybe vett eszközökkel - végzett elsődleges beavatkozói tevékenység

A fenti feladatokat a társadalom, az egyes nemzetek saját fejlődésük és döntésük alapján végzik. Nézzük meg nemzetközi összehasonlításban – közeli országokra tekintve - a tűzoltósági megelőzési és beavatkozói tevékenység ellátását.

Romániában a katonaság szervezetéhez tartoznak a tűzoltóságok, a legutóbbi átszervezést követően megyei veszélyhelyzeti főfelügyelőség látja el az egyes adott földrajzi területeken található tűzoltóságok szakmai irányítását és ellenőrzését. Külön speciális egységként egészségügyi mentőszolgálattal is rendelkeznek az állami, kórházi mentőszolgálat mellett SMURD[3] rövidített néven.

Szlovákiában a belügyminiszter irányítása alatt Tűzoltó és Mentő Erők-ként került megnevezésre a jelen cikk témáját lefedő tevékenységet ellátó szervezet, érdekességképpen a megyei eső számú vezetők az elnökök, Szlovákia első számú tűzoltóparancsnoka pedig az országos elnök vezetve az elnökségnek nevezett szervezeti egységét.

Lengyelországban szintén és a nevében is állami tűzoltóság működik és hasonlóan a többi országhoz, a speciális mentési feladatokra is készen állnak a hagyományos, hétköznapinak tekinthető tűzoltási és műszaki mentési, katasztrófavédelmi feladatok mellett.

Magyarországon 2012-ben történt meg az előtte működő és egyenként önálló hivatásos önkormányzati tűzoltóparancsokságok integrálása a hivatásos katasztrófavédelmi szervezetbe, közismertebb nevén a katasztrófavédelembe. Ezen túl az adott év április elsejével megtörtént a már integrált hivatásos tűzoltóságokkal közösen a teljes katasztrófavédelem átszervezése. Hármas fő feladatrendszer került meghatározásra (tűzoltóság, polgári védelem, iparbiztonság), új szervezeti struktúra és bővebb körű szervezeti egységek álltak fel helyi, megyei és országos szinten. A szervezet tevékenységi köre a nemzetközi kitekintésben említetteknek megfelelően igen széles körű, egyes esetekben a legbővebb (pl. iparbiztonsági tevékenységek).

KUTATÁS A KATASZTRÓFAVÉDELEM BEAVATKOZÁSI TEVÉKENYSÉGÉNEK FEJLESZTÉSÉRE

A tudományos kutatás segítségével történő szervezet és tevékenységfejlesztés az élet minden területén megjelenik. A katasztrófavédelem, a tűzoltóság területe sem lehet így kivétel, az elmúlt évtizedekben sok példa erősíti ennek a tevékenységnek a védelmi területre való ráhatását.

Egy ide vonatkozó területet tárgyaló cikkből idézve:

„Az államtudomány új kereteit a jog és a közigazgatás, a védelem (rendvédelem, honvédelem, katasztrófavédelem), a közrend és biztonság (nemzetbiztonság), és más az állammal és a társadalommal kapcsolatos kérdések kutatása adja. E fenti megközelítés alapján látható, hogy az államtudományok alapvetően a társadalomtudományok területén érvényesülnek, azonban azt is látni kell, hogy az állam hatékony, fenntartható, biztonságos működéséhez és működtetéséhez mindig is szükségesek voltak a különböző műszaki kutatási eredmények és azok felhasználása.” [1]

Jelen írás is egy kutatási projekt részeleme melynek címe: A jó állam biztonsági kihívásai és fejlesztési alternatívái a katasztrófák elleni védekezés technikai fejlesztésében. Az egy felsőoktatási intézményben folyó kutatás egyben közvetlen hatással van – az érintett

[3] a SMURD román rövidítés: Serviciul Mobil de Urgenţă, Reanimare şi Descarcerare, azaz mobil veszélyhelyzeti kiszabadítási és újraélesztési szolgálat. A megnevezéshez egy közelebbi tevékenységi kör, közúti balesetek során a sérültek kimentése a roncsolódott gépjárművekből és a szükség stabilizálási vagy újraélesztési feladatok ellátása. A SMURD mentőautói a hagyományos mentőgépjárművekkel azonosan felszereltek, a tűzoltói szakfelszereléseket az egyszerre riasztott tűzoltó gépjárművek tartalmazzák.

rendvédelmi szervezet mellett – a további hasonló kutatói tevékenységekre és a felsőoktatás vonatkozó területére is. [2] [3]

Egy erről szóló publikációban jelen írás szerzője is ide tartozóan megjelentette: „A megelőző tűzvédelem korábbi normatív szabályozása helyett ma a mérnöki módszerek előtérbe kerülésével szembesülhetünk, amely megfelelő tűzvédelmi mérnöki kultúra biztosítása esetén lehet hatékonyabb. A tanszéken való oktatás magas színvonalához ezért felhasználjuk a hazai felsőoktatási kapcsolatainkat, így a Szent István Egyetem Ybl Miklós Építéstudományi Kar Tűz - és Katasztrófavédelmi Intézetének Tűzvédelmi Laboratóriuma, valamint a Budapesti Műszaki és Gazdaságtudományi Egyetem Építőmérnöki Kar Építőanyagok és Magasépítés Tanszék Laboratóriuma által nyújtott lehetőségeket. A gyakorlati képzés teljessé tételéhez szükséges, hogy rendszeres és kiváló kapcsolatot ápoljunk a BM Katasztrófavédelmi Oktatási Központtal, a Fővárosi Katasztrófavédelmi Igazgatósággal, valamint felhasználjuk a BM Országos Katasztrófavédelmi Főigazgatóság által nyújtott lehetőségeket is.” [4]

A tudományos kutatás és a felsőoktatás igen szoros kapcsolata a következő, szintén a vizsgált területről származó írás alapján: „Ahhoz, hogy a hatóság a veszélyes üzemekkel kapcsolatos, megnövekedett számú feladatait hatékonyan és minőségileg el tudja látni, fontos, hogy az ezeket a feladatokat végző szakemberek rendelkezzenek a szükséges ismeretekkel, így a megfelelő szaktudást biztosító, magas szintű képzésük – ezen belül bizonyos szintű kémiai és technológiai ismeretek elsajátítása – elengedhetetlen. A Nemzeti Közszolgálati Egyetemen több vegyészeti jellegű tantárgy oktatása folyik, melyek célja a képzésből kikerülők szakértelmének biztosítása. Ezek a tantárgyak egymáshoz kapcsolódva, egymásra épülve készítik fel a hallgatókat a későbbi munkájuk során alkalmazandó ismeretekre.” [5]

Természetesen – sajnos és közismerten – tűzoltói beavatkozások kiemelten hordoznak magukban biztonsági kockázatokat a beavatkozó erők számára. [7] „A minél előbbi beavatkozás a sérültek, az életveszélyben lévők számára is nagyobb biztonságot nyújt, valamint a rövidebb vonulási idő miatt a kármennyiség sem tud akkora mértékben növekedni, például egy tűzeset során. Amennyiben a gyorsabb elsődleges beavatkozás során a tűz terjedése mérsékelhető vagy egy műszaki mentés során a felderítési és beavatkozási feladatok rövidebb idő alatt elvégezhetőek, kisebb tűzoltói erőkre lehet szükség, és a káreset veszélyszintje is feltételezhetően csökkent mértékű lehet.” [8] A biztonsági kockázat fennáll a káreset helyszínén minden jelenlévőre, azonban ennek a kockázatnak a mértéke csökkenthető több irányon keresztül is, amint a kérdéskörre vonatkozólag a szerző egyik írásában meg is fogalmaz: „Feltételezés, hogy a tűzoltói beavatkozások során a hatékony beavatkozás fogalma nem jelenti a beavatkozás vagy a beavatkozó tűzoltó biztonságának háttérbe szorítását. Egy hatékony tűzoltói kárfelszámolás megfelelően gyors a mentendő személy érdekében, szem előtt tartja a mentőerők biztonságát, amely magával vonja a készenlét mielőbbi visszaállítását is.” [9]

A JOGI SZABÁLYOKHOZ VALÓ KAPCSOLÓDÁSA A TERÜLETNEK ÉS A KUTATÁSNAK

A kutatási terv alapozása szerint, a széleskörű halmazból a részekre tekintve: Magyarország kormánya a 2014-2020 közötti Közigazgatási- és Közszolgáltatás-fejlesztési Stratégiájában külön intézkedésként fogalmazta meg a közszolgáltatások színvonalának javítását. A közszolgáltatásokhoz kapcsolódó szervezetrendszer hatékonyabbá tétele ezen intézkedésen belül nevesített alponton belül jelenik meg. A Kormány célul tűzte ki, hogy 2014-2020 között felül kell vizsgálni, hogy melyek azok a közszolgáltatások, amelyek piaci alapokon működtethetőek, és akár egy kormányzati szerv is eredményesen tudja nyújtani az adott közszolgáltatást. Ezen stratégiában ehhez kapcsolódóan a közszolgáltató szervezetek menedzsmentjének, szolgáltatási minőségének és kapacitásának átfogó fejlesztése is nevesített

célként jelenik meg. Deklarálásra került a stratégia, hogy a hatékonyan működő intézményrendszer szükséges, de nem elégséges feltétele a hatékony, az ügyfelek számára megfelelő minőségű közszolgáltatás biztosításának, ugyanis magának az adott szervezetnek is hatékonyan kell működnie, amelynek az alapja a szervezet fejlesztése.

Itt érthetjük úgy, hogy a témakörre vonatkoztatva a cél magának a katasztrófavédelemnek és azon belül a kutatási tevékenységnek megfelelően a beavatkozó tevékenységnek a fejlesztése elérendő cél kormányzati elvárás szerint is. A hatékonyság növelése, az ügyfél elégedettsége vonatkoztatható a rövidebb kiérkezési időre, gyorsabb kárfelszámolásra, magasabb megmentett értékre, kisebb mértékű személyi tárgyi sérülésekre vagy biztosabban megmentett emberi életekre. Egy előző és vonatkozó írás alapján: *„ …már igen hamar konkrét eredményeket lehet elérni egy megfelelő… …gyakorlat végrehajtásával, valamint további képzési és kísérleti lehetőségek is nyitva állnak az adott környezetben. Rövid távon egyes szempontok szerint (mint például a légzőkészülékes levegő-felhasználási liter/perc arány) nem biztos, hogy eredmény érhető el, azonban két erős pozitívum ekkor is megjelenik. Az egyik a hatékonyabb és biztonságosabb feladat-végrehajtásból adódó gyorsabb eseménykezelés, így a kevesebb felhasznált levegőmennyiség..”* [10]

A jogszabályi háttért tekintve jelen kutatás tervezetéből: A kutatás Alaptörvénybeli és jogszabályi kapcsolódási egyik pontja Magyarország Alaptörvénye, melynek G cikkének 2. pontja kimondja: „Magyarország védelmezi állampolgárait”. A XX. cikk alapján: *„Mindenkinek joga van a testi és lelki egészséghez.”* Ezen jog érvényesülését Magyarország a környezet védelmének biztosításával is elősegíti. Az Alaptörvény XXVI. cikkében foglaltak szerint: „*Az állam a működésének hatékonysága, a közszolgáltatások színvonalának emelése, a közügyek jobb átláthatósága és az esélyegyenlőség előmozdítása érdekében - törekszik az új műszaki megoldásoknak és a tudomány eredményeinek az alkalmazására.”*

A katasztrófavédelem, mint a fenti pontokban említett védelem egyik biztosító szervezet, tevékenysége során ellátja Magyarország állampolgárainak és az ország területén tartózkodók katasztrófavédelmi, tűzvédelmi és mentő tűzvédelmi szempontú védelmét, figyelemmel életükre és testi épségükre, vagyonbiztonságukra. Az Alaptörvény által adott állami garanciák egyik biztosítója tehát a hivatásos katasztrófavédelmi szervezet valamint a különböző jogállású tűzoltóságok (önkormányzati, önkéntes, létesítményi).

„A felsőfokú végzettségű és tiszti állományú szakembereinek mindenkori utánpótlásáról elsősorban a Katasztrófavédelmi Oktatási Központ és a Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézete gondoskodik. A folyamatosan a szervezetre terhelődő újabb felelősségi körök között mind a három szakterületet érintően találunk újabb feladatokat.” [11]

„Az Intézetnél a „megrendelők”, azaz a BM Országos Katasztrófavédelmi Főigazgatóság és területi szervei, a megyei katasztrófavédelmi igazgatóságok számára az említett három szakterületnek megfelelően a három tanszék szervezi és végzi az oktatási tevékenységet BSc, MSc szinten, valamint részt vesz a kapcsolódó tárgyak oktatásában a PhD doktori képzés során. A három tanszék a tűzvédelmi és mentésirányítási, katasztrófavédelmi műveleti és az iparbiztonsági tanszékek.” [12]

Az állam amint látható, egyértelműen törekszik az új műszaki megoldások és a tudomány különböző eredményeinek alkalmazására. Ez a törekvés megjelenik már nyíltan maguknál a minisztériumoknál is. Erre lehet példa a Belügyi Tudományos Tanács, melynek elnökének szavai szerint: *„A belügyi tudományos munka olyan kutató, alkotó, tudományszervező tevékenység, amely a rendészettudomány valamennyi területére kiterjed. Célja az ágazatban létrehozott tudományos értékek feltárásának elősegítése, a tudományos eredmények gyakorlatban történő alkalmazásának előmozdítása, továbbá a rendészettudomány tudomány-rendszertani helyének, szerepének erősítése, valamint tárcaszintű koncentrációja.”*

A 2011. évi CXXVIII. törvény által került megalkotásra „a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló” jogszabály, ami a következő

preambulum szerint: „Az Országgyűlés, a lakosság biztonságának és biztonságérzetének növelése céljából, a természeti és civilizációs katasztrófák elleni védekezés hatékonyságának fokozása, a katasztrófavédelmi szervezetrendszer erősítése, a katasztrófavédelmi intézkedések eredményességének növelése érdekében az Alaptörvény végrehajtására, az Alaptörvény XXXI. cikk (5) és (6) bekezdése, 53. cikke és 54. cikke alapján a következő törvényt alkotja".

A fenti törvény szövege szerint a katasztrófavédelem nemzeti ügy, a védekezés egységes irányítása pedig állami feladat. Az általánosnak tekinthető tűzoltósági beavatkozásokon túl a kiemeltebb káresetekre gondolva és idézve a katasztrófavédelmi törvény szövegét „A védekezést és a következmények felszámolását az erre a célra létrehozott szervek és a különböző védekezési rendszerek működésének összehangolásával, az állampolgárok, valamint a polgári védelmi szervezetek, a gazdálkodó szervezetek, a Magyar Honvédség, a rendvédelmi szervek, a Nemzeti Adó- és Vámhivatal, az állami meteorológiai szolgálat, az állami mentőszolgálat, a vízügyi igazgatási szervek, az egészségügyi államigazgatási szerv, az önkéntesen részt vevő civil szervezetek és az erre a célra létrehozott köztestületek, továbbá nem természeti katasztrófa esetén annak okozója és előidézője, az állami szervek és az önkormányzatok bevonásával, illetve közreműködésével kell biztosítani."

Amint látható, az egyes helyi - készenléti - rendvédelmi vagy egyéb szervezetek által nem kezelhető káresetek esetén deklaráltan megjelennek a kötelező közreműködések a különböző társszervezetek (állami, önkéntes, állampolgári) részéről.

A hivatásos katasztrófavédelmi szervezet, a tűzoltóságok a téma szempontjából vonatkozó törvényi megjelenése az 1996. évi XXXI. törvény[4] alapján (tűzvédelmi törvény) egyértelmű:

Az 1. §-ból: „E törvény hatálya kiterjed Magyarország területén folytatott, a tűzvédelemre kiható valamennyi tevékenységre és a tűzoltóság által végzett műszaki mentésre."

A 2. §-ból: „A tűzoltás és műszaki mentés állami feladat."

Szintén a fenti törvény alapján: „A tűzvédelemmel és a műszaki mentéssel kapcsolatos kötelezettségeket az e törvény hatálya alá tartozóknak a jogszabályokban, szabványokban, hatósági előírásokban meghatározottak szerint kell teljesíteni." Az említett jogszabályokra és a kutatás témája szerinti – rendvédelmi – tevékenységre jó példa a 39/2011. (XI. 15.) BM (belügyminiszteri) rendelet, a tűzoltóság tűzoltási és műszaki mentési tevékenységének általános szabályairól. Ennek szövege alapján a katasztrófavédelem, a tűzoltóságok beavatkozásainak hatékonyságnövelése, a technikai eszközhasználat fejlesztése kutatás és a szervezet által ellátott beavatkozó, mentő tűzvédelmi tevékenység közvetlen kapcsolatot mutat:

A harmadik paragrafus alapján: „A tűzoltás és műszaki mentés szabályain a tűzoltás és a műszaki mentés irányításának, szervezésének, vezetésének, előkészítésének és végrehajtásának szabályait, valamint a beavatkozásban részt vevők kötelességeit és jogait kell érteni."

„A tűzoltóság a tudomására jutott tűzesethez és a műszaki mentést igénylő esetekhez - a már eloltott és utólagosan bejelentett tűzesetek kivételével - biztosítja a feladat végrehajtásához rendelkezésre álló és szükséges erők, eszközök kirendelését, a helyszínre haladéktalanul kivonul, az életveszélyt elhárítja, a tűz továbbterjedését megakadályozza, a tüzet szakszerűen eloltja, a műszaki mentést elvégzi és a tűzvizsgálati cselekmény elvégzése érdekében szükséges feladatokat végrehajtja. A tűzoltóság a tudomására jutott utólagosan bejelentett és eloltott tűzeset helyszínén - amennyiben a bekövetkezett tűzeset eloltása és a tudomásra jutás közötti időszak a 2 órát nem haladta meg - intézkedik a helyszín biztosítása, és a szükséges tűzvizsgálati cselekmény elvégzése érdekében."

[4] a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

Az hogy egy káreset helyszínén meddig terjed a beavatkozó katasztrófavédelmi, tűzoltói erők beavatkozása, kárhelyszíni elsődleges irányítása a rendelet alapján a következőképpen került szabályozásra: „Az elsődleges beavatkozás addig tart, amíg a közvetlen veszélyhelyzet meg nem szűnt, vagy az esemény felszámolásának irányítását az irányításra jogosult szervezet átvette. A tűzoltóság ezután e rendeletben foglalt feladatait az átvételre jogosult szervezet irányítása mellett végzi."

Az, hogy Magyarország területén földrajzilag milyen területeken kell tűzoltói beavatkozást végrehajtani, a következőképpen van meghatározva a fenti BM rendeletben:

„A műszaki mentési tevékenység során különösen

a) az épületkároknál, építménybaleseteknél,

b) a közlekedési baleseteknél,

c) a természetes vizekben bekövetkezett baleseteknél,

d) a csatornákban, kutakban és egyéb víztározókban bekövetkezett baleseteknél,

e) a közüzemi berendezések, közművek meghibásodásával összefüggő veszélyhelyzeteknél, baleseteknél,

f) a magasban, mélyben, föld alatti üregekben (barlangokban, szakadékokban) bekövetkezett baleseteknél,

g) a veszélyes anyagok szabadba jutásánál, nukleáris baleset során,

h) a természeti csapások során és minden hasonló esetben

az élet- és a vagyonmentés, valamint az alapvető élet- és vagyonbiztonság érdekében végrehajtott tűzoltói feladatokat kell érteni."

Amint látható, nem véletlenül lehet a híradásokban a lehető legkülönbözőbb káresetek során látni a katasztrófavédelem tűzoltó egységeit.

A jogszabályi környezet ismertetése végén a szóban forgó belügyminiszteri rendelet 51. paragrafusát érdemes megemlíteni, amely alapján láthatóak a rendvédelmi szerv több feladata közül (pl. tűzoltás) az egyik (műszaki mentés) során végzendő tevékenységek:

„A műszaki mentés során végrehajtandó főbb feladatok

a) az életmentés,

b) a közvetett és közvetlen élet- és balesetveszély elhárítása,

c) az állatok, tárgyak és anyagi javak mentése értékük, pótolhatatlanságuk, az állatjóléti szempontokra vagy funkcionális fontosságukra tekintettel,

d) az esemény által okozott további környezeti károk mérséklése,

e) a közlekedési forgalom helyreállításának elősegítése.

A hivatásos katasztrófavédelmi szerv radiológiai, biológiai, vegyi felderítést és mentesítést végez, amennyiben az a műszaki mentésre vonatkozó jelzés, vagy a helyszíni felderítés alapján indokolt." [13]

A kutatás, melynek részeként íródik ezen írás is a jó állam biztonsági kihívásai és fejlesztési alternatívái a katasztrófák elleni védekezés technikai fejlesztésében céllal kerülne megvalósításra. Amint a fenti részletes példákból látható: kapcsolódik az Alaptörvényhez a katasztrófavédelem által ellátandó személyi-, vagyoni-, és környezetvédelmi feladataival. Az Alaptörvényhez való közvetlen kapcsolat megjelenik továbbá az új műszaki megoldásoknak és a tudomány eredményeinek alkalmazásában közösen mind a katasztrófavédelem szervezetében és mind a Nemzeti Közszolgálati Egyetemen. A kutatás vezetője – jelen írás szerzője – egyben az érintett rendvédelmi szervezet, a hivatásos katasztrófavédelmi szerv tagja, valamint a kutatóhely Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet tűzvédelmi és mentésirányítási tanszék oktatója és kutatója.

A KUTATÁS CÉLJA ÉS TEVÉKENYSÉGE

A jó állam fogalmába tartozóan a megfelelő és jó kormányzás része a lakosság életének, testi épségének és anyagi javainak biztosítása. A rendvédelem területén és azon belül a

katasztrófavédelem tevékenységei során a tűzoltók számára biztosítani szükséges a lehető legmagasabb szintű egyéni védelmet, ami közvetlen kapcsolatot jelent a beavatkozás biztonságára, hatékonyságára is.

Jelen kutatás során a katasztrófavédelem beavatkozási célú szervezeti egységei, tűzoltósági erői kerülnek vizsgálatra a különböző szakmai tevékenységek, tűzoltások, műszaki mentések hatékonyságnövelése céljából. *„Országunkban a nap minden órájában és annak minden percében mintegy kétezer fő tűzoltó áll folyamatosan készenlétben annak érdekében, hogy riasztás esetén 120 másodpercen belül elindulhasson a jelzés szerinti káresethez."* [14] A jelenleg használt megoldások megfelelőbb használati módjának és az elérhető új típusú légzésvédelmi eszközök alkalmazhatóságának kutatására, adaptálhatósági vizsgálatára kerül sor.

Nem csak a hazai lehetőségek áttekintése, hanem nemzetközi kitekintésre és összehasonlítási folyamatok során a legjobb módszerek és tapasztalatok megtalálására van lehetőség.

A cél a Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézeténél lefolytatott kutatás által a katasztrófavédelmi, tűzoltói hatékonyság és egyben a beavatkozás biztonságának növelése. Mind a Nemzeti Közszolgálati Egyetem, mind a hivatásos katasztrófavédelmi szervezetre értve: *„A szervezet számára elsőrendű, hogy a megnőtt felelősségi körök ellátásához a megfelelő beosztásokban megfelelő képzettséggel, ismeretekkel rendelkezők lássák el a szolgálatot."* [15]

A várható eredmények közvetlen haszonnal járhatnak a lakosság élet és vagyonbiztonságára, a jó tapasztalatok nemzetközi szinten is publikálhatóakká válnak. Maga az egyetemi oktatási és kutatási tevékenység is jól tudja használni a kapott adatokat, elért eredményeket.

A BEAVATKOZÓI HATÉKONYSÁG ÉS A BIZTONSÁG NÖVELÉSÉNEK VÁRHATÓ EREDMÉNYEI

A várhatóan egy év időtartamú kutatás alapján a fenti cél elérhető, lefolytatható. Az eredmények folyamatos hazai és nemzetközi publikálhatóságára jó lehetőségek állnak rendelkezésre. A katasztrófavédelmi, tűzoltósági kárfelszámolási hatékonyság és a beavatkozás biztonságának növelése, a légzésvédelem fejleszthetőségének vizsgálata megvalósulhat úgy, hogy ezen a területen az elmúlt években kiemeltebb hazai tudományos kutatások nem történtek. *„A személyi, a beavatkozói biztonság mellett tehát a beavatkozás biztonsága, mint az azonnali életveszélyben lévők mentése, a közvetlen élet és balesetveszély elhárítása tevékenység lehetőségekhez és a körülményekhez képesti minél jobb módszerekkel való véghezvitele is fontos és elsőrendű."* [16]

Gyakorlati tapasztalatok, önálló tudományos eredmények születnek a tűzoltósági operatív tevékenységek, a jelenleg használt légzésvédelmi eszközök és eljárások területén. A legjobb gyakorlatok a katasztrófavédelmi, tűzoltói beavatkozások területén, azok hatékonyságát célzóan valamint a légzésvédelmi nemzetközi megoldások, gyakorlatok és tapasztalatok megtalálására igen jó lehetőségek nyílnak. A konkrét szakmai és tudományos eredmények elérését követően megvizsgálásra kerülnek az új megoldások integrálási lehetőségei.

Mind a szakmai terület számára, mind az egyetemi oktatás számára új eredmények és ismeretek érhetőek el. Egy végső összefoglaló műben bemutatásra kerülnek az elért és bizonyított eredmények továbbá a folyamatosan keletkező részeredmények publikálása megtörténik a hazai és a nemzetközi szakirodalomban. A nemzetközi szintű konferenciákon, tudományos eseményeken és szakmai konzultációkon a kutatás során megszerzett részkövetkeztetések külföldön történő megismertetésére igen jó lehetőségek állnak rendelkezésre. A hazai kutatás nemzetközi szintű szakmai, tudományos szintű elismerésére, a

Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézeténél folyó oktatói és kutatói tevékenység nagyobb elismertségére lehet számítani.

A KONKRÉT KUTATÁS FELÉPÍTÉSE, ANNAK FOLYAMATA

Az első szakasz

A 2017. január elejétől várhatóan 2017. április végéig terjedő időtartam került meghatározásra a kutatás első szakaszára. Itt a kutatás alapozó tevékenységeinek elvégzésére kerül sor. A Hipotézisek alapján a hazai katasztrófavédelmi, tűzoltósági beavatkozásainak hatékonyságán légzésvédelmi eszköz használata esetén (azt igénylő káreseteknél) lehet javítani akár más vagy újabb típusú eszközök használatával, akár eljárásrendek, kiképzési módok módosításával. A kutatási szakaszban megtörténik a katasztrófavédelem szervezetének és a különböző jogállású tűzoltóságok rendszerszintű vizsgálata. Ezen vizsgálatok során a katasztrófavédelem helyi szerveinek (kirendeltségek és tűzoltó-parancsnokságok) valamint azon megyei szintű szervezeti egységek elemzésére kerül sor, amelyek a beavatkozásokban közvetlenül érintettek (pl.: katasztrófavédelmi műveleti szolgálat, katasztrófavédelmi mobil labor, műveletirányítás). Az elmúlt évek beavatkozásainak elemzése alapján, a kutatás során megalkotott szempontrendszer szerint megtörténik a statisztikai alapozó adatbázis létrehozása. Ebből az adatbázisból lehet következtetni a jövőbeli tendenciákra és így a várható tűzoltói beavatkozásokra is. Néhány a gyűjtésre és elemzésre kerülő főbb adatok köréből a katasztrófavédelmi és tűzoltói beavatkozásokkal kapcsolatosan: műszaki mentések, tűzesetek száma, a kárértékek, a sérült/elhunyt személyek, a használt technikai eszközök és járművek, stb.

A hazai vonatkozó légzésvédelmi eszközök használatát érintően konkrét mérések és azok előkészítései történnek az idő, levegőfogyasztás, felhasznált levegőmennyiség, stb. körében. Ezen megszerzett valamint az elérhető egyéb mérési eredmények adatbázisban kerülnek rögzítésre, továbbkutatható formában. A kutatás végső céljához - a fenti alapadatok gyűjtésével és ebből következtetések levonásával - a lehető legközelebbi várható eredmények, a legmegfelelőbb hatékonyságnövelési és légzésvédelmi megoldások választhatóak ki. Az első szakaszban sor kerül továbbá a magyarországi katasztrófavédelem szervezetében jelenleg használt légzésvédelmi eszközök rendszerezésére, elemzésére, a használati módjuk vizsgálatára. Itt különösen a jelenleg használt különböző típusok és azok mennyisége, a rendszerben való feltalálási helyük, a használati eljárásrendek szabályozottsága lesz a kutatási tevékenység. A megszerzett és elért eredmények publikálására sor kerül mind folyóiratokban, mind a vonatkozó és elérhető hazai és nemzetközi konferenciákon.

A második szakasz

Ezen szakasz kutatási terv szerinti időtartama 2017 májusától fog tartani 2017 szeptemberéig. Az első szakaszban foglalt alapozó kutatásokra épülve a nemzetközi környezet vonatkozó adatai és a külföldi tendenciák vizsgálata is megtörténik. Nemzetközi vonatkozó adatokkal bővül a kutatási adatbank a katasztrófavédelmi, tűzoltósági beavatkozó szervezetekről, azok esetszámáról, a feltalált jó hazai és nemzetközi módszerekről. Külön adatbázis készül a kutatás segítéséhez európai és nem európai országok elérhető adatainak felhasználásával. A külföldi kitekintés során különösen a már az első szakaszban elért adatokhoz kapcsolódó információk megszerzése, rögzítése történik meg országonként és összesített formában is. Ilyenek például a műszaki mentések, tűzesetek száma a közelmúltban, azok változása évről évre, a hivatásos vagy egyéb jogállású tűzoltóságok száma és azok létszáma, az elérhető technikai eszközeik, eltérések a hazai lehetőségektől, stb. A technikai eszköz jellegű vizsgálat során a külföldön használt légzésvédelmi célú eszközök áttekintésére is sor kerül a használati

eljárásrendekkel egyetemben. Ezen információk a kutatási adatbázis nemzetközi részében kerülnek rögzítésre. Cél a legjobb gyakorlatok megtalálása az adaptálhatóság vizsgálatának megalapozására. Az elérhető légzőkészülék használattal kapcsolatos nemzetközi mérési eredmények összegzése mellett a lehetőségek szerinti mértékben külön mérések végzésére is sor kerül az első szakasz céljaival összhangban. A szakaszban elért kutatási eredmények publikálására sor kerül a szakmai, tudományos folyóiratokban, a vonatkozó és elérhető konferenciákon. Lehetőségek szerint a kutatási részeredmények külföldi publikálására figyelem fog fordítódni.

A harmadik szakasz

Az egy éves időtartamra tervezett kutatás három szakaszra tagolódott, így a harmadik a végső szakasz. Ennek időbeli határoltsága 2017 szeptemberétől 2017 december végére került tervezésre. Az első és a második szakaszban megszerzett szervezeti, működési és a légzésvédelmi célú technikai eszközökkel kapcsolatos mérési adatok, konkrét kutatási eredmények szintézisére kerül sor. Az elkészült hazai és nemzetközi, beavatkozási és technikai adatokat tartalmazó adatbázis felhasználásra kerül, következtetések levonásával kidolgozásra kerülnek konkrét javaslatok a tűzoltói beavatkozások hatékonyságnövelésére, a légzésvédelmi eszközök használati területén megtehető lépésekre. A nemzetközi szinten szerzett legjobb gyakorlatok, módszerek, technikai eszközök adaptálhatóságának vizsgálata megtörténik, konkrét javaslatok kerülnek kidolgozásra azok magyarországi alkalmazhatóságára valamint az esetleges negatív példák elkerülésére. Elérésre kerül a kutatási cél, a katasztrófavédelem beavatkozó tevékenységének hatékonyságnövelése a légzésvédelmi terület fejlesztésével. Várhatóan konkrét eredmények születnek a légzésvédelmet igénylő beavatkozások során a benntartózkodási idő növelésére, a tűzoltót érő terhelés és veszélyt jelentő kockázatok csökkentésére, a telemetriai eszközök alkamazhatóságára. A feltett hipotézisek részét képező, a vonatkozó kárfelszámolások hatékonyságnövelésére várhatóan egyértelműen bizonyításra kerül. Mind a folyamatosan elért kutatási eredmények, mind a végső összegzett kutatási eredmények publikálásra kerülnek az elérhető konferenciákon és a folyóiratokban. Elkészül a teljes kutatást és az abban elért eredményeket összefoglaló mű. Ennek a szakasznak és így egyben a teljes kutatás végére a nemzetközi publikációk is elkészülnek, valamint a különböző kiadványokba megküldésre kerülnek.

A kutatás nemzetközi szintje

A katasztrófavédelem, a mentő tűzvédelem mindenhol megjelenik a világon ahol emberek élnek társadalomban. Minden nemzet a saját biztonságát a saját maga által meghatározottak alapján látja el, figyelemmel az elérhető gazdasági lehetőségekre. A sokszínű világunkban biztosan vannak olyan pontok, megoldások, eljárások, technikai eszközök, amelyeket megfelelő megelőző vizsgálatok alapján integrálni lehet a magyarországi környezetbe, elérhető és reális gazdasági erők ráfordításával.

A legjobb gyakorlat, jó gyakorlat[5] megtalálása érdekében a kutatás során több nemzetközi kitekintésre is sor kerül. A magyarországihoz közelebbi, adaptálható lehetőségek elérése

[5] A jó gyakorlat vagy bevált gyakorlat (angolul best practice) a vállalati menedzsment és minőségbiztosítás területén olyan, rutinszerűen végzett tevékenységre utal, ami széles körű tapasztalatokon alapul, és több szervezetben is sikeresnek bizonyult. Gyakran nevezik az angol kifejezés tükörfordításaként félrevezetően „legjobb gyakorlatnak”. Ez azonban nem helytálló, hiszen semmilyen (adott körben vagy időszakban bevált) gyakorlat nem garantálja, hogy nem létezik nála jobb gyakorlat. Forrás: Wikipédia, letöltve: 2017.02.23.

érdekében nem csak egy, hanem széleskörű külföldi tapasztalatszerzés indokolt és egyben tervezett is. Ezek megvalósulása érdekében anyaggyűjtésre kerül sor V4 országokban: Románia, Szlovákia, Lengyelország. A szélesebb körű, gazdaságilag erősebb országok által használt eszközbeli vagy eljárásbeli megoldások megtalálása érdekében tervezés alatt áll a kutatás Németországra, Egyesült Államokra és Oroszországra való kibővítése is.

KÖVETKEZTETÉSEK

A cikk egy nagyobb kutatás (a katasztrófavédelem beavatkozó képességének hatékonyságnövelése) keretéről (jogszabályi, területi), annak alapjairól (a kutatási terv egyes részletei, vonatkozásai) adott általános információkat, megadva a kutatás környezetét, igényét és hasznosságát.

A kutatás folytatója és egyben jelen cikk szerzője a kutatás várható eredményeiről, annak felhasználhatóságáról igen bizakodott. Ismerve a hazai és a nemzetközi vonatkozó tárgyú tűzoltói beavatkozó tevékenységeket, a jelenleg folyó magyarországi és külföldi kutatásokat láthatóvá válik, hogy lesznek igen széles körben felhasználható eredmények, melyek jó lehetőséget nyújtanak közvetlen hasznosíthatóságra és további kutatási alapokra egyaránt.

FELHASZNÁLT IRODALOM

[1] BLESZITY J., FÖLDI L., HAIG Zs., NEMESLAKI A., RESTÁS Á.: Műszaki kutatások és hatékony kormányzás, HADMÉRNÖK 11:(3) pp. 221-242. (2016)

[2] BLESZITY J., KATAI-URBAN L., GROSZ Z.: Disaster Management in Higher Education in Hungary, Administrativa Un Kriminala Justicija - Latvijas Policijas Akademijas Teoretiski Praktisks Zurnals 67:(2) pp. 66-70. (2014)

[3] BLESZITY J., DOBOR J., ENDRŐDI I., GRÓSZ Z., KÁTAI-URBÁN L., KRIZSÁN Z., RESTÁS Á.: Kátai-Urbán Lajos, Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet önértékelés intézményakkreditáció, Budapest: BM Országos Katasztrófavédelmi Főigazgatóság, 2016. (ISBN:978-615-80429-2-5)

[4] RESTÁS Á., PÁNTYA P., HORVÁTH L., RÁCZ S., HESZ J.: A tűzvédelem komplex oktatása a Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézetében, In: RESTÁS Á., URBÁN A., Tűzoltó Szakmai Napok 2016. 186 p., Budapest: BM OKF, 2016. pp. 177-181.1-2. (ISBN:978-615-80429-0-1)

[5] DOBOR J.: A kémia és a kémiával kapcsolatos tárgyak oktatásának fontossága a katasztrófavédelmi képzésben, BOLYAI SZEMLE XXIII.:(3) pp. 223-229. (2014)

[6] PÁNTYA P., KALAMÁR N.: A Magyar Katasztrófavédelem Által Végzett Beavatkozások, Védelem Tudomány: Katasztrófavédelmi Online Tudományos Folyóirat 4:(I.) pp. 88-99. (2016)

[7] PÁNTYA P.: A tűzoltói beavatkozás veszélyei, In: Dr DOBOR J., HEGEDŰS H., URBÁN A., Katasztrófavédelem 2014 - Tudományos konferencia. Budapest Nemzeti Közszolgálati Egyetem, 2015. pp. 133-137., (ISBN:978-615-5491-97-9)

[8] PÁNTYA P.: A tűzoltói beavatkozás veszélyes üzem?, BOLYAI SZEMLE 23:(3) pp. 36-42. (2014)

[9] PÁNTYA P.: Hatékonyság vagy biztonság? A tűzoltói beavatkozásokról, In: RESTÁS Á., URBÁN A., Tűzoltó Szakmai Napok 2016. 186 p., Budapest: BM OKF, 2016. pp. 164-167., 1-2., (ISBN:978-615-80429-0-1)

[10] PÁNTYA P.: Eredmények a tűzoltók beavatkozói készségének növelésében, BOLYAI SZEMLE XXIV:(4) pp. 172-180. (2016)

[11] BLESZITY J., GRÓSZ Z., PÁNTYA P., KRIZSÁN Z.: A katasztrófavédelem szak oktatásának aktuális kérdései, BOLYAI SZEMLE 23:(3) pp. 7-13. (2014)

[12] PÁNTYA P.: A katasztrófavédelem szak nappali rendszerű hallgatóinak képzése, szakterületre orientálása, BOLYAI SZEMLE 22:(3) pp. 41-46. (2013)

[13] URBÁN A., RESTÁS Á.: Hűtőruházat alkalmazása a tűzoltók veszélyes anyag jelenlétében történő beavatkozása során, In: RESTÁS Á., URBÁN A., Tűzoltó Szakmai Napok 2016. 186 p., Budapest: BM OKF, 2016. pp. 182-185. 1-2., (ISBN:978-615-80429-0-1)

[14] PÁNTYA P.r: Füsttel telített, zárt terekben történő tűzoltói beavatkozások vizsgálata a biztonság szempontjából = EXAMINING THE SAFETY OF FIRE SERVICE INTERVENTIONS IN SMOKE-FILLED CONFINED SPACE, BOLYAI SZEMLE 22:(3) pp. 47-58. (2013)

[15] PÁNTYA P.: Új kiképzési lehetőségek tűzoltók számára, In: POKORÁDI L.; Műszaki Tudomány az Észak-kelet Magyarországi Régióban 2013: konferencia előadásai. 518 p. Debreceni Akadémiai Bizottság Műszaki Szakbizottsága, 2013. pp. 417-424., (Elektronikus Műszaki Füzetek; 13.), Műszaki Tudomány az Észak-Kelet Magyarországi Régióban, (ISBN:978-963-7064-30-2)

[16] PÁNTYA P.: Lehetőségek a katasztrófavédelmi, tűzoltói beavatkozó biztonság növelésére, In: POKORÁDI L.; Műszaki Tudomány az Észak-kelet Magyarországi Régióban 2014. 435 p. MTA Debreceni Akadémiai Bizottság, 2014. pp. 214-222., (Elektronikus Műszaki Füzetek; 14.), (ISBN:978-963-508-752-5)

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

AZ AGILIS SZOFTVERFEJLESZTÉS ALKALMAZÁSÁNAK LEHETŐSÉGEI A MAGYAR HONVÉDSÉG SZÁMÁRA

POSSIBLE APPLICATIONS OF THE AGILE SOFTWARE DEVELOPMENT FOR THE HUNGARIAN DEFENCE FORCES

GEREVICH János

(ORCID: 0000-0001-7236-4514)

gerevich.janos@agilexpert.hu

Absztrakt

Még a közelmúltban is a hadászat volt az egyik inkubátora a különböző műszaki fejlesztéseknek, előbb jelentek meg egy új technológia katonai alkalmazásai és csak utána következhetett a civil használatba vétel. Példa lehet erre a GPS vagy akár az Internet is. Napjainkra ez a trend változni látszik, vannak olyan műszaki területek, melyek újításait a honvédelem és a hadászat már csak a kifejlődésüket követően veszi át. Egy ilyen terület a szoftverfejlesztés is, jelenleg rengeteg eszközre és architektúrára készülnek a szoftverek különböző programozási nyelveken, szerteágazó technológiai alapokon, funkciók sokaságát megvalósítva. A számtalan új és gyorsan változó követelményhez az informatikának is alkalmazkodnia kellett, új szoftverfejlesztési módszerek jelentek meg, melyek gyűjtőnév gyanánt az agilis szoftverfejlesztési módszertan nevet kapták. Az új módszerek alkalmazásában a sok éves múltra visszatekintő nagy szervezetek általában szkeptikusak, jelen cikk ezt a problémát tárja fel, majd ezt követően egy lehetséges megoldást kínál rá.

Kulcsszavak: *szoftvertechnológia, projekt-módszertan, Scrum, szoftverfejlesztés, szoftvertervezés, automatizált tesztelés, hadiipar, pályázati kiírás*

Abstract

Even in the recent past the army was the incubator of various technical developments, usually a new technology appeared in military applications first and the civil usage just followed it later. For example, it could be the GPS or the Internet as well. Today, this trend seems to be changing. There are innovations in different technical areas which have been adapted by the defence and the military after their inventions only. The software development is such an area, currently uncountable functions are made for wide variety of devices and architectures in different programming languages based on several technologies. The information technology had to adjust to the new and rapidly changing requirements, therefore several new software development methods were born and these are called as agile software development methodologies. Usually the large organizations with long history are sceptical about the new methods; this article helps us to get to know better with this problem and gives us an insight about the possible solution for it.

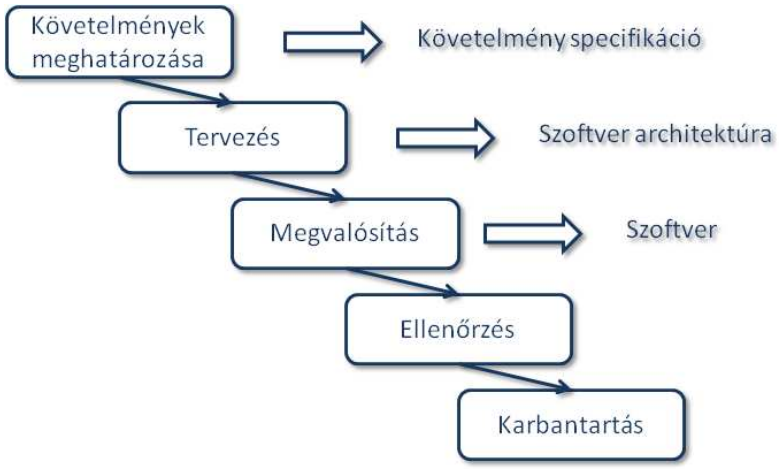
Keywords: *software technology, project methodology, Scrum, software development, software design, automated testing, defence industry, calling for tender*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.15.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.21.

BEVEZETÉS

Napjainkban az informatikai projektek műszaki projektként jelennek meg a köztudatban, ugyanakkor műszaki projekt egy építészeti, gépészeti és természetesen egy szoftverfejlesztési projekt is. Egy tipikus építészeti projekt lehet egy létesítmény megtervezése majd felépítése. Gépészeti projekt lehet egy fegyverfejlesztés. Az építészeti projektek során statikusok, külső és belső építészek finomítják, vizsgálják át a terveket, míg végül egy elfogadott komplett terv születik, mely alapján felépül a létesítmény. Egy gépészeti projektben hasonlóan először a tervek készülnek el, majd a tervek alapján készül el az eszköz, melynek tulajdonságait laboratóriumi körülmények között vizsgálják. A felmerülő hibákat a tervek finomításával és újabb prototípusok készítésével javítják.

A fenti példákban kézzelfogható, fizikailag létrejövő végeredményt kapunk, az építészet kapcsán egy kész épületet, egy eszközfejlesztés esetében egy prototípust. Az informatikai projektek a kézzelfoghatóság szempontjából szerteágazóak lehetnek. Egy szerverpark beüzemelése karakterisztikáját tekintve építészeti projekthez hasonlítható, tervezés, megvalósítás, átadás (tesztelés). Egy informatikai rendszer üzemeltetése hasonlítható egy gépészeti projekthez, ahol létező fizikai és létező szoftver rendszereket hangolnak össze, szabnak testre, majd az együttes működésüket tesztelik, egyfajta prototípusként. Az informatika egy különleges és izgalmas ágazata a szoftverfejlesztés, mely jellegét tekintve eltér az imént említett informatikai projektektől. Az informatikában is évtizedeken át széleskörűen alkalmazták a vízesés modellt [1], amely az alábbi lépéseket azonosítja a projekt megvalósítása során:



1. ábra Eredeti vízesés modell [2]

A fenti statikus modell feltételezi, hogy minden produktív lépés végterméke egy teljes értékű dokumentum vagy megoldás, melyet a későbbiekben már nem kell módosítani. Ez a modell megfelelő lehet egy szoftver alap architektúrájának vagy prototípusának kialakításához, de nehézkesen vagy egyáltalán nem alkalmazható egy változó szoftverre, mellyel kapcsolatban folyamatosan igények merülnek fel a felhasználók, illetve a megrendelő részéről.

Úgy gondolom, hogy itt fontos megjegyezni, hogy minden szoftver esetében két különálló egységet azonosíthatunk: architektúra és funkcionalitás. Az architektúra kialakításhoz a vízesés modell célszerű lehet, azonban manapság ezek a feladatok ritkábban fordulnak elő, mert az informatikai ipar kész architektúrákat biztosít, ezekre példa a .NET Framework [3] vagy a Java Enterprise Edition [4].

Az architektúra kapcsán fontos előre tudni, hogy milyen fizikai eszközökön fog az adott szoftver futni, milyen számítási teljesítménnyel lehet kalkulálni, milyen fizikai környezetben fogják alkalmazni a kifejlesztendő megoldást. Ezen az alkalmazási szinten elengedhetetlen a lépcsőzetes tervezés – megfelelő választás lehet a vízesés modell, azzal a megkötéssel, hogy az elkészülő végtermék egy futtató környezet vagy egy keretrendszer, mely a későbbiekben alapja lehet bármilyen alkalmazásnak a legegyszerűbb oktatói programok és a nagyvállalati szoftverek [5] széles spektrumán. Napjaink alkalmazott szoftverei a két véglet közötti számtalan egyedi alkalmazásra mutatnak példát.

Ha az architektúrát fixnek tekintjük, akkor az adott architektúra által biztosított virtuális térben az egyedi alkalmazások matematikai leképezések halmazaként is tekinthetőek, melyekről akár matematikai módszerekkel is eldönthető, hogy megoldják-e a kitűzött feladatot. [6] Nagyon fontos megjegyezni, hogy az egyedi alkalmazások implementálása során már csak információval dolgoznak a szoftverfejlesztők, ez egy jelentős különbség más műszaki projektekhez képest. Az iménti felismerésből az következik, hogy valójában hatalmas szabadsággal rendelkeznek a programozók a szoftvert futtató virtuális környezetben. Ezért is különösen fontos a megfelelő módszerek, szabályok, technológiák alkalmazása a szoftverfejlesztési projektek során, és ez alól nem lehet kivétel a Magyar Honvédség sem.

A vízesés modell első ránézésre szimpatikus választás lehet katonai alkalmazási területeken. Követelmények meghatározása, funkciók implementálása, tesztelés és végeredményként létrejön az eredetileg kigondolt szoftver. Ha azonban alaposabban megvizsgáljuk a katonai alkalmazási területeket, legyen az béke vagy tábori rendszer, ha felhasználókkal, jogosultságokkal, adatbázisban tárolt adatokkal rendelkezik a kifejlesztendő szoftver, akkor az egy egyedi alkalmazás. A katonai alkalmazások esetében különös tekintettel oda kell figyelni a biztonsági, jogosultsági, megbízhatósági, fenntarthatósági, hibatűrési, katasztrófatűrési szempontoknak, azonban az informatika szemszögéből a katonai szoftverfejlesztés a nagyvállalati szoftverfejlesztés, ezen belül az egyedi alkalmazásfejlesztés egy speciális ágazata és ugyanazokkal a problémákkal kell megküzdenie, amelyekkel a civil szoftverfejlesztésben is találkozhatunk.

AZ AGILIS SZOFTVERFEJLESZTÉS BEMUTATÁSA

A specifikációs erőforrások végessége

Napjaink szoftverei iránt egyre több és több igény merül fel minden alkalmazási területen, nem kivétel ez alól a katonai célú alkalmazás sem. Az igények túlnyomó részben a megvalósítandó üzleti funkciókra vonatkoznak. Az igények megnövekedett száma egy statikus projektmódszertan számára elhúzódó specifikációs időszakot jelent, ráadásul nagyon speciális szaktudást igényel.

A vízesés modell esetében a fejlesztés megkezdéséhez a teljes specifikáció előállítása szükséges, mivel a fejlesztés és a tesztelés alapja ez a dokumentum lesz. A legnagyobb probléma a hagyományos statikus specifikációs módszerekkel, hogy kizárólag írott formában emberi nyelven állítanak elő egy szabályrendszert, nincs direkt kapcsolat a szoftver virtuális világával. A követelményrendszert értelmezni kell és az értelmezés folyamata hibákat rejthet, a szoftver bonyolultsága hatványozottan növekszik a funkciók számához viszonyítva.

A modern kor szoftverei esetében fontos szempont a felhasználói élmény, a letisztult grafikus felület, melyekhez előre elkészített képernyőtervekkel kell rendelkezni egy statikus fejlesztési módszertan esetében is. Sajnos a felületek működését nem lehet meghatározni a rendszer által kezelt adatok nélkül, teljes körű követelményrendszerre van szükség, amit megrendelői oldalon elvégezni nehézkes feladat, későn jelennek meg az első eredmények, csak a fejlesztési, tesztelési időszak végén lehet visszacsatolás. Sok éves szoftverfejlesztői,

rendszerszervezői tapasztalattal rendelkező szakemberek számára is nehézkes ez a fajta specifikációs módszer.

Az agilitás egy válasz az új igényekre

Az üzleti szférában, a civil szoftverfejlesztésben immár 15 éve elindult egy kezdeményezés, mely új alapokra helyezi az informatikai rendszerek, különösen az egyedi szoftverek előállítását. Az a felismerés, hogy a követelményrendszer alacsony szintű meghatározásában a fejlesztőcsapat is részt vehet, ha egy megfelelő üzleti tudással – lehet az hadászat is – rendelkező szakember részesévé válik a fejlesztési folyamatnak új dimenziókat nyitott a szoftverek előállításában. A Kiáltvány az agilis szoftverfejlesztésért [7] című dokumentumot 2001-ben fogalmazták meg korunk vezető szoftvermérnökei, melyhez 12 agilis alapelvet [8] azonosítottak. Az első négy alapelv üzenete az, hogy a megrendelői elégedettséget a folyamatosan jó minőségben előállított szoftverrel lehet elérni, mely megköveteli az aktív megrendelői és beszállítói együttműködést. Ezt követően a kiegyensúlyozott projektkörnyezet és az ütemezett előrehaladás fontossága kerül külön kiemelésre, ezekre azért van szükség, hogy a feladat végrehajtását végzők nyugodt és előre tervezhető munkakörnyezetben tudjanak dolgozni, így egyfajta plusz motivációt kapjanak. Az utolsó négy alapelv a kreatív gondolkodást és a mérnöki szabadság fontosságát hangsúlyozza, abból kiindulva, hogy egy motivált közegben, ahol a megvalósítást végzők magukénak érzik a szoftvert, ott lehetőséget kell biztosítani a saját ötleteik, koncepcióik megvalósítására, amennyiben azok a projekt célját szolgálják.

Az agilis kiáltvány nem definiál konkrét módszertant, csak az alapelveket fekteti le, több agilis módszertan is létezik, köztük az egyik legelterjedtebb a Scrum, amely az alábbi szerepköröket, szereplőket és feladatokat azonosítja:

Product owner / terméktulajdonos – „A projekt vezetésének központi szereplője, aki döntéshozási jogokkal is fel van ruházva, ezáltal egyszemélyes döntéshozóként felelős a kifejlesztendő funkciókért és azok elkészítésének sorrendjéért." [9; 15. o.] Ezen felül a terméktulajdonos további feladatai:

1. Kapcsolattartás az ügyféllel
2. Az üzleti és technológiai követelmények összefogása
3. A minőség ellenőrzése a fejlesztés során
4. Együttműködés a Scrum további szereplőivel (ScrumMaster, Fejlesztőcsapat)

ScrumMaster – „Mindenki számára igyekszik bemutatni és felölelni a Scrum értékeit, alapelveit és gyakorlatát. Egyfajta edzőként lép fel, vezetői szintű folyamatokat határoz meg és segíti a Scrum csapatot, valamint a szervezet fennmaradó részét saját teljesítményének javításában" [9; 16. o.] A ScrumMaster további feladatai:

1. Felmerülő belső és külső problémák megoldása
2. A Scrum hatékonyságának növelése
3. A Scrum-hoz szükséges környezet megszervezése

Fejlesztőcsapat – „A tradicionális szoftverfejlesztési megközelítés különböző szerepköröket tárgyal, például architekt, programozó, tesztelő, adatbázis adminisztrátor, grafikusfelület tervező és így tovább" [9; 16. o.] A fejlesztőcsapat feladatai a Scrum-on belül:

1. Tervezési feladatok ellátása
2. Fejlesztési feladatok ellátása
3. Tesztelés elvégzése
4. Önszerveződés (agilis megközelítés)

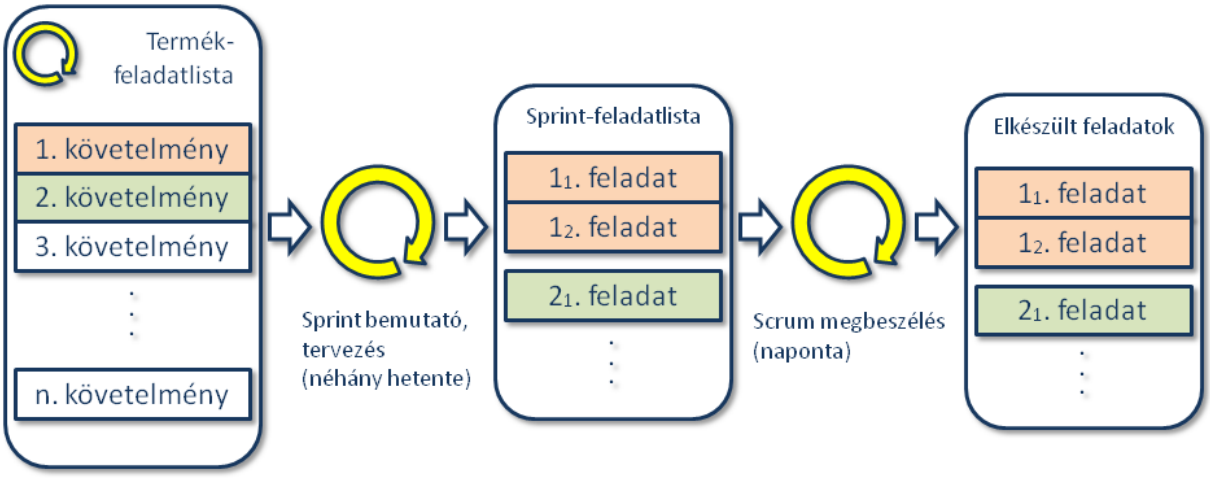
A szoftvertechnológiával foglalkozó irodalomban az ideális szoftverfejlesztő csapat résztvevőinek száma alapvetően eltérő, véleményem szerint egy erős technológia háttérrel rendelkező fejlesztés során ez a szám körülbelül 3-6 fő, tekintettel arra, hogy bizonyos feladatok automatizálhatóak, például: tesztelés, release management. Fontos megemlíteni a Scrum esetében, hogy nem javasolt az alkalmazása a 6-9 főnél nagyobb fejlesztőcsapatok esetében, ilyenkor újabb Scrum csapatok létrehozása ajánlott.

A Scrum egy iteratív szoftverfejlesztési módszertan [10], melynek kiindulási alapja a product backlog avagy a termék-feladatlista, mely a fejlesztés sorrendjében együttesen tartalmazza a termék előállításához szükséges még visszamaradt feladatokat. A fejlesztés elkezdésének pillanatában tartalmaznia kell az addig azonosított összes követelményt. A módszertan lehetővé teszi a követelmények és a sorrend megváltoztatását, feladatok összevonását vagy szétbontását.

Az agilis kiáltvány 3. pontja szerint minél gyakrabban kell működő szoftvert szállítani, a Scrum értelmezésében ez az alapelv a fejlesztések sprintekbe szervezésében nyilvánul meg. Egy fejlesztési sprint egy rövid fejlesztési időszak (általában 1-3 hét), melynek a végén működő szoftvert kell előállítania a fejlesztőcsapatnak, ahol a sprint feladatai a product backlog tetején szereplő legmagasabb prioritású feladatokból kerülnek ki.

Lényeges különbség egy hagyományos módszertanhoz viszonyítva, hogy a sprint-feladatlista előállítása a terméktulajdonos és a fejlesztőcsapat közös feladata, melyet egy erre a célra szánt körülbelül 4 órás közös tervezésen tesznek meg. A tervezések során, a termék-feladatlista tetején szereplő követelményeket a fejlesztőcsapat értelmezi, majd kisebb feladatokra bontja, egyfajta megvalósíthatósági tervet készítve. A fejlesztési sprint során ezeket a konkrét feladatokat kell megoldania a fejlesztőcsapatnak.

Az agilis kiáltvány 1. pontja szerint az ügyfél elégedettségét működő szoftverrel kell kivívni, ennek módja a Scrum módszertan szerint az előző fejlesztési sprint eredményeinek bemutatása az ügyfél képviselőjének sprintről-sprintre. Amennyiben az ügyfél nem tud részt venni a demonstráción, a bemutató megtartása akkor is hasznos, mert így a fejlesztőcsapat minden tagja láthatja az előző időszak eredményeit.



2. ábra A Scrum folyamata (saját szerkesztés)

Ez a módszer önmagában nem jobb, mint a vízesésmodell és félreértelmezhető, valamint komoly kérdéseket vet fel, hogy valóban az a szoftver fog-e elkészülni, amelyet a megrendelő szeretett volna, mert a követelmények és a megfogalmazott elvárások folyamat közben változhatnak. Ha a megrendelő nem veszi ki a részét a rá háruló feladatokból, nem bocsájt rendelkezésre egy terméktulajdonost a projekt időtartamára, akkor a Scrum csapat tehetetlenné válik megfelelő támogatás és követelményrendszer hiányában.

Természetesen a megfelelő szabályok betartásával a Scrum egy nagyon hatékony módszer is lehet, mellyel kimagasló eredmények érhetőek el. A módszer alkalmazásának alapfeltétele a korszerű technológiai háttér, valamint a fejlesztőcsapat, a terméktulajdonos és a megrendelő agilis hozzáállása, ami az addig megszokott szervezeti berendezkedést alárendeli a projekt sikerének.

Példának okáért, ha egy katonai bevetéseket szimuláló szoftvert szeretnénk kifejleszteni, akkor szükséges egy olyan katonai szakértő, aki az adott terület fogalomrendszerét, terminológiáját, szabályait átadja a fejlesztők számára és folyamatosan részt vesz a fejlesztésben. Így az adott szakértő a kifejlesztendő szoftver terméktulajdonosává válik, ezt követően már kapcsolattartóként képviselni tudja a projektet a megrendelő felé. Az sem okoz gondot, ha terméktulajdonos a megrendelő oldaláról kerül a projektbe, de nagyon fontos, hogy a fejlesztés időtartamára a fejlesztőcsapattal napi szinten együtt dolgozzon.

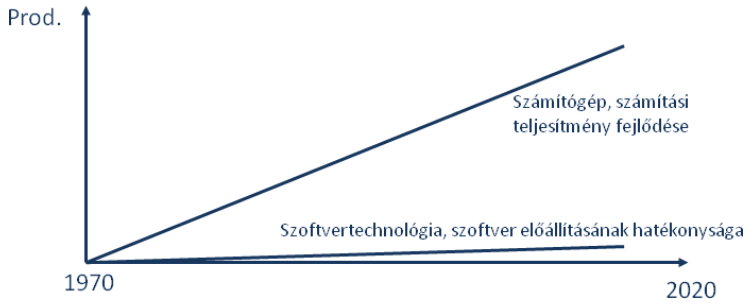
EVOLÚCIÓS SZOFTVERFEJLESZTÉS - A SZOFTVER, MINT ÉLŐ ENTITÁS

Az iteratív szoftverfejlesztési módszertanok lényege a rövid időszakonkénti release (kiadott verzió) előállítása. A helyesen alkalmazott Scrum esetében ez az időtartam néhány egymást követő fejlesztési sprintet jelent. A gyakorlatban egy teljes iteráció, melynek a végeredménye egy kiadható verzió egy néhány hetes, esetleg néhány hónapos időintervallumot ölelhet fel. A ciklikus demók következtében a fejlesztés során is közel stabil állapotú szoftvereket kapunk, melyek lehetőséget biztosítanak a folyamatos újratervezésre, a gyors változtatásra, ami nagyon hasznos lehet minden alkalmazási területen.

Az iteratív szoftverfejlesztés, mint projektmódszertan önmagában kevés, a jobb szoftvertechnológiai teljesítmény elérése érdekében a megfelelő szoftverfejlesztést támogató eszközök szabályozott alkalmazása is szükséges. A követelményeket és a sprint során azonosított fejlesztési feladatokat egységesen kell tudni kezelni, valamint megfelelő számú fejlesztési, tesztelési és fejlesztést támogató környezet szükséges, ahhoz hogy a Scrum a gyakorlatban is sikeresen megvalósítható legyen. A fejlesztést támogató rendszerek felhasználói szintű ismerete a terméktulajdonos, a ScrumMaster és a fejlesztőcsapat számára is kötelező.

A korszerű technológiák alkalmazása a fejlesztőket is új kihívások elé állítja. Ha a megrendelői oldalról plusz erőforrásnak tekinthető a szakértő beépítése a fejlesztő csapatba, akkor a fejlesztők oldaláról is extra energiaráfordítás az azonosított funkciókra, konkrét fejlesztési feladatokra vonatkozó automatizált tesztek elkészítése. Az speciális környezetek közül az egyik legfontosabb a tesztek automatizált futtatását lehetővé tévő tesztfuttató környezet.

A folyamatosan gyorsuló számítógépek, a növekedő számítási kapacitás lehetővé teszi, hogy a kifejlesztett szoftvert tesztesetek tízezreivel, tesztforgatókönyvek százaival fedjük le és folyamatosan teszteljük a magas minőség elérése érdekében. Egy teszt elkészítése ugyan sok időt igényel a fejlesztők részéről, de ezt követően az elkészített programkód szerves részévé válik a szoftver fejlesztői környezetének. A rendszer forráskódjában történő bármely változásról a tesztfuttató-környezetek azonnal visszajeleznek, így a szoftver a virtuális térben egy élő entitássá válik, melynek egyfajta mérhető minősége lesz. Az következő ábra szemléltetve hasonlítja össze az elmúlt évtizedekben végbement számítási teljesítménynövekedést és a szoftvertechnológia fejlődését.



3. ábra Hardverek sebességének fejlődése, szoftvertechnológia hatékonyságának fejlődése (saját szerkesztés)

Amíg a gépekről elfogadja a tudományos világ, hogy a Moore törvény [11] alapján az egységárra jutó számítási teljesítmény egyre gyorsabban növekedik, vagyis az integrált áramkörökben a tranzisztorok száma 18 havonta megduplázódik, addig az emberek, konkrétan az emberi agy ugyanolyan számítási képességekkel rendelkezik, mint 50 évvel ezelőtt.

A szoftvertechnológia hatékonyságán, ezáltal a költségeken, kizárólag az új projektmódszertanok és a fejlesztést támogató eszközök bevonása javíthat. Míg a korszerű számítógépek és a fejlesztést támogató eszközök beszerzése egyszeri költségként jelenik meg egy fejlesztési projektre levetítve, addig a fejlesztési projekt szereplőinek bérköltsége folyamatos kiadás. Ebből a megállapításból következik, hogy hosszú távon luxus a szoftverfejlesztési projektek egy kalap alá vétele az egyéb informatikai projektekhez, mert a leghatékonyabb módszerek alkalmazásához más projektstruktúrára és eszközparkra van szükség.

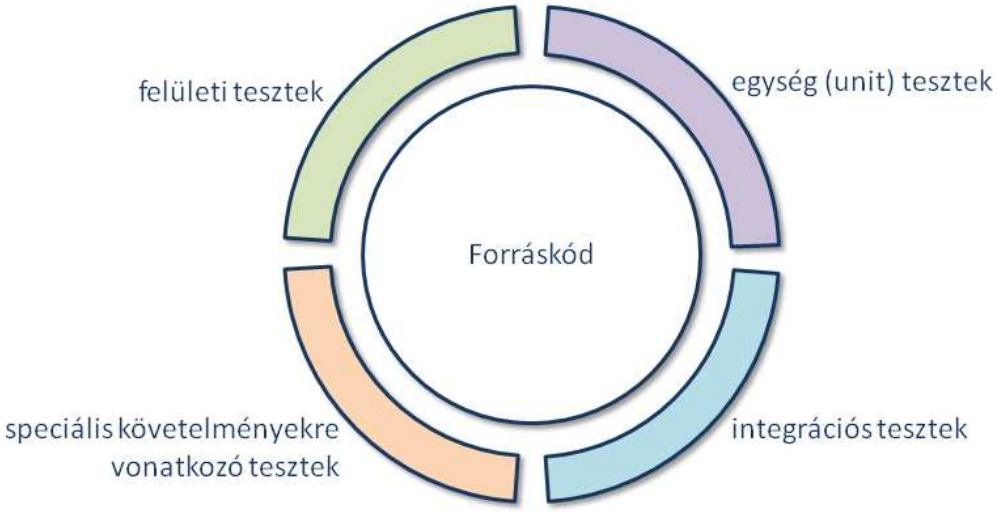
Ahogy a harcászatban újabb és újabb eszközök jelennek meg, úgy a szoftvernek is gyorsan le kell tudnia követni a változásokat. Ha van egy harcszimuláló szoftverünk, melyet hagyományos harcászati eszközökre fejlesztettünk ki a vízesés modellt alkalmazva, akkor komoly fejtörést okozhat a drónok bevezetése a rendszerbe, mert a követelményeket külön kell meghatározni. Célszerű, ha a specifikálást azok végzik, akik az eredeti specifikációt létrehozták, holott lehet, hogy már nem is dolgoznak ott, ahol az eredeti dokumentum elkészült. A fejlesztést követően is problémákba ütközünk, újra kell tesztelni manuálisan az egész rendszert.

Egy agilisan előállított szoftverben ezt a módosítást a terméktulajdonos és a fejlesztők együttesen oldják meg. Az új követelmény elemzését, apró feladatokra lebontását együttesen egyszerűen el tudják végezni, meghatározzák az új és megváltoztatandó használati eseteket, majd ezt követően változtathatnak a rendszer produkciós kódján. Az eddigi működést lefedő automatizált tesztek egyértelmű visszajelzést adnak a lefektetett követelmények és az új rendszer különbségeiről, melyekről már egyszerű eldönteni, hogy elvárt működésről vagy hibáról van szó. A hibák javítását követően a rendszer már képes kezelni akár a drónokat is egy szimulált csatában.

A módszertan tovább csiszolható, oly módon, ha a fejlesztők először a teszteket készítik el és utána futtatják meg a szoftvert. Ebben az esetben a virtuális téren belül a kódnak az a része éli túl a változtatást, mely a drónra is helyesen működött és a „rossz” kód kipusztul a rendszerből. A kipusztulást a fejlesztők „okozzák”, mikor kibővítik a rendszer működését és a drónra helytelenül működő kódot átalakítják. Ez a fejlesztési módszertan egy merőben új, szoftverekre értelmezett evolúciós folyamatot hoz létre.

Ha az automatizált tesztek kialakításakor a harcászati szempontokat is szem előtt tartjuk, akkor ezzel a módszerrel a katonai alkalmazás egy új szintje is elérhető. Kieső számítás kapacitás kezelése, alkalmazott algoritmusok közötti váltás, DoS támadás kiszűrése, stb…

Ellenség által használt támadási technikák beépítése a tesztkörnyezetbe, ezekre válaszoló védelmi funkciók kialakítása.



4. ábra Automatizált tesztekkel lefedett forráskód (saját szerkesztés)

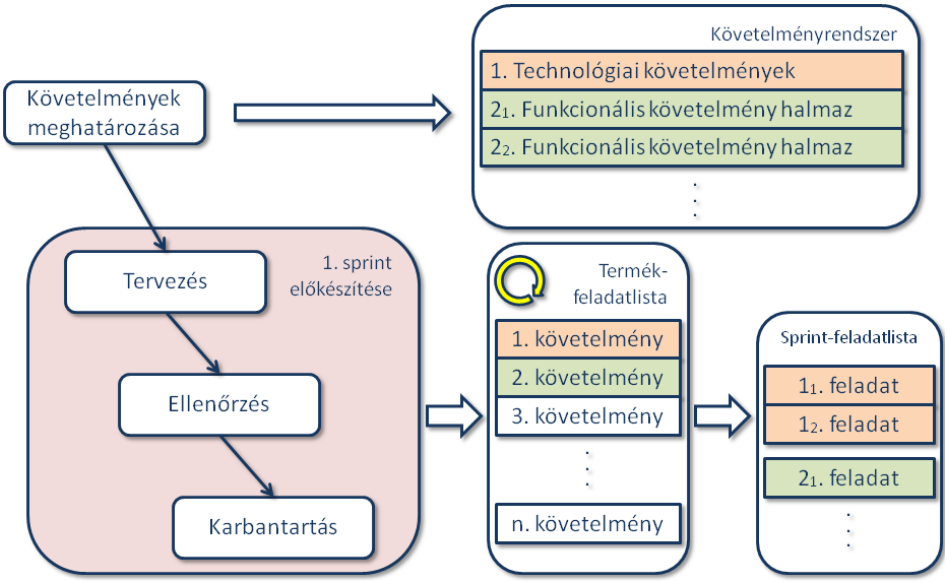
Az automatizált és a manuális tesztelés ugyanolyan fontos a sprint időtartama alatt, mert az egyik a konkrét funkciót fedi le, a másik a funkciót és a rendszer integritását vizsgálja együttesen. Utóbbi különösen akkor igaz, ha szakértő végzi a manuális tesztelést. Ez a fajta megközelítése a szoftverek előállításának aktív részvételt követel meg a megrendelőktől is, a probléma mély megértésének folyamata közös tevékenységgé válik. A módszer legnagyobb előnye az, hogy az elkészült termék a technológiai és az üzleti korlátok között is a lehetséges maximumot fogja produkálni, mert folyamatos tesztelés alatt áll üzleti és technológiai oldalról egyaránt. A módszer lehetőséget biztosít arra, hogy a széleskörű funkcionalitás ötvöződjön a megfelelő technológiai háttérrel.

A VÍZESÉS MODELL ALKALMAZÁSÁNAK LEHETŐSÉGEI A KÖVETELMÉNYEK MEGHATÁROZÁSÁRA

A modern kor szoftvere bonyolult és egyre bonyolultabbá válik, a régi és az újonnan létrejövő rendszereket össze kell kapcsolni, virtuális világ épül a szemünk láttára. Az implementáció során új tervezési módszerekre van szükség, erre lehet válasz az agilis szoftverfejlesztés. Mindezek ellenére, amikor egy újabb területet akarunk leképezni, kell egy kiindulási alap. A scrum szerint ez a product backlog, avagy termék-feladatlista, arról nem szól ez a módszertan, hogyan lehet ezt a feladatlistát elkészíteni.

A vízesés modell egy speciális alkalmazási területe lehet a termékre vonatkozó feladatlista előállítása. Ebben az esetben a cél egy olyan lista elkészítése, amely tartalmazza a leendő szoftver magas szintű áttekintését konkrét feladatokra lebontva. Az elsődleges feladat a teljes probléma feltérképezése, a kapcsolódó szakmai területek azonosítása, majd a probléma feladatcsoportokra és azon belül magas szintű feladatokra bontása. A verifikáció, a tesztelés arról szól, hogy a feladatok szétbontása valóban lefedi-e a teljes problémát. Az esetleges kérdések, problémák a tervezés magas szintjén is dokumentálhatók.

Az alábbi ábrán látható a Vízesés modell alkalmazásának lehetősége az agilis szoftverfejlesztési projektek előkészítéséhez. Ez egy speciális vízesés, mely mellőzi az implementálást, ennek oka, hogy ez a tevékenység teljes mértékben az agilis sprintekre tevődik át.



5. ábra A vízesés modell alkalmazásának lehetősége az agilis szoftverfejlesztési projektek előkészítése során (saját szerkesztés)

Ha egy katonai célú agilis projekt előkészítése zajlik, akkor ennek fényében a megfelelő dokumentációk és magas szintű tervezés megvalósítható a kapcsolódó katonai szakterületek bevonásával, ezt követően a kialakított követelményrendszerrel elindulhat a fejlesztés. Ha a fejlesztés folyamán újabb kérdések merülnek fel, akkor a karbantartás folyamatlépésben a feltárt kérdések tisztázhatóak és beépíthetőek a követelményrendszerbe, azaz a termék-feladatlistába. A megoldás nagy előnye, hogy egy szűkebb projektcsapat dolgozik a sprintek megvalósításán, ugyanakkor a fejlesztés teljes életciklusa alatt minden követelményhez a kapcsolódó szakterület megszólítható, a kérdések tisztázhatóak, így a fejlesztés végére a valódi követelményrendszer áll össze. Ha a dokumentációk karbantartása folyamatos, akkor az implementált szoftver és a hozzá kapcsolódó dokumentumok teljes mértékben lefedik egymást.

KATONAI CÉLÚ AGILIS SZOFTVERFEJLESZTÉS – MILITARY SCRUM

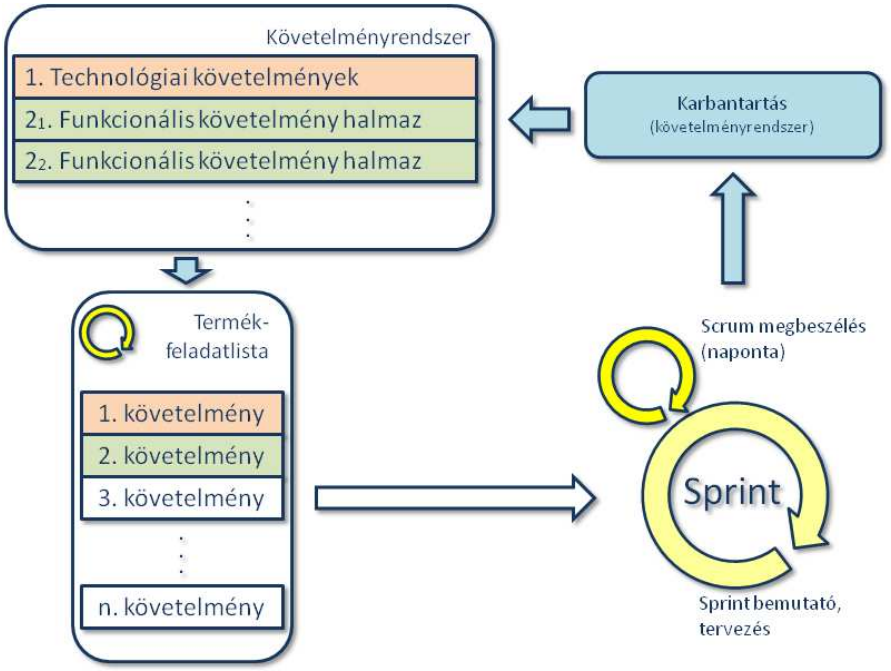
A termékre vonatkozó feladatlista megléte előfeltétele az agilis szoftverfejlesztési projekteknek. A Scrum módszertan összességében annyit mond a tervezésekről, hogy a követelményeket fejlesztési feladatokra kell szétbontani. Itt az a kérdés, hogy egy nagyobb projekt esetében elegendő-e csak a termék feladatlistájának karbantartása és frissítése. Minden alkalmazási területen lényeges minden részlet, ezek megértése, felkutatása már a tervezések előtt is szükséges. A statikus módszertanok válasza erre, hogy a fejlesztés előtt körbe kell járni minden területet. A gyakorlat azt mutatja, hogy az implementáció során is nagyon gyakoriak a rendszer teljes egészére vonatkozó, működést érintő kérdések, melyekre a válasz fogós lehet még a szakértők számára is.

Ha az implementálást agilis eszközökkel végezzük, akkor az evolúciós szoftverfejlesztés alkalmazása lehetővé teszi a gyors visszajelzést a specifikálást végzők számára, és ebből kifolyólag egyfajta kutatási tevékenységgé válik egy adott sprint-re vonatkozó részletes specifikáció előállítása, mert a témával kapcsolatos tárgyi tudás és az automatizált tesztkörnyezetben létező szoftver viselkedése, vizsgálata alapján konkrétan meghatározhatóak a követelmények a következő 1-2 sprintre.

Grafikus felülettel rendelkező szoftverek esetében a képernyőtervek és az azok működését leíró magyarázó szövegek megfelelő kiindulási pontnak tekinthetőek egy tervezéshez.

Felülettel nem rendelkező szoftverek esetében is a keletkező leírások elegendőek az implementálás megkezdéséhez.

A rendszeres sprinttervezések során a fejlesztők részéről nagyon hasznos és lényegi észrevételek hangozhatnak el az implementációval kapcsolatban, melyek a konkrét fejlesztési feladatok meghatározásánál fontosak lehetnek. Ebben a 4 órás tervezésben a cél az, hogy jól átgondolt alacsony szintű követelmények és megvalósítási tervek szülessenek, ám az itt feltárt összefüggések visszahathatnak a teljes követelményrendszerre is. Nem szabad elfelejteni, hogy a tervezést végző csapat része a terméktulajdonos is, aki szakmai szemmel vesz részt ezeken a megbeszéléseken. Az ő elsődleges feladata a feltárt problémák értelmezése, feltárása. A megoldások hatással lehetnek az egyes követelményekre vagy extrém esetben a teljes követelményrendszerre is. Az is elképzelhető, hogy egyéb szakmai területek bevonása szükséges az adott kérdés tisztázásához.



6. ábra Az agilis szoftverfejlesztési sprintek visszahatása az eredeti követelményrendszerre (saját szerkesztés)

A gyakorlatban ez a módszer azt jelenti, hogy a sprint időszaka alatt a következő sprint előkészítő tervezése is megvalósulhat, valamint a termékre vonatkozó feladatlista vezetése, karbantartása is ekkor zajlik. A fejlesztéssel párhuzamosan a felkészülés megvalósítható a soron következő sprintre.

Az előzőekben vázolt projektmódszertanban a fejlesztési feladatok előkészítéséhez 4 szintű tervezési tevékenység szükségeltetik. Példának okáért a megrendelő legyen a Magyar Honvédség. Az alábbi táblázat mutatja a felelősségi körök alakulását a tervezési tevékenységek során.

	Követelményrendszer meghatározása	**Termékre vonatkozó feladatlista kialakítása és karbantartása**	**Sprint-feladatlista meghatározása**	**Tesztforgatókönyvek elkészítése**
MH szakterület	x	x		
Terméktulajdonos	x	x	x	x
Fejlesztőcsapat			x	x

1. táblázat Tervezési szintek és felelősségi körök (saját szerkesztés)

1. *Követelményrendszer meghatározása* – a szoftverfejlesztési projekt első lépése, mely a megrendelő és terméktulajdonos közös feladata. Itt történik a magas szintű követelmények meghatározása, feltárása, strukturálása. Ennek a tervezési szakasznak a feladata a megfelelő dokumentációk előállítása, melyek tartalmazzák a követelmény-halmazokat és az azonosított felelősségi köröket.
2. *Termékre vonatkozó feladatlista kialakítása és karbantartása* – ez a tevékenység két részre bontható szét. Az első lépésben a megrendelő teljes körű részvétele is szükséges, mert ekkor határozzák meg a termék-feladatlista első változatát, ezt követően már a terméktulajdonos a megfelelő kommunikáció mellett egyedül is vezetheti azt. Ebben a dokumentumban jelennek meg a megrendelő által megfogalmazott új követelmények, valamint a sprint tervezések és fejlesztések során azonosított újabb feladatok.
3. *Sprint-feladatlista meghatározása* – ez a lépés a tervezések során azonosított megvalósítási tervek létrejöttét jelenti. A termékre vonatkozó egyes feladatok részfeladatokra történő szétbontása ezen a szinten valósul meg. Itt már nem szükséges a direkt megrendelői jelenlét.
4. *Tesztforgatókönyvek elkészítése* – ebben a lépésben a fejlesztők és a terméktulajdonos közösen teszteseteket dolgoznak ki, ez a legalacsonyabb szintű specifikálása a kifejlesztendő szoftvernek. A tesztesetek dokumentálását és jóváhagyását követően – ami visszavonatkoztatható a sprinttervezési dokumentációra vagy akár a teljes szoftver követelményrendszerére – az automatizált tesztek elkészíthetőek a fejlesztőcsapat által.

Az imént felvázolt módszertan nem a klasszikus Scrum, mert extra dokumentáció készítését írja elő és folytonos visszatekintő ellenőrzést vár el, azonban ezekkel a megkötésekkel egy nagyvállalati vagy államizgatási szerv is alkalmazhatja belső vagy külső fejlesztések során egyaránt.

KÖVETKEZTETÉSEK

A cikkben bemutatott lépcsőzetes tervezési és előkészítési tevékenység az államapparátus működésére jellemző munkamódszer, mely teljes mértékben alkalmazható az agilis szoftverfejlesztési projektek előkészítése során. Ha az állam a megrendelésen túl részesévé válik az agilis sprinteknek, megjelenik a rendszeres bemutatókon, akkor egy átlátható folyamat során kerül kialakításra a megrendelt szoftver, melynek végső formája még a fejlesztés során módosítható, változtatható.

Ha a megfelelő katonai szempontok is szerves részévé válnak a tervezésnek és a folyamatos visszatekintésnek, akkor tetszőleges katonai szakterület által is alkalmazható a Scrum módszertan speciális továbbfejlesztett változata a *Military Scrum*.

A Magyarországon jelenleg hatályos jogszabályokból kifolyólag a Magyar Honvédség kizárólag közbeszerzési eljárás során szerezhet be egyedi szoftvereket. Ez az eljárás a szoftverfejlesztést a műszaki projektekhez sorolja és ugyanabban a mederben kezeli. Ez azt eredményezi, hogy a pályázati kiírások során olyan követelményrendszer jelenik meg, mely nem adaptálható egy agilis szoftverfejlesztési projekt számára. Mégis mi lehet a megoldás arra, hogy az agilis szoftverfejlesztés, mint modern megközelítés meg tudjon jelenni az állami megrendelésekben?

Kézenfekvő válasz lehet a problémára a projektek kiírásának két részre bontása:

1. Prototípus előállítása
2. Teljes rendszer implementálása

A prototípus előállítása többlet ráfordítást igényel a pályázók részéről, azonban ebben az esetben a megrendelő kap egy limitált funkcionalitású működő szoftvert a pályázat első körének végére. A módszer előnye, hogy a terjedelmes sablon dokumentációk helyett a prototípus előállításának menetére vonatkozó dokumentumok és egy működő végtermék áll elő, ezzel valódi döntési alapot biztosítva a megrendelő számára.

A projekt időtartamára és költségvetésére mind megrendelői és pályázói oldalon is megalapozottabb becsléseket készíthetnek az elkészült prototípusok tapasztalatai alapján. Természetesen a győztes kihirdetésénél az ajánlati áron túl szempontnak kell lennie az adott cég addig végrehajtott agilis projektjeinek száma és az agilis projektek során használt dokumentációs, tervezési és fejlesztési módszertanok bemutatása.

A jogalkotók részéről érdemes lenne a szoftverfejlesztési projekteket külön kalap alá venni és egy korszerű szabályozást kidolgozni erre a területre vonatkozóan, mert kevesebb pénzből hatékonyabb és jobb minőségű szoftvereket vásárolhatna az állam a szoftvergyártóktól.

FELHASZNÁLT IRODALOM

[1] Waterfall model, Wikipédia
https://en.wikipedia.org/wiki/Waterfall_model (letöltve: 2016. 12. 20)

[2] ROYCE, W.: Managing the Development of Large Software Systems. In: Proceedings of IEEE WESCON, 26 (1970) p. 329.

[3] .NET Framework
https://www.microsoft.com/net (letöltve: 2016. 12. 20)

[4] Java Enterprise Edition
http://www.oracle.com/technetwork/java/javaee/overview/index.html
(letöltve: 2016. 12. 20)

[5] Enterprise software, Wikipédia
https://en.wikipedia.org/wiki/Enterprise_software (letöltve: 2016. 12. 20)

[6] FÓTHI Á.: Bevezetés a programozáshoz, harmadik, javított kiadás (egyetemi jegyzet), Budapest, ELTE IK, (2012) 30-35. o.
http://people.inf.elte.hu/bzsr/progmod2/konyv.pdf (letöltve: 2016. 12. 20)

[7] Kiáltvány az agilis szoftverfejlesztésért
http://agilemanifesto.org/iso/hu/manifesto.html (letöltve: 2016. 11. 29)

[8] Az Agilis Kiáltványt alkotó elvek
http://agilemanifesto.org/iso/hu/principles.html (letöltve: 2016. 11. 29)

[9] RUBIN K. S.: Essential Scrum. Ann Arbor, Michigan, USA, Pearson Education, Inc., 2013. pp. 15-16.

[10] LARMAN, C., BASILI, V. R.: Iterative and Incremental Development: A Brief History. In: Computer, 36 (2003. 06) pp. 47-56.

[11] MOORE, G. E.: Cramming More Components onto Integrated Circuits. In: Electronics Magazine, 38 (1965. 04. 19) No. 8. pp. 114-117.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

IT BIZTONSÁGI KOCKÁZATOK ÉS KOCKÁZATKEZELÉS

IT SECURITY RISKS AND RISK MANAGEMENT

JAKUS Attila; TICK Andrea

(ORCID ID); (ORCID ID)

attila.jakus.92@gmail.com – Tick.Andrea@uni-bge.hu

Absztrakt

Az IT biztonság területe napjainkban egyre fontosabbá válik a vállalatok és a magánszemélyek életében is. Az informatikai vagyon, kiemelten az adatvagyon, a vállalatok számára meghatározó jelentőségű. Az informatika elválaszthatatlan a vállalati működéstől, a vállalat üzleti folyamataitól. Különösen igaz ez a pénzügyi és biztosítási területre, ahol a visszaélések jelentős károkat tudnak okozni. Az IT biztonsági kockázatok menedzsmentje kulcsszerepet tölt be ezen a területen, hiszen a biztosítókban dolgozó szakemberek, ügyintézők nem informatikusok, mégis sokféle IT biztonsági kockázattal találkozhatnak a munkájuk során. Kezelik az ügyfelek személyes és pénzügyi adatait, mindezt sokszor távoli eléréssel, mobiltelefon vagy saját notebook használatával. Ezért is kulcskérdés az informatikai vagyon védelmében az alkalmazottak biztonságtudatossága. A cikk megvizsgálja és elemzi, hogy milyen IT biztonsági kockázatok azonosíthatók a biztosítási területen, milyen eljárással lehet és érdemes értékelni ezeket a kockázatokat, milyen tipikus kockázatkezelési módszerek állnak rendelkezésre és adódik-e lehetőség a social engineering előfordulására, illetve csökkentésére.

Kulcsszavak: *IT biztonság, IT kockázat, adatvagyon, biztosítási piac*

Abstract

Nowadays for enterprises as well as for individuals IT security is concerned to be a more and more important field in the IT profession. The IT asset, especially the data asset is of dominant importance for the enterprises. Information Technology is inseparable from corporate operation, from the business processes of an enterprise. It is particularly true in the finance and insurance sectors, where IT abuses can cause serious damage to the IT asset even to the business. IT risk management has a key role in this field, since employees, assistants working for these enterprises are not IT experts, even so they might face several types IT security risks during their everyday work. They handle the clientele, their private and financial data, often in remote access using cellular phones or own notebooks. Therefore, it is cruial to increase employees' IT consciousness and awareness in favor of protecting the corporate IT asset. This paper examines and analyses what types of IT security risks can be identified in the field of insurance, how these risks can be evaluated and are worth of evaluating, what typical risk management methods are available and whether there is a chance of the emergence or rolling back of social engineering.

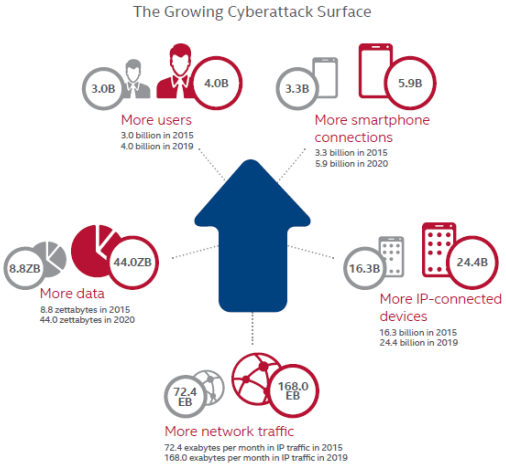
Keywords: *big data, social engineering, IT security, IT risks, IT asset, data asset, insurance market*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.11.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.20.

BEVEZETÉS

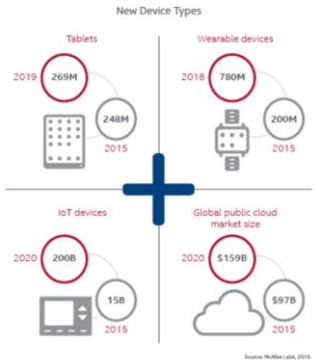
Az IT területén még az egyre nagyobb hangsúlyt élvező biztonságtudatosság fényében is, időről-időre történnek visszaélések. Az elektronikus támadási felület napról napra bővül (1. ábra), egyre több a felhasználó, és a felhasználók egyre többször és többféle módon veszik használatba az internet adta lehetőségeket. A több felhasználó, nagyobb mennyiségű adatot is jelent, növelve így a lehetséges visszaélések számát. A McAfee becslései szerint az adatmennyiség 2020-ra eléri a 44 zettabyte-ot (1. ábra), ami a jelenlegi elérhető adatmennyiségnek közel ötszöröse [1].

A McAfee felmérései alapján a felhasználók száma 2019-re eléri a négy milliárd főt, ami egy milliárdos növekedést jelent 2015-höz képest. Az előrejelzés szerint az IP alapú eszközök száma 2019-re 24,4 milliárd (a 2015-ös érték másfélszerese), míg a mobiltelefonok száma 2020-ra 5,9 milliárd (a 2015-ös értéknek majdnem kétszerese). A hálózati forgalom is jelentősen, több mint kétszeresére nő, 168 exabyte lesz 2019-ben [1].



1. ábra Növekvő kibertámadási lehetőségek [1]

A becslésben nem szabad azt a tényt figyelmen kívül hagyni, hogy egyre több embernek nem csak egy eszköze csatlakozik a hálózathoz, hanem általában legalább kettő, de előfordul három, négy esetleg még több is (2. ábra).



2. ábra A felhasználók és „okos” eszközeik [1]

A mai mobiltelefonok mindegyikéről elmondható, hogy „okosak” tehát támadási oldalról van, illetve lehet rajtuk értékes információ. Az otthoni számítógép, laptop mellett a tabletek is megjelennek ebben a felsorolásban. Ezen kívül használunk okosórákat, okos televíziókat, okos gépjárműveket, vagy például olyan okos segédeszközöket, mint a google szemüveg. Ezek az eszközök gyakran lehetőséget nyújtanak arra, hogy hálózaton keresztül

összehangoljuk őket, egyikről lássuk a másikat és fordítva. Ez a lehetőség, viszont nem csak nekünk jelenthet könnyebbséget, hanem azoknak is, akik valamilyen visszaélést szeretnének végrehajtani. Mivel minden eszköz másfajta védelemmel van felszerelve, és nincs két egyforma felhasználó, aki ugyanazokat az eszközöket ugyanolyan módon használja, rendkívül nagy kihívást jelent naprakésznek maradni az elkövetkező időszakban az IT biztonság területén. Az elektronikus világban, bármit teszünk, annak nyoma marad, a digitális lábnyomunkat otthagyjuk magunk után.

TÁMADÁSOK, FENYEGETETTSÉGEK

Az IT területén még az egyre nagyobb hangsúlyt élvező biztonságtudatosság fényében is, időről-időre történnek visszaélések. 2015 decemberében a MacKeeper (egy segédprogramokat öszegyűjtő program) belső szerveréről 13 millió felhasználói adatot töltöttek le, köztük e-maileket, jelszavakat, telefonszámokat, személyes adatokat. A Facebook (Központ, Kormányzati Eseménykezelő, 2013) hasonló hibát jelentett be, ők az információszivárgást a Facebook Download Your Information Tool-t használó felhasználók között észlelték. Ezzel az eszközzel a felhasználói fiók teljes tartalmát lehet letölteni. A hiba kijavításáig körülbelül hatmillió regisztrációhoz tartozó e-mail címet és telefonszámot lehetett megszerezni.

Az autókban megjelenő új fejlesztések a hozzáférés fenyegetettségének külön csoportját jelentik, amelyre érdemes nagy hangsúlyt fektetni a jövőben. Az elmúlt évben a Chrysler, General Motors, Toyota és a Ford is jelentett különböző mértékű sérülékenységeket. A Nissan elektromos autók feltörését egy mobilalkalmazáson keresztül tudták véghezvinni, tehát a biztonsággal kapcsolatos visszaélések kérdése nem kizárólag az online szolgáltatások terén fontos, hanem hétköznapjaink kulcseleme [1]. Az applikációban lévő rést megtalálva lehetőség nyílt arra, hogy az illetéktelenek különböző adatokat tulajdonítsanak el, például alvázszám, töltöttségi állapot, gps naplók; vagy éppen hozzáférjenek a gépjármű belső rendszeréhez, irányítva a klímaberendezést, elérhetetlenné téve különböző létfontosságú rendszereket. A probléma a Nissan Leaf és eNV200 típusú elektromos autó tulajdonosait érintette, közel kétszázezer embert.

A biztonsági visszaélésekkel kapcsolatos kockázatok felmérésére és ésszerű kezelésére érdemes időt fordítani, hiszen a károk mértékét néhány esetben még felbecsülni is nehéz lenne. Ezt végig gondolva jutott arra a döntésre a svéd adatvédelmi hatóság, hogy az ottani közszférából kitiltja a Google felhő alapú szolgáltatásait [2]. Szerintük a szolgáltatás túl sok lehetőséget ad a Google kezébe az adatok kezelésének kérdésében, ami aggályokat vetett fel több szempontból is, a vállalati adatok kezelésének területén. Ameddig a felhasználói szerződések ilyen szempontból hiányosak, addig a svéd állami szervek a Google naptár, e-mail és adatfeldolgozási funkciók nélkül dolgoznak.

A biztonságtudatosság növelése érdekében Berlinben a közelmúltban tesztelték a köztisztségviselőket. A berlini rendőrség dolgozói kaptak egy próba adathalász linket, amelyet a 466 alany közül 252, azaz az alkalmazottak több mint fele meg is nyitott. A teszt 35 résztvevője még az utasításokat is követte, megadva saját használatú jelszavukat, s így megnyílt az adathalász link [3].

A támadások, fenyegetettségek típusai

Az IT területén végrehajtható támadásoknak rengeteg típusa van, a határ kizárólag a csalók kreativitásán múlik. A számítógépes bűnözésben a támadás forrása és célpontja szerint négy típust különböztethetünk meg (1. táblázat) [4].

Számítógépes bűnözés		
Támadás forrása	**Támadás célpontja**	**Példa**
A bűncselekmény célja a számítógép támadása. Az elkövető egy másik gépet használ a támadás indítására.	Egy konkrét beazonosított számítógép.	DoS támadás (Denial of service) Hacker tevékenység
Az elkövető egy számítógépet használ arra, hogy visszaélést kövessen el egy másik számítógép ellen.	A célpont nem feltétlenül definiált. A támadás pontos cél nélküli.	Kiterjesztett DoS támadás Vírus
A visszaélés eszköze a számítógép. A gép a bűncselekmény végrehajtására használt, de a cél nem egy másik számítógép.	A főbb célpontok az adatok, vagy a számítógépen tárolt információk.	Csalás Jogtalan hozzáférés Phishing Keylogger telepítése
A számítógép a visszaélés szimbóluma. Az elkövető a gép használóját csapja be és használja bizalmas információk megszerzésére.	A célpont a számítógép használója.	Social engineering különböző típusai (Phishing, hamis weboldalak, csaló emailek, spam mailek, hamis önéletrajzok)

1. táblázat A számítógépes bűnözés kategóriái

A biztonsági megoldások leggyengébb láncszeme az ember, sok visszaélés épít erre. A személyes ráhatás (*social engineering*) olyan gépfüggetlen eljárás, melynek lényege, hogy a támadó a rendszerrel dolgozó emberektől megszerzett adatok segítségével tör be a rendszerbe. Részben ilyen jellegű visszaélés a személyazonosság lopás (*identity theft*), ami akkor következik be, amikor az eltulajdonított személyes adatokkal a csaló visszaél. Az ilyen jellegű visszaélések esetében kiemelt szerepe van a biztonságtudatosság erősítésének.

A támadások többféleképpen csoportosíthatók, megkülönböztetnek *aktív* és *passzív* támadásokat [5]. A passzív támadás azt jelenti, hogy a támadó hozzáfér különböző bizalmas információkhoz, de a kommunikációt megváltoztatni nem tudja, tehát hamis információk küldésére nincs lehetősége. Célja az észrevétlen információszerzés. Ezzel szemben egy aktív támadás esetében a támadó behatol a rendszerbe, képes adatokat megváltoztatni, és az információcserét befolyásolni, ki tudja adni magát a küldőnek vagy a címzettnek.

Az előzőekben felsorolt tipikus visszaélések aktív, illetve passzív kategóriáit mutatja a 2. táblázat.

Passzív támadások	**Aktív támadások**
adat remanencia	átejtés
célzott adatbányászat	DoS támadás
kémkedés	hátsókapu
kisugárzás	HTTP beágyazás (HTTP tunneling)
kukabúvárkodás	jelszótörés
lehallgatás	kártékony kód
shoulder surfing	közbeékelődéses támadás (man-in-the-middle attack)
sniffing	social engineering
	személyazonosság lopás
	vírus
	féreg

2. táblázat Aktív és passzív támadások

IT KOCKÁZAT, KOCKÁZATMENEDZSMENT

A vállalatok működésében a kockázatnak kritikus szerepe van. Az üzleti döntések során figyelembe kell venni a döntéssel együtt járó kockázatokat és a lehetséges hasznokat is. Az informatikai kockázatokat gyakran hagyják figyelmen kívül, ami a későbbiekben számos esetben okoz problémákat. Az informatikai kockázatnak több meghatározása ismert.

A RiskIT megközelítése szerint informatikai kockázat alatt az IT használatával kapcsolatos üzleti kockázatot értjük [6]. A Computer and Information Security Handbook meghatározása szerint a kockázat = fenyegetettség x sebezhetőség x az informatikai vagyon értéke (Risk = Threat × Vulnerability × Asset Value) [7]. A COBIT 4.1 magyar változata szerint a kockázat az üzleti életben annak a lehetősége, hogy egy adott fenyegetés ki fogja aknázni egy eszköz, illetve eszközcsoport sebezhetőségeit annak érdekében, hogy az eszközökben veszteséget

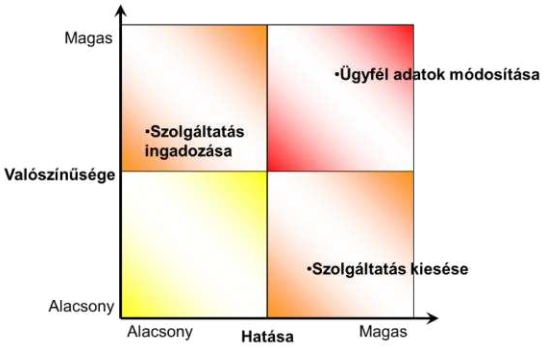
és/vagy kárt okozzon. Mérése általában a bekövetkezés hatásának és valószínűségének kombinációjával történik [8]. Az ISO/IEC 27005:2011 szerinti definícióban IT kockázat alatt értik annak a lehetőségét, hogy egy fenyegetettség kihasználja az informatikai vagyon sebezhetőségét és így kárt okoz a szervezetnek.

Az IT kockázatok sokfélesége a mindennapi működésbeli hibáktól a ritkábban előforduló nagyobb horderejű támadásokig is előfordulhatnak. Az elmúlt időszakban az üzleti rendszerek kritikus fontosságúvá váltak, a tőlük való nagymértékű függőség eredménye, hogy a kockázatokat kötelező felmérni és kezelni. Az informatikai veszélyek egyre nagyobb hányadát teszik ki a vállalatra vonatkozó teljes kockázati halmaznak. Az IT rendszereket veszélyeztető tényezők a szervezetre gyakorolt hatás szerint négy alapvető csoportra oszthatók, ezek a *biztonság*, *rendelkezésre állás*, *teljesítmény*, *megfelelőség* (3. ábra).

3. ábra Az IT rendszereket veszélyeztető tényezők [9]

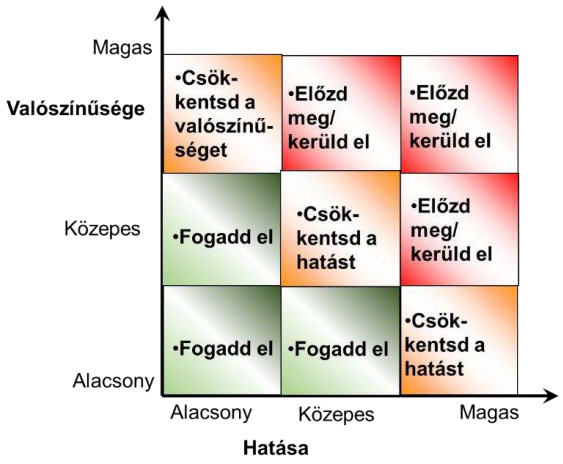
A kockázatmenedzsment két nagyobb területe a kockázatok értékelése és kezelése. A kockázatmenedzsment során az első lépést a lehetséges veszélyek feltárása, a kockázatok azonosítása jelenti. Egy kockázatot célszerű pontos leírással, lehetséges hatásaival, előfordulásának gyakoriságával, kiváltó okaival együtt feljegyezni, hiszen egy összetett vizsgálat, összehasonlítás sokkal pontosabb képet ad majd róla és használható a kockázatok elemzésére és értékelésére. Mivel az előzetesen becsült kockázatok 20%-a okozza a bekövetkezett teljes kockázati hatás 80%-át a kockázatmenedzsmentben is használt Pareto-elv alapján, ezért a kritikus kockázatokra való odafigyelés meghatározó a fenyegetettségek kezelése során.

A kockázatok elemzése és értékelése történhet kvalitatív és kvantitatív módon is, lényege egy rangsor felállítása, amely a lehetséges veszély nagysága alapján állít fel egy sorrendet a kockázatokra vonatkozóan. Kvantitatív értékelés esetén pontosan meg tudjuk mondani, hogy egy adott kockázat bekövetkezése milyen hatást eredményez (kihatás mértéke), pl. 1 napos szolgáltatásleállás forintban kifejezve mekkora kárt okoz a vállalatnak. Kvalitatív módszer esetében gyakran alkalmazott eszköz a szakértői becslés vagy kategóriák definiálása. Ilyen az értékelésben gyakran alkalmazott módszer a kockázati mátrix, amely a kockázatokat az előfordulásuk valószínűsége és a kockázati hatás nagysága alapján osztja be (4. ábra).



4. ábra Lehetséges IT kockázati mátrix

A kockázatok értékeléséhez úgy járul hozzá, hogy a jobb felső részben levő kockázatok a kritikus fontosságúak, a középső területen levők fontosak, míg a bal alsó területen elhelyezkedők kevésbé fontosak. Ennek alapján már kialakíthatók a kockázatkezelési alternatívák (5. ábra).

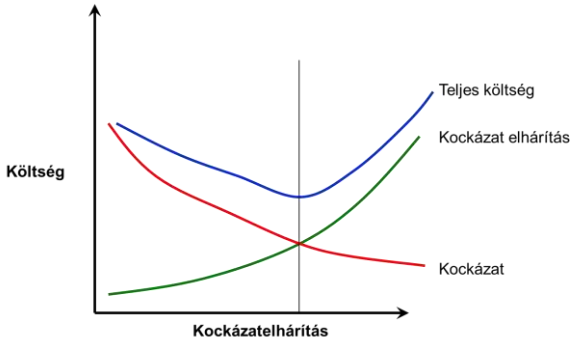


5. ábra Kockázatkezelési alternatívák

A kockázatkezelés gyakran alkalmazott alternatívái, a kockázat megelőzése, elkerülése, a kockázat előfordulási valószínűségének és/vagy hatásának csökkentése, a kockázat áthárítása illetve a kockázat elfogadása, amikor nem teszünk semmit.

Amennyiben a választ megadtuk, a vizsgálat nem érhet véget, hiszen újból ellenőrizni kell, hogy megéri-e, nem hoz-e magával új kockázatokat a változtatás, vagy éppen lehetséges-e meglépni. A megelőzés mellett a hatás csökkentése is opció, ilyenkor elfogadjuk a tényt, hogy előfordulhat a baj, de legjobb tudásunk szerint felkészülünk rá, pl. biztosítást kötünk. A kockázat áthárítása szintén egy lehetséges megoldás, például egy külső szállítót bízhatunk meg a feladattal.

A kockázatkezelési alternatíváknak költsége és erőforrásigénye van, figyelni kell arra, hogy ne legyen drágább a kockázat kezelés, mint az esetlegesen bekövetkező károkozás során fellépő költség (6. ábra).



6. ábra Kockázatelhárítás és költsége [10]

A kockázatmenedzsment ciklikus tevékenység, mivel a kockázatkezelési eljárások végrehajtása után időről időre felül kell vizsgálni a kockázatokat (mivel újabbak jelenhetnek meg) és ennek megfelelően változik a kiértékelés is.

Az informatikai irányítás és a kockázatok kezelése

Az informatikai irányítás (IT Governance) ma már önálló tudományterület a vezetés és szervezés tudományon belül, és a vállalkozás irányításának kihagyhatatlan részét alkotja. Noha az informatikai feladatok ellátásáért az informatikai részleg vezetője a felelős, azonban

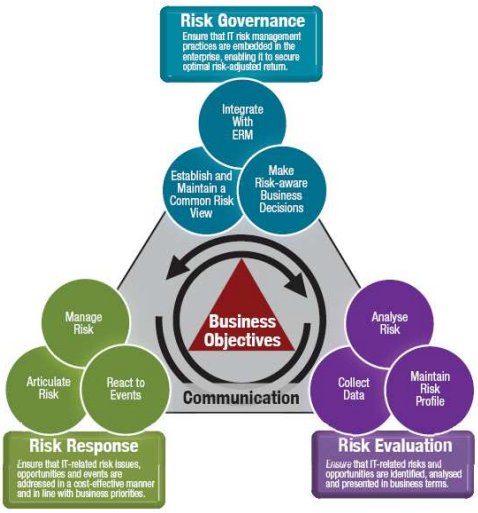
az informatika fejlesztési és stratégiai irányvonalának meghatározásáért a felelősséget az igazgatótanácsnak és az ügyvezető igazgatóknak kell viselniük. Az informatikai irányítás elemei, a vezetői képességek, szervezeti felépítés, a folyamatok együttesen biztosítják azt, hogy a szervezet stratégiájának és célkitűzéseinek megvalósítását a szervezet informatikája folyamatosan tudja segíteni és ki tudja teljesíttetni.

Az informatikai irányítás a vállalatirányítási és ellenőrzési kapcsolatok és eljárások olyan struktúrája, amely új érték hozzáadásával, ugyanakkor a kockázatok és az informatika által kínált előnyök együttes mérlegelésével kívánja megvalósítani a vállalkozás célkitűzéseit.

Az informatikai irányítás fókuszterületei [4] az üzleti és informatikai stratégiai illesztése, az értékelőállítás, az erőforrás gazdálkodás, a kockázatkezelés, és a teljesítménymérés.

A RiskIT keretrendszer

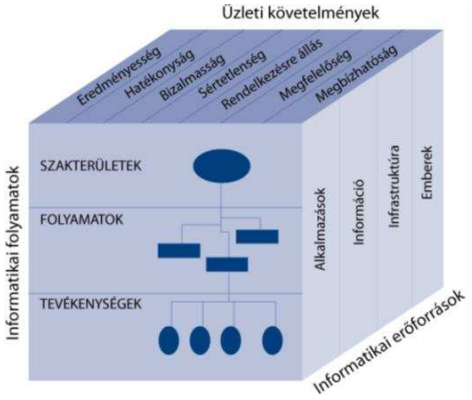
Az ISACA (Information Systems Audit and Control Association - Informatikai Auditorok Nemzetközi Egyesülete) megközelítésében az informatikai irányítás kockázatkezelési területe a RiskIT keretrendszerre épül, amely end-to-end, átfogó megközelítésben tárgyalja az IT használatával kapcsolatos kockázatokat, a kockázatmenedzsment kérdéseit, valamennyi szervezeti szint igényeit és a vállalati kultúra szempontjait is figyelembe véve. Három fő területe a kockázatmenedzsmenttel kapcsolatos irányítási feladatok (risk governance), a kockázatok értékelése (risk evaluation) és a kockázatok kezelése (risk response) (7. ábra). A RiskIT keretrendszer folyamatmodellje bemutatja az egyes területekhez kapcsolódó részfolyamatokat, a folyamatok input és output folyamatait (kapcsolatait), a menedzsment eljárásokat; szerepköröket, felelősségi köröket [RACI – Responsible, Accountable, Consulted, Informed mátrix)], a folyamat célokat és metrikákat és a terület érettségi modelljét.



7. ábra A RiskIT keretrendszer elemei [6]

A COBIT 4.1 keretrendszer

Az ISACA által kidolgozott COBIT (Contol Objectives for IT and Related Technology) olyan keretrendszer, amely általánosan alkalmazható és elfogadott az informatikai biztonsági ellenőrzés és szabályozás területén. Célja „egy irányadó, naprakész, nemzetközileg elfogadott informatikai irányítási kontroll keretrendszer kutatása, kidolgozása, közzététele és népszerűsítése” [8]. A COBIT kocka (8. ábra) bemutatja a COBIT főbb összetevőit és alapelvét, vagyis, hogy az üzleti követelményeknek megfelelő informatikai célok elérése érdekében az informatikai folyamatok menedzselik az informatikai erőforrásokat.



8. ábra A COBIT kocka [8]

A COBIT kocka egyik dimenziója az informatika területét négy szakterületre osztja. Ezek a szakterületek a 4.1 verzióban a „Tervezés és Szervezés" (Plan and Organise), a „Beszerzés és Megvalósítás" (Acquire and Implement), a „Szolgáltatás és Támogatás" (Deliver and Support), valamint a „Figyelemmel kísérés és Értékelés" (Monitor and Evaluate). A szakterületek megfeleltethetők az informatika főbb felelősségi területeinek, a tervezés, fejlesztés, kivitelezés, működtetés és figyelemmel kísérés területeinek. A területeket folyamatokra, azokat pedig tevékenységekre bontja a COBIT. Valamennyi folyamathoz kontroll célkitűzések tartoznak. A COBIT jelenleg használt változata a COBIT 5. Kialakításának egyik legfontosabb célja volt, hogy az üzleti és az informatikai oldalt közelebb hozzák egymáshoz, annak érdekében, hogy az együttműködés hatékonyabbá válhasson. A COBIT 5 támogatja a vállalatokat az IT optimális értékének előállításában a hasznok realizálásán, a kockázatok kézbentartásán és az erőforrások megfelelő használatán keresztül. A COBIT 5 integrált keretrendszert ad, épít a legújabb szabványokra, keretrendszerekre és legjobb gyakorlatokra a vállalati és az informatikai területekről mint például a COS ERM válllati keretrendszerre vagy az ISO/IEC 27000 IT szabványcsaládjára.

Az ISO/IEC 27000-szabványcsalád

Az ISO/IEC 27000-es szabványcsalád az információbiztonsági irányítási rendszerekkel kapcsolatos szabványokat tartalmazza. Az információbiztonsági irányítási rendszerek célja, hogy kockázatkezelési folyamat alkalmazásával és a kockázatok megfelelő kezelésével megfelelően támogassák az információk biztonságát.

A szabványcsalád legfontosabb ajánlása az ISO/IEC 27001 szabvány, amelyben az információbiztonság irányítási rendszer követelményeit tartalmazza. A szabvány legújabb változatában 35 információbiztonsági szabályozási célt határoz meg és 114 kontrollt azonosít az információbiztonsági politika, az informatikai biztonsági irányítási rendszer szervezése, a humán erőforrások biztonsága, eszközkezelés, hozzáférések ellenőrzése, titkosítás, fizikai biztonság és a környezet biztonsága, működésbiztonság, kommunikáció biztonsága, rendszerek beszerzése, fejlesztése és fenntartása, beszállítói kapcsolatok, információbiztonsági incidensek kezelése, üzletmenet-folytonosság valamint a megfelelőség ellenőrzési területeken [11].

A szabvány lehetőséget teremt a szervezetek számára, hogy saját információbiztonságukra vonatkozóan kockázatelemzést végezzenek, majd a kockázatelemzést követően képesek lesznek meghatározni az alkalmazandó kontrollokat. Speciális esetben ez jelentheti az eredeti listában szereplő 114 kontroll kiegészítését is. A kockázatértékelés is nagyobb hangsúlyt kapott, bár annak módszertana nem került meghatározásra.

Az ISO/IEC 27002-es szabvány - az információbiztonság menedzsmentjének gyakorlati kódexe - segítséget nyújt az ISO/IEC 27001 szabványban definiált szabályozási célok és intézkedések értelmezéséhez. Gyakorlati útmutatást ad a szervezet információbiztonságának felmérésére, illetve az alkalmazott kontrollok hatékonyságának meghatározására.

IT BIZTONSÁGI KOCKÁZATOK ÉS KEZELÉSÜK BIZTOSÍTÁSI TERÜLETEN

Az elmúlt időszakban lezajlott botrányok, csődök a biztosítási területen rávilágítottak az informatika kulcsszerepére, az IT biztonsági kockázatok menedzsmentjének fontosságára. A biztosítókban dolgozó szakemberek nem informatikusok, de nagyon sokféle IT biztonsági kockázattal találkoznak rendszeresen. Ügyfelek személyes és pénzügyi adatait kezelik, sokszor a saját notebookon, mobiltelefon segítségével, miközben az ügyfelek és a vállalat sem tudja, milyen IT biztonsági ismeretekkel rendelkeznek, tisztában vannak-e a tipikus IT biztonsági kockázatokkal és a lehetséges védekezési módokkal. Az adatok megfelelő védelme nélkül nem lehet ellenőrizni az adatok kiszivárgását. Az átgondolatlan, ellenőrizetlen módosítások adatvesztést okozhatnak és a nyomnélküli adatvesztés esetén kicsi a helyreállíthatóság esélye. Ennek egy következménye lehet, hogy az adatok nem érhetőek el, amikor szükség van rájuk. Egy vállalat nem tud biztonságosan működni, ha azok az emberek, akik az IT rendszereket használják és működtetik, nem ismerik szerepüket és felelősségüket a rendszerben, nem értik meg a szervezet IT biztonsági szabályzatát, gyakorlatát és eljárásait, nincs legalább alapvető képük a különböző menedzsment, üzemeltetési és technikai eljárásokról.

Biztonsági kockázatok értékelése egy vizsgált biztosítási cégnél

A vizsgált biztosítónál nincs külön IT biztonsági főosztály, szervezeti egység (bár egy hazai vezető biztosítási területen működő cégről van szó), de van 3-4 olyan szakértő, akik munkaidejük egy jelentős részében IT biztonsági feladatokkal foglalkoznak. A vállalat legfontosabb informatikai vagyona az ügyféladatbázis és az alapszolgáltatást nyújtó alkalmazások, pl. partnerkiszolgáló rendszerek. A kérdés, hogy milyen kockázatok merülnek fel és arra milyen védekezési lehetőségekkel tud válaszolni a cég.

IT biztonsági elemek a vizsgált cégnél

A vizsgált cég esetén az IT biztonság kérdése egyre fontosabb, egyre több biztonsági terméket használnak, legfőképpen Symantec-es termékeket. Végpont védelemmel kezdték a védelem kialakítását, majd a standard biztonsági elemek következtek, mint a proxy és a tűzfal, a határvédelem kiépítése. Jelenleg több mint tíz terméket használnak.

Napjaink egyik kihívása a nulla napos sérülékenység és a malware. A nulla napos sérülékenységek ellen még nem adtak ki védelmi eljárást a cégnél, így a védekezés is nehezebb, mint egyéb esetekben. Azonban malware fertőzés, vagy zombi gép gyanúja esetén a kifelé irányuló kommunikációt blokkolják, de a leggyakrabban követett eljárás a kliens gép újratelepítése, amennyiben egy ilyen eset előfordul (zombi számítógép lesz valakinek a gépe, vagy botnetet telepítenek rá). Az ilyen helyzeteknek a kezelésére is vannak kidolgozott eljárások.

A vállalat esetében három főbb terület emelhető ki a tipikus visszaélések közül, a belső támadások közül az adatszivárgás és a személyes ráhatás (social engineering), a külső támadások közül példaként a locky-t, a ransomware (olyan malware, amely valamilyen fenyegetéssel, pl. makro vírus egy ártalmatlannak tűnő emailben, próbál pénzt kicsikarni a felhasználóból) vírusok. Különösen nagy problémát jelenthet, ha egy kulcsfontosságú alkalmazott anyagaival történik mindez.

A locky vírus továbbra is terjed, a biztonsági szakértők szerint a jelenlegi legfontosabb vírusnak számít [12]. A locky vírussal kapcsolatos kockázat csökkentését támogató intézkedés lehet a backup megoldás és a mentés.

Egy másik visszaélés típus elsődlegesen a belső alkalmazottakhoz kapcsolódik, az adatszivárgás. Mivel a cég legfontosabb vagyona az adat, az ügyféladatbázis, kiemelt szerepe van az adatszivárgás megelőzésének, ami ellen használnak adatszivárgást megelőző szoftvert a védelemben. Fokozott figyelmet kell fordítani adatszivárgási szempontból az

adminisztrátori jogkörrel rendelkezőkre, hiszen nekik van joguk ügyféladatok lekérdezéséhez, exportálásához, amivel akár vissza is lehet élni. Ezen a területen is előfordultak incidensek, amelyek elsősorban biztonságtudatosságbeli problémákhoz voltak köthetők. Ilyen eset amikor a felhasználó más cégnek küld ügyféladatot, pl. ha valaki az ügyfélrekord három attribútumára lekérdezést végez (pl. vezéknév, keresztnév, szerződésszám) az ügyféladatbázisból és azt tovább küldi, vagy titkosítás nélkül küld olyan excel táblát, amiben van ügyféladat, akkor az egy biztonsági incidens lesz, amit kezelni kell. Ebben az esetben értesíteni kell az IT biztonsági felelőst (security officer) aki dönt a helyzet kezeléséről. A cégnél végeznek előszűrést, és a gyanús eseteket továbbítják IT biztonsági felelősnek. Ebben a helyzetben az a legfontosabb, hogy az ügyfél ne lehessen beazonosítható, ne lehessen az adataival visszaélni. A cég az adatszivárgások ellen viszonylag jó hatásfokkal tud védekezni.

A harmadik visszaélés fajta a személyes ráhatás (social engineering), ami gépfüggetlen eljárás, így ez ellen a visszaélés ellen talán a legnehezebb a védekezés. Lehet előzetesen megvizsgálni a jelentkező hátterét (pl. pszichológiai tesztekkel), titoktartási nyilatkozatot aláíratni, de ettől függetlenül is elfordulhatnak ilyen esetek, pl. a jelszóelkérés, az ember marad a leggyengébb láncszem a védelemben.

A vizsgált cégnél 2009-ben volt egy conficker virusos eset. A vírus folyamatosan kizárta (kilockolta) az összes felhasználót a rendszerből, és nem csak a felhasználókat hanem az adminisztrátorokat is. A conficker, egy a Microsoft Windows operációs rendszert támadó féreg (worm), 2008 novemberében észlelték először. Kihasználta a Microsoft patch sérülékenységét így hozzáfért fájl megosztásokhoz, felhasználó azonosítókhoz.

A lehetséges védelmi intézkedések közé tartozik a vírusirtó naprakész adatbázissal, valamint az új felhasználóra vonatkozó megfelelő beléptetési feltételek. Ez utóbbinak része az új alkalmazott számítógépének előkészítése, többek között a tűrt, támogatott, tiltott programok meghatározása.

A cég meghatározó informatikai vagyona az ügyféladatbázis és az alapszolgáltatást nyújtó alkalmazások, pl. partnerkiszolgáló rendszerek. A kapcsolódó kockázatok lehetnek az adatvesztés, adatmódosítás, jogosulatlan szolgáltatás igénybevétel, vírusok. Ezekre a vizsgált cégnél is a hálózattal, architektúrával kapcsolatos szokásos védelmi eljárásokat alkalmazzák, mint tűzfal, DMZ, a felhasználók megfelelő autentikációja, vírusirtó szoftver.

A felhasználók általában webes szolgáltatásként veszik igénybe a cég szolgáltatásait (biztosítások kötése, követése), ahol kiemelt figyelmet kap az ügyfél autentikáció és a tranzakció védelme.

Nem csak végponti védelmet alkalmaznak (pl., tűzfal, proxy szerverek, vírusirtók), hanem hardeningelési technikákat is. A hardeningelésre alkalmas szoftverekkel vizsgálják a kiszolgáló szerverek sérülékenységét. A legfontosabb vizsgálandó vagyonelemek az ügyfél adatokat tartalmazó, vagy éles rendszerek (production server). Ezeknek az alkalmazásoknak gyakran vannak publikus IP címeik, ezért ezeket évente legalább kétszer egy blackbox vagy penetration teszttel elemzik sebezhetőségi szempontból. A „blackbox” teszt a funkcionalitás tesztje, amit a specifikációval való összehasonlítással lehet ellenőrizni. A „penetration” teszt során kifejezetten a sebezhetőségeket térképezik fel. A tesztek, elemzések eredményeinek alapján a rendszerfejlesztésnek vagy üzemeltetésnek kötelessége a javításokat elvégezni.

A vállalatnál van formális kockázatértékelés, van kockázatkezelési osztály is. Ha új partner kiszolgáló rendszert fejlesztettek, ami nagy mennyiségű adatot kezel, vagy nagyszámú felhasználó tartozik hozzá, akkor a kockázata is nagy. Kockázatot jelenthet, ha a rendszer nincs megfelelően dokumentálva, implementálva, patchelve, karbantartva, nincs BCP (üzletmenet folytonossági terv), vagy nincs DRP (katasztrófa elhárítási terv). A kockázatértékelés alapján döntik el, hogy egy rendszer elindítható-e vagy sem.

A vizsgált cégnél használnak szabványokat a kockázatok kiértékelésére, ezek a COBIT 5, az ISO 27000, 27001:2005. Alkalmaznak az architektúra menedzselésére TOGAF-ot is,

amely olyan nemzetközileg elfogadott módszertan, mely nagyvállalati architektúrák (Enterprise Architecture) menedzselésére szolgál [13].

A vizsgált cégnél van biztonsági szabályzat, amely sok részterületre kiterjed. Külön szabályzat van az alábbi területekre: személyazonosság-menedzsment (identity management), domain beléptetés, incidenskezelés, változáskezelés, üzletmenetfolytonosság, kockázatmenedzsment. Több tucat biztonsághoz köthető szabályzat és eljárás van, így külön eljárás szabályozza az alábbi területeket: vírusvédelem, sürgős, vagy ad-hoc változtatás, incidenskezelésre, patchelési folyamat (milyen gyakran, mit patchelünk, milyen tesztalakalmazások vannak). A biztonságtudatosság növelésére a cég kihasználja az elektronikus kommunikáció lehetőségeit. A szabályzatok, eljárások publikus része a vállalati intraneten keresztül érhető el, illetve emailen történik a tájékoztatás.

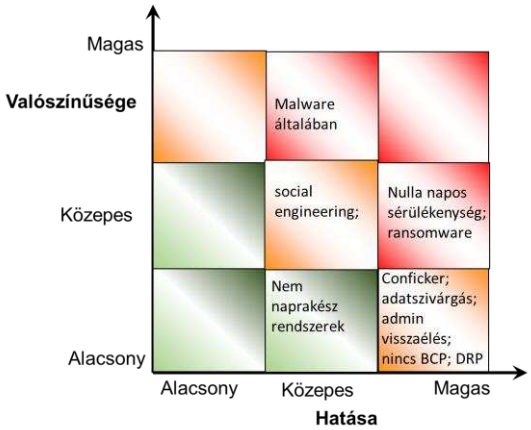
A kockázatok értékelése

A vállalatnál feltárt kockázatok értékelés a nem adhat teljeskörű képet a kockázatokról, mégis a legfontosabb vállalati kockázatokat szemlélteti. A valószínűség és a hatás is három értéket kaphat: alacsony, közepes és magas. A kockázati érték magas, ha a valószínűség vagy hatás közül az egyik legalább közepes, a másik pedig magas. A kockázati érték közepes, ha a valószínűség vagy hatás közül az egyik magas és a másik alacsony, vagy mindkettő közepes. Egyéb esetben a kockázati érték alacsony (3. táblázat).

kockázat neve	valószínűsége	hatása	kockázat értékelése	intézkedés
nulla napos sérülékenység	közepes	magas	magas	FireEye
malware általában (vírus, féreg, kémprogram, agresszív reklámprogram)	magas	közepes	magas	antivirus szoftver, kliens újratelepítés, kifele irányuló kommunikáció blokkolása
malware: ransomware	közepes	magas	magas	backup
malware: conficker vírus	alacsony	magas	közepes	vírusirtó naprakész adatbázissal
adatszivárgás	alacsony	magas	közepes	adatszivárgás elleni szoftver
visszaélés admin jogkörrel	alacsony	magas	közepes	naplózás, nyomonkövetés
social engineering	közepes	közepes	közepes	oktatás
nem naprakész rendszerek (oka: fejlesztés: nincs dokumentáció)	alacsony	közepes	alacsony	rendszerfejlesztési szabványok használata
nem naprakész rendszerek (oka: karbantartás hiány, patch nem naprakész)	alacsony	közepes	alacsony	karbantartási policy-k használata
nincs BCP, DRP	alacsony	magas	közepes	naprakész BCP, DRP

3. táblázat Kockázatok és értékelésük

A kapcsolódó kockázati mátrix látható a 9. ábrán.



9. ábra Kockázati mátrix az interjú alapján

A biztonságtudatosság

Az IT biztonsági kockázatok, kiemelten a biztonságtudatosság vizsgálatának elemzése szintén nem ad teljes képet, mivel a minta nem reprezentatív, de jól szemlélteti egy kis vagy közepes vállakozásnál (biztosítási tanácsadással foglakozó cég alkalmazottai és egy biztosítási bróker kft tanácsadói és ügyintézői) felmerülő kritikus kockázatokat és a lehetséges válaszadási eljárásokat, mivel a kitöltők szakterülete, háttere azonos. A résztvevők 56,3%-a teljes munkaidős, míg 20,8%-a részmunkaidős alkalmazott. IT biztonsági szempontból ennek azért van jelentősége, mert ismert, hogy a visszaélések nagy részét a belső alkalmazottak követik el, hiszen ők ismerik a környezetet, van hozzáférésük a rendszerekhez és az alkalmazott védelmi eljárásokat is tudhatják. A vállalkozók, partnerek (fejlesztők, tanácsadók, egyéb külső közreműködők) szintén jelenthetnek biztonsági kockázatot, pl. az informatikai területen dolgozó vállalkozók hozzáférhetnek bizalmas anyagokhoz. A kérdőíves felmérés alapján három csoport megléte feltételezhető, melyek

- a biztonságtudatos csoport, ahol a cég is figyelmet fordít az IT biztonsági kockázatok elkerülésére, a munkavállalók képzésére,
- a kevésbé biztonságtudatos csoport,
- és a kockázatot jelentő csoport, melynek egyik oka, hogy a cég nincs felkészülve a munkavállalók képzésére, így az emberi tényező okozza a legnagyobb biztonsági kockázatot.

Ezek a munkavállalók kockázatot jelentenek a cég számára, hiszen nem biztonságtudatosak, legyenek teljes munkaidős vagy részmunkaidős alkalmazottak.

A csoportképzés alapját adta, hogy két különböző klaszterezési eljárás során 9 kérdés mindkét eljárásban szignifikánsnak bizonyult, így ezekkel a változókkal készült el a csoportképzés. A következő kérdések szerepeltek a felmérésben (10. ábra).

A felmérés kérdései
Létezik-e az IT biztonságért felelős csapat a vállalatnál?
Tudod-e kit értesíts ha munkahelyeden használt gépedet vírusos, vagy egyéb támadás érte?
Észleltél-e már a munkahelyen trójai, vagy egyéb vírusos támadást a gépeden?
Tudod-e hogyan kell ellenőrizni, hogy vírusos a számítógéped?
Adtál-e már meg bármilyen munkahelyi jelszót másnak?
Ha formázod a merevlemezt, és kitörlöd a fájlokat akkor az összes adat végleg elveszik.
Milyen biztonságosnak tartod a saját számítógéped?
Engedélyezve van-e a tűzfal a számítógépeden?
Automatikus frissítésre van állítva a számítógéped?
Mennyire vagy elővigyázatos, amikor egy csatolt fájlt nyitsz meg e-mailben?
Tudod mi a "phishing"?
Van-e antivírus telepítve, frissítve és engedélyezve a számítógépeden?
Az én számítógépem értéktelen a hackerek számára.
Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?
Vannak-e rendelkezések arról, hogy hogyan, mire és mire nem használhatod az e-mailezést munka közben?
Engedélyezve van-e a vállalat bizalmas adatainak (személyes adatok, pénzügyi adatok) tárolása a saját eszközeiden?
Töltöttél-e, és telepítettél-e már le programot a munkahelyeden?
Kérte el már a főnököd, vagy bárki akit ismersz a jelszavad?
Ugyanazokat a jelszavakat használod a munkahelyen, mint a privát felhasználói fiókjaidban?(gmail,facebook...)
Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?
Amennyiben kitörölsz egy fájlt a számítógépről vagy hordozható eszközről, a rajta lévő információ már nem kinyerhető.
Részt vettél-e IT biztonsági képzésen?

10. ábra A felmérés kérdései

A két eljárásban (hierarchikus klaszterelemzés Ward módszerrel, illetve K-közép módszerrel) a csoportban körülbelül azonos számú egyed került, a válaszadások eltérőek, így a három csoport megléte valószínűsíthető [14].

Két csoport esetén az elemzés során két azonos létszámú csoport jött létre, illetve négy csoport esetén 2 csoport nagyon hasonlónak bizonyult. A három csoport esetén a következő csoportnagyságok születtek a kalszterezési eljárás során minden kérdés felhasználásával (4. ábra).

		K-közép eljárás 3 csoport			
		1	2	3	Összesen
		fő	fő	fő	fő
Ward Method 3 csoport	1	11	0	5	16
	2	0	11	10	21
	3	9	0	2	11
	Összesen	20	11	17	48

4. táblázat Csoportlétszámok Ward és K-közép eljárás során

Mivel 9 kérdés bizonyult szignifikánsnak, ezért ezekkel a változókkal K-közép eljárással újra megnéztük, hogy milyen csoportok jöttek létre, és ezen csoportokat a többi változóval együtt jellemeztük.

A kilenc szignifikáns kérdés látható a 11. ábrán.

A felmérés szignifikáns kérdései
Létezik-e az IT biztonságért felelős csapat a vállalatnál?
Tudod-e kit értesíts ha munkahelyeden használt gépedet vírusos, vagy egyéb támadás érte?
Tudod-e hogyan kell ellenőrizni, hogy vírusos a számítógéped?
Tudod mi a "phishing"?
Az én számítógépem értéktelen a hackerek számára.
Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?
Engedélyezve van-e a vállalat bizalmas adatainak (személyes adatok, pénzügyi adatok) tárolása a saját eszközeiden?
Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?
Részt vettél-e IT biztonsági képzésen?

11. ábra A felmérés szignfikáns kérdései

Érdekes módon olyan kérdések mint a jelszóhasználat, jelszóátadás bárkinek pl. főnöknek, amely a social engineering egyik kritikus eleme, vagy az emailekben érkező csatolmányok automatikus megnyitására szolgáló szabályok, illetve programletöltések nem bizonyultak szignifikánsnak.

Feltételezéseink szerint az emberi tényező nagy százalékban okoz IT kockázatot, amelyet a felmérés is alátámasztott. Ennek egyik formája a social engineering, mely jelenti például a jelszómegosztást. A biztonságtudatosságot erősíti, hogy a felhasználók jelszóhasználati szokásai a munkahelyi és a privát jelszavak esetében biztatók, jelentős részük, 81,3%-uk más jelszavakat alkalmaz a munkahelyi rendszerekben, mint a privát rendszerekben. Azonban még így is jelentős azoknak az aránya, akik azonos jelszavakat használnak a különböző rendszerekben. Ha ez a jelszó illetéktelen kezekbe kerül, akkor a felhasználó által használt rendszerekhez jogosulatlan hozzáférés valósulhat meg és így különböző visszaélésekre lesz lehetőség. Az így feltört rendszerek között lehetnek fontos vállalati adatokat tartalmazó rendszerek, de a felhasználó olyan privát rendszerei is, mint a home banking rendszer.

A válaszadók közel 23 százaléka tudatosan adta meg másnak is munkahelyi jelszavát, ezzel lehetőséget adva mások számára, hogy az ő nevében használják a rendszert, illetve azokhoz a rendszerelemekhez szerezzenek hozzáférést, amelyhez nem feltétlenül fértek volna hozzá. Az a kérdés is felmerül, hogy a nemet klikkelőkből, hányan adták meg tudtukon kívül

ezen adataikat, vagy hányszor és hogyan adtak erre lehetőséget. Az emberek többsége jóindulatú és konfliktuskerülő, és szívesen segít másnak, ezért meg sem fordul a fejükben, hogy megkérdőjelezzék a belépési adatok elkérésének okát, vagy szükségességét. Egy vállalatnál a jogosultságok kiterjedésének meghatározása fontos IT biztonsági kérdés. A jelszóátadás elkerülésére az oktatás, továbbképzés jelenthet megoldást, hiszen az emberi tényező a leggyengébb láncszem a védekezésben.

A jelszómegosztás, mint a jelszómegadás része további biztonsági kockázatokat rejthet magában. A felhasználók egy része úgy gondolhatja, hogy ha egy munkahelyi vezető, vagy a rendszergazda kéri el a jelszavát akkor azt oda is kell adni. Ez nem igaz, és egyben biztonsági kockázatot is jelent. A jelszómegosztás szintén lehetőséget ad illetéktelen hozzáférésre, visszaélések végrehajtására. Védekezni a felhasználók képzésével lehet.

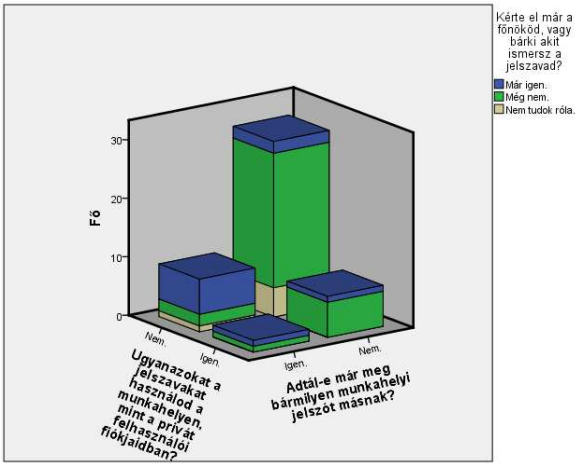
A vizsgálat biztonságtudatosságot erősíti, hiszen tudatosan csak az esetek 15%-ban adták meg az alkalmazottak a jelszavakat (6. táblázat). A 60%-os nem/nem arányt azonban szükséges növelni a tudatosság növelésével. A válaszadók több mint 20%-a már megadta a jelszavát a főnökének, amely arányt tovább kell csökkenteni. Itt közepesen erős, létező összefüggés van, mely a social engineering faktor meglétét támasztja alá (V=0,577, CHI^2=16, p=0.000).

Adtál-e már meg bármilyen munkahelyi jelszót másnak? * Kérte el már a főnököd, vagy bárki akit ismersz a jelszavad?

		Kérte el már a főnököd, vagy bárki akit ismersz a jelszavad?			
		Már igen.	Még nem.	Nem tudok róla.	Total
Adtál-e már meg bármilyen munkahelyi jelszót másnak?	Igen.	14,6%	6,3%	2,1%	22,9%
	Nem.	6,3%	60,4%	10,4%	77,1%
Total		20,8%	66,7%	12,5%	100,0%

5. táblázat Jelszómegosztás

A 12. ábrán látható, hogy vannak olyan munkavállalók, akik ugyanazokat a jelszavakat használják a munkahelyen, mint a privát felhasználói fiókokban, már meg adták a jelszavaikat másnak, és a főnökük is elkérte tőlük. Ők a legkockázatosabb csoportba tartoznak biztonságtudatosság szerint, hiszen azzal, hogy megadják jelszavukat, szinte minden fiókjukhoz illetéktelenek hozzáférhetnek.



12. ábra Jelszóhasználati, jelszómegadási eredmények

A vírusok egy jelentős része emailben csatolt fájlként érkezik. Fontos, hogy ezt tudják a felhasználók, amikor leveleznek.

A csatolt fájlok automatikus megnyitása jelentős károkozással járhat, rosszindulatú programok, pl. zsarolóprogramok telepítése történhet meg. A felmérés résztvevőinek 8,3%-a nincs tudatában ennek a problémának, ők jelentik a legnagyobb kockázatot ebben az esetben.

A felhasználók 33%-a megnyitja a csatolt fájlt, ha a feladó ismert, pedig más nevében is lehet emailt küldeni és így visszaélést végrehajtani. Ilyen szempontból a felhasználók egy jelentős része nem kellően tájékozott ezen a területen, áldozata lehet egy ilyen típusú visszaélésnek.

Bár kapcsolat nem mutatható ki a csatolt fájlok megnyitásának gyakorlata és a munkahelyi email használat korlátozása között (mire lehet és mire nem lehet a munkahelyi emailt használni), mégis az rajzolódik ki, hogy a szektorban dolgozók többsége, jelen esetben háromból kettő ember bárkivel, bárhogyan, bármiről levelezhet, tehát semmiféle módon nincsen szabályozva ez a terület. Ennél a kérdésnél is vannak olyan válaszadók (12,5 %), akik tudják, hogy vannak korlátozások, de nem ismerik őket, így nem is tudnak ezeknek megfelelni. Ez szintán kockázatot jelenthet a vállalkozás számásra.

A klaszterezés esetén ezek a kérdések nem kerültek be a klaszterképzés változói közé, de a klaszterek jellemzésébe igen. A kilenc kérdéssel elvégzett elemzés hasonló létszámú csoportokat hozott létre, mint az összes változóval elkészített klaszterek (6. táblázat).

Klaszthereknagyságok eltérése					
		Kilenc változóval készített klaszterek nagysága			
		1	2	3	Összesen
		fő	fő	fő	fő
Klaszter létszámok minden változó felhasználásával	1	15	5	0	20
	2	0	11	0	11
	3	0	5	12	17
	Összesen	15	21	12	48

6. táblázat K-közép eljárással készült klaszternagyságok eltérése

A három klaszter tulajdonságait vizsgálva az első csoport esetében létezik IT részleg, míg a második csoport többsége nem tudja, a harmadik esetében pedig többen állították, hogy nem létezik, mint azt, hogy létezik. Valószínű, hogy a harmadik csoportba tartozók kisebb cégeknél dolgoznak (pl. biztosítási bróker kft-k) ahol az IT biztonsági területhez nem tartozik külön szervezeti egység a cég mérete miatt. Az, hogy a második klaszterben lévők nem tudják, hogy van-e ilyen szervezeti egység nagy biztonsági kockázatot jelenthet, hiszen ezek a válaszadók nincsenek tisztában az IT biztonság vállalati szerepével.

A munkatársak az első klaszterben mind részt vettek IT képzésen, míg a második és a harmadik klaszterben szinte soha senki nem vett részt IT képzésen. Az első csoportban mindenki tisztában van azzal, hogy kit kell értesíteniük vírusfertőzés esetén, tudják, hogy hogyan kell ellenőrizni, hogy vírusos-e a gépük, míg a második csoport fele nem tudja kit értesítsen, és 1/3-uk nem tudja, hogyan ellenőrizze a vírusosságot. A harmadik csoport ugyan tudja kit értesítsen, de a csoport nem tudja hogyan ellenőrizze a gépét, így biztonsági kockázatot jelent a vállalat számára, hiszen nem tudja mikor értesítse az IT munkatársat.

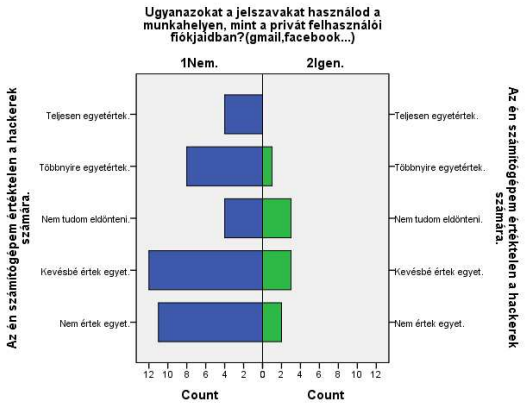
Az első klaszterbe tartozók - nevezhetjük őket most már biztonságtudatos csoportnak, ahol a vállalat számára is fontos az IT szervezeti összefogása, a munkavállalók biztonságtudatossá tétele - 87%-a ismeri az egyik gyakran előforduló visszaélést, a phishing-et (adathalászatot). Azonban a második klaszterbe tartozók - őket nevezhetjük kockázatos csoportnak, ahol megvannak a biztonságtudatosság elemei, de mivel nincs IT szervezeti egység vagy a munkatársak nem tudnak róla, és nem kapnak a munkatársak megfelelő képzést, még nem biztonságtudatos felhasználók - nem tudják mi a phishing, így könnyen megtéveszthetők. Védekezésként a felhasználók tájékoztatása javasolt pl. levélben. A harmadik csoport - az óvatlan csoport – fele nem tudja mi a phising, de itt tréninggel növelhető a biztonságtudatosság. Mindez azt jelentheti, hogy az átlag dolgozó, például egy üzletkötő sok esetben nem kapja meg a megfelelő IT biztonsági képzéseket. Ez felveti azt a problémát, hogy egy átlag felhasználónak vagy saját ismereteire, tapasztalataira kell támaszkodnia a

munkavégzése során, ha biztonságról van szó, vagy valamely másodlagos csatornából érkező információból tudja a kellő lépéseket megtenni, legyen az például egy körbeküldött email. Ennek a tudatában viszont kevésbé hibáztatható egy alkalmazott bármilyen esemény előfordulása esetén, hiszen nagyrészüknek soha nem lett ismertetve az IT biztonsági szempontból szükséges cselekvések köre. Mivel egy-egy ember is kellően nagy károkat tud okozni az informatikai vagyonban, mindenféleképpen szükséges a számítógéppel, illetve internet eléréssel dolgozók teljeskörű tájékoztatását az informatikai biztonság szempontjából.

A vállalat IT szabályozása, illetve annak ismertetése a munkatársakkal csökkenti az IT kockázatokat. Ebben a kérdésben is nagy eltérések mutathatók ki a három csoport között. A biztonságtudatos csoport esetében szabályozva van a bizalmas adatok tárolása, a különböző weboldalak használata, az email használata, illetve a programok letöltése a számítógépekre. A kockázatos csoport esetében a válaszadók 95 és 90%-a szerint sem a weboldalakra sem az emailezésre vonatkozó korlátozások nincsenek a vállalatnál, azaz kockázatos weboldalakat is megnyithatnak. A weboldalak nagy része cookie-kat használ, ami újabb kockázatot jelenthet (pl. adatokat gyűjthet a felhasználó viselkedéséről). A weboldalak látogatásának engedélyezése növeli egy lehetséges támadás esélyét. Az óvatlan csoport 25%-a említette, hogy vannak korlátozások, de nem ismeri őket, így nem is tud ezeknek megfelelni. Az email használati szabályozás még a biztonságtudatos csoportnál is kockázatot jelenthet, hiszen ugyanannyian válaszolták, hogy nincs korlátozás, mint ahányan igennel válaszoltak. A kockázatos csoport esetén semmiféle korlátozás nincs a válaszadók szerint, magában rejtve a lehetséges bejövő vírusok, fertőzött csatolmányok kockázatát.

A vállalat bizalmas adatainak kérdésében az első csoport tisztában van a szabályozással, bár 40%-ban itt is engedélyezve van a bizalmas adatok saját eszközön való tárolása, mely kockázati szempontból azt jelenti, hogy a munkahelyen használt informatikai környezet mellett az otthoni, kevésbé védett környezetben fellépő kockázatokkal is számolni kell. Az otthon használatos eszközök, különösen a portábilis eszközök, mint a mobil telefon, a laptop, tablet általában kevésbé védettek. A felhasználók elveszíthetik őket, ezeket az eszközöket könnyebb ellopni, mint a céges eszközöket, így az adatok illetéktelen kezekbe kerülhetnek. A kockázatos csoport 1/3-a nem tudja, hogy engedélyezve van-e a bizalmas adatok saját eszközön való tárolása, így a csoportban lévő másik 1/3-dal már nagy IT kockázatot jelentenek a vállalat számára. Az óvatlan csoport 15%-a nem tud szabályozásról, ezzel kisebb kockázati tényezőt jelentenek.

Alapvetően kijelenthető, hogy egyetlen hálózatra csatlakozott gép sem értéktelen a hackerek számára, hiszen sokféle támadás létezik, rengeteg, különféle céllal. Itt nem feltétlen adatlopásra kell gondolni, hiszen különböző trójai szoftverekkel, vírusokkal akár a számítógépünk felett más is átveheti az irányítást, innen végezve a támadásokat. Összességében a válaszadók nagyobb része gondolja az állítást kevésbé, vagy nem igaznak. Lényegében ebben a szektorban dolgozók, vállalati adatokat, pénzügyi adatokat és tranzakciókat, valamint személyes adatokat is kezelnek, vagy azokhoz hozzáférnek. A három csoport három különböző módon jellemezhető. A biztonságtudatos csoport mindegy egyes tagja tisztában van azzal, hogy minden gép értékes a hackerek számára, bár még itt is vannak, akik ugyanazokat a jelszavakat használják, ezzel kockáztatva az IT biztonságot (13. ábra). A kockázatos csoport 62%-a vagy nem tudja eldönteni, hogy értékes-e a gépe, vagy úgy gondolja, hogy a gépe valószínűleg értéktelen a hackerek számára, míg az óvatlan csoportban vannak a legtöbben akik teljesen egyetértenek abban, hogy gépük értéktelen a hackerek számára. Mindkét csoportban a biztonságtudatosság növelése a cél.



13. ábra Tudatos jelszóhasználat és a számítógép értéke a biztonságtudatos csoportban

A klaszterezéssel létrehozott csoportokat diszkriminancia elemzéssel visszaellenőriztük, azaz megnéztük, hogy a szignifikáns változók milyen mértékben különítik el a csoportokat, mennyivel jobb-vagy éppen rosszabb a csoportosítás az empírikus csoportosításnál. A változók közötti linearitás létezik (R=0,682), a korreláció nem mutatott kiugróan magas értékeket ($|r|<0,4$), azaz az esetek inkább függetlenek egymástól, illetve a többváltozós normál eloszlás feltételét is ellenőriztük a Mahalanobis távolság kiszámolásával. A csoportok nagyjából azonos elemszámokat tartalmaznak, és a független változók száma kisebb, mint a legkisebb csoportnagyság. A kovarianciamátrixok homogenitása éppenhogy teljesül (Box's M=125,831, sig=0,001) nagyon pici szignifikancia szint mellett. A diszkriminancia elemzés 2 erős és szignifikáns elválasztó függvény meglétét mutatja, 3 jól elkülönülő csoporttal (7. és 8. táblázat).

Eigenvalues

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Correlation
1	3,410[a]	67,8	67,8	,879
2	1,623[a]	32,2	100,0	,787

a. First 2 canonical discriminant functions were used in the analysis.

7. táblázat A két elválasztó függvény erőssége az összes változó beszámításával

Wilks' Lambda

Test of Function(s)	Wilks' Lambda	Chi-square	df	Sig.
1 through 2	,086	100,376	18	,000
2	,381	39,539	8	,000

8. táblázat A két elválasztó függvény szignifikanciája az összes változó beszámításával

A változók közül a legnagyobb hatással az IT képzésen való részvétel van a csoportokra (Wilks' Lambda=0,437), míg a „Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?", a „Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?" illetve „Az én számítógépem értéktelen a hackerek számára" kérdések közel azonos jelentőségűek (Wilks' Lambda=0,5).

A struktúra mátrix alapján az első dimenziót a szervezeti szabályozással, a vállalati IT felelősségvállalással azonosíthatjuk, míg a második dimenziót a munkavállalói biztonságtudatossággal (9. táblázat).

Structure Matrix

	Function	
	1	2
Részt vettél-e IT biztonsági képzésen?	,551*	-,394
Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?	,466*	,174
Tudod mi a "phishing"?	,379*	-,187
Tudod-e kit értesíts ha munkahelyeden használt gépedet vírusos, vagy egyéb támadás érte?	,354*	,149
Létezik-e az IT biztonságért felelős csapat a vállalatnál?	,346*	,088
Engedélyezve van-e a vállalat bizalmas adatainak (személyes adatok, pénzügyi adatok) tárolása a saját eszközeiden?	,197*	,005
Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?	,309	,613*
Az én számítógépem értéktelen a hackerek számára.	,354	-,455*
Tudod-e hogyan kell ellenőrizni, hogy vírusos a számítógéped?	,114	-,138*

Pooled within-groups correlations between discriminating variables and standardized canonical discriminant functions
Variables ordered by absolute size of correlation within function.
*. Largest absolute correlation between each variable and any discriminant function

9. táblázat A dimenziókat meghatározó kérdések

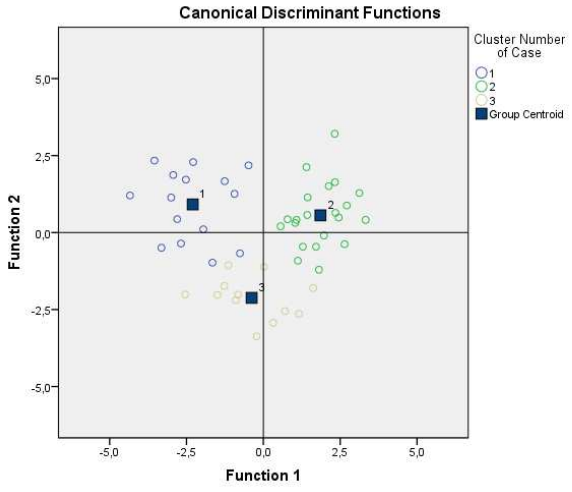
Ezek alapján az első csoport a második dimenzióban rendelkezik magasabb értékkel, a második csoport az első dimenzióban míg a harmadik csoport mindkét dimenzióban alacsony értékekkel rendelkezik (10. táblázat). Így az első csoport a biztonságtudatos, ahol a képzés teszi tudatossá a munkavállalót. A második csoport ténylegesen a kockázatos csoport, hiszen van részleges szabályozottság, de a munkavállalók sok esetben nem tudnak a szabályozásokról, nem kapnak tréninget. A három csoport inkább a szervezeti szabályozottságban különbözik, mint a biztonságtudatosságban (14. ábra).

Functions at Group Centroids

	Function	
Cluster Number of Case	1	2
Biztonságtudatos	-2,297	,914
Kockázatos	1,858	,559
Óvatlan	-,381	-2,120

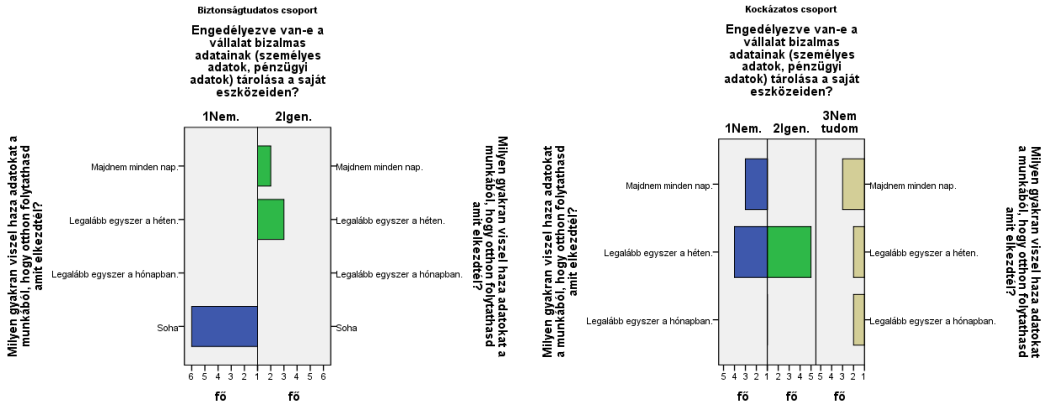
Unstandardized canonical discriminant functions evaluated at group means

10. táblázat A csoportközéppontok 2 elválasztó függvény esetén



14. ábra A három csoport elhelyezkedése kilenc változó figyelembevételénél

A biztonságtudatos csoport esetén inkább nem visznek haza adatokat otthoni munkavégzésre, azonban a kockázatos csoport vagy minden nap vagy legalább egyszer egy héten (85,7%), míg az óvatlan itt a legmegbízhatóbb, hiszen csak egy fő visz haza adatokat, s Ő is csak egyszer egy hónapban. A biztonságtudatos csoportban csak azok visznek haza adatokat, ahol a szabályzat ezt megengedi (15. ábra), míg a kockázatos csoportban annak ellenére hazaviszik az adatokat, hogy nem tudják engedélyezve van-e. Ez a sebezhetőség szempontjából különösen fontos, hiszen a saját otthonukban egy másik hálózatra csatlakozva más biztonsági feltételek mellett végzik a felhasználók ugyanazt a tevékenységet. Az is elég valószínű, hogy az otthoni informatikai környezet kevésbé biztonságos, mint egy nagyvállalatnál lévő, tehát könnyebb támadási felületnek mondható.



15. ábra Bizalmas adatok kezelése és adatok hazavitele

A klasszifikációs táblában kapott eredmények alapján a 2. és a 3. csoport találati aránya 100%, így ezek nagymértékben elkülönülnek egymástól. Mivel az 1. csoport találati aránya 86,7%, így a biztonságtudatosságot még növelni kell a munkavállalókban. A keresztvalidáció találati értéke kisebb, mint az eredeti, de a 81,3%-os teljesítménye jónak mondható, így megbízhatónak tarthatjuk a csoportosítást.

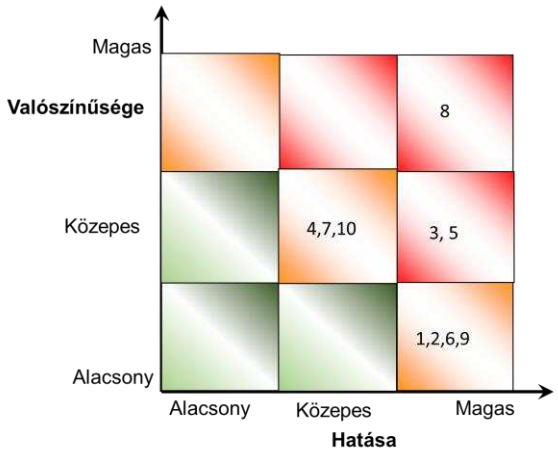
KÖVETKEZTETÉSEK

A vizsgálatok alapján kiemelhető, hogy az emberi tényező, a biztonságtudatosság, valamint a vállalati IT felelősségvállalás játszanak fő szerepet az IT kockázatok esetében. A kockázatértékelés nem ad teljes körű képet, mégis sikerült egzakt vizsgálattal alátámasztani azt az empirikus tapasztalatot, hogy a képzések, tréningek, figyelemfelhívó tájékoztatások érdemben növelhetik a munkavállalói biztonságtudatot, így a kockázatos csoporttagok illetve az óvatlan csoportba tartozók idővel a biztonságtudatos csoportba fognak tartozni. Felhasználva a cikk elején megadott kockázati mátrixot, a következő kép alakul ki (11. táblázat)

a kérdés témaköre	kockázat	valószínűsége	hatása	kockázat értékelése	intézkedés
vírusfertőzés (trójai, stb.)	1.vírusfertőzés (trójai, stb.)	alacsony	magas	közepes	antivírus program
jelszómegosztás, jelszóhasználat	2.illetéktelen hozzáférés	alacsony	magas	közepes	oktatás
adathalászat	3.adatokkal való visszaélés (adathalászat)	közepes	magas	magas	oktatás
email sebezhetőség	4.vírusfertőzés (email), adatvesztés	közepes	közepes	közepes	antivírus program
adattárolás saját eszközön	5.adatokkal való visszaélés (adattárolás)	közepes	magas	magas	oktatás, titkosítás, jogosultsági rendszer, szabályozás
számítógép védelmének hiányosságai (antivírus, tűzfal, frissítés)	6.vírusfertőzés, hackertámadás, adatszivárgás	alacsony	magas	közepes	frissítések telepítése, antivírus program, tűzfal telepítés
internet használati sebezhetőség	7.vírusfertőzés (internet), adatvesztés	közepes	közepes	közepes	szabályozás, oktatás
képzés hiánya	8. vétlen károkozás	magas	magas	magas	oktatás
nincs IT biztonsági csapat	9. nincs incidenskezelés	alacsony	magas	közepes	felelősségi körök meghatározása
programtelepítés lehetősége	10. vírusfertőzés (program-telepítés)	közepes	közepes	közepes	antivírus

11. táblázat Kockázatértékelési táblázat

A kapcsolódó kockázati mátrix látható a 16. ábrán (a számok az egyes kockázatokat jelentik).



16. ábra Kockázatértékelési mátrix

A kockázatelemzési mátrix is azt támasztja alá, hogy az emberi tényező, a képzés hiánya, a vétlen károkozás adja a legmagasabb kockázati kategóriákat, valamint a biztonságtudatossági szint nem megfelelő a vállalatnál, növelésének kiemelt szerepe van az IT biztonság területén. A válaszadók közel 70%-a soha nem vett részt IT biztonsági képzésen, így nem várható el a biztonságtudatos munkavégzés. Valamilyen formában akár a belépéskor szokásos képzés részeként meg kell jelenjen az IT biztonsági képzés. Az adathalászatot (phishing) a felmérés szerint a kitöltők 56%-a nem ismeri, pedig ez a visszaélés jelentős károkat okozhat. A bizalmas adatok saját eszközökön való kezelése, tárolása a felmérés szerint a válaszadók 35,4 százalékának engedélyezett, további 19%-a pedig nem is ismeri a szabályozást. A saját eszközök védelme általában elmarad a vállalati eszközökétől, a cégnek meg kell fontolnia a bizalmas anyagok tárolásának tiltását saját eszközökön. Közepes kategóriába kerültek a felmérés alapján a vírusfertőzés, a jelszómegosztás, az email sebezhetőség, a számítógép védelmi hiányosságok, az internet használattal összefüggő sebezhetőség, a programtelepítési lehetőség és az IT biztonsági csapat hiánya.

Javasolt a legkevesebb jogosultság alkalmazása, vagyis mindenki csak azzal a jogosultsággal rendelkezzen, amire a munkájához szükség van. Fontos az IT biztonsági kockázatok rendszeres felmérése, értékelése és ennek alapján az intézkedések aktualizálása.

Mivel a védelem leggyengébb láncszeme a felhasználó, így a biztonságtudatossággal kapcsolatos képzés az egyik legfontosabb eszköz az IT kockázatkezelésben.

FELHASZNÁLT IRODALOM

[1] Intel Security, (2015) McAfee Labs, 2016 Threats Predictions. http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf, 2016. 02 23

[2] DAVIES, S. (2015) Nem használhatja a svéd közszféra a Google felhő alapú szolgáltatásait. http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/ 2016. 02 25

[3] SCHIRMACHER, D. (2013) Phishing-Test bei der Berliner Polizei. http://www.heise.de/security/meldung/Phishing-Test-bei-der-Berliner-Polizei-3028064.html 2016. 02 12

[4] ISACA, (2015) CISA Review Manual 2015. Rolling Meadows, IL 60008 USA: ISACA.

[5] VASVÁRI, G. (1997). Biztonsági rendszerek szervezése. Budapest: Pro-Sec kft.

[6] ISACA. (2009). The RiskIT Farmework. Rolling Meadows, IL 60008 USA: ISACA

[7] CABALLERO, A. (2009). Chapter 14. In J. Vacca, Computer and Information Security Handbook. Morgan Kaufmann Publications, Elsevier Inc.

[8] ISACA Budapest Chapter. (2011). CobiT 4.1 (magyar kiadás). http://www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf, 2014. 02 15

[9] PÓSERNÉ, V. O. (2007). IT kockázatok, elemzésük, kezelésük. Hadmérnök. http://www.zmne.hu/hadmernok/archivum/2007/3/2007_3_poserne.html, 2015. 12. 11

[10] FEHÉR, P. (2012). Működési kockázatok kezelése. http://www.slideshare.net/pethich/mkdsi-kockzatok-kezelse, 2016. 03. 10

[11] IsecT Ltd. . (2016). Information security standards. http://www.iso27001security.com/index.html, 2016. 08. 22

[12] GOMBASZÖGI, A. (2016). Megint terjed a Locky "zsaroló" vírus és mutánsai . http://www.excom.hu/hir-ujdonsag-forum/hirek/64-megint-terjed-a-locky-zsarolo-virus-es-mutansai.html, 2016. 03. 23

[13] Open Group. (2011). TOGAF. http://pubs.opengroup.org/architecture/togaf9-doc/arch/, 2016. 03. 22

[14] SAJTOS, L., MITEV, A. (2007) SPSS Kutatási és adatelemzési kézikönyv, Alinea Kiadó

HADMÉRNÖK

XII. Évfolyam 1 szám – 2017. március

A NEGYEDIK GENERÁCIÓS HADVISELÉS INFOKOMMUNIKÁCIÓS ASPEKTUSAI. – FOGALMI KITEKINTŐ

INFOCOMMUNICATION ASPECTS OF THE FOURTH GENERATION WARFARE – CONCEPTUAL VIEW

JOBBÁGY Szabolcs

(ORCID: 0000-0002-2104-4665)

jobbagy.szabolcs@uni-nke.hu

Absztrakt

Értékelő elemzésemben rendszerezni kívánom a kutatási témám - A digitalizáció hatása a tábori híradás korszerűsítésére. A híradó erő modernizációja, „digitalizálása". – vizsgálatának szempontjából meghatározó jelentőséggel bíró főbb alapfogalmak definícióit és összefüggéseit. Úgy gondolom, hogy egy adott téma kutatásának egyik meghatározó része kell, hogy legyen a kérdéskörrel kapcsolatban felmerülő fogalmak tisztázása egységes értelmezésük érdekében. Ennek megfelelően egyfajta általános kitekintéssel vizsgálni kívánom a negyedik generációs hadviselés, az információs műveletek, a számítógép – hálózati hadviselés, a hálózatközpontú hadviselés, valamint a hálózat nyújtotta képesség fogalmát. Az egyes meghatározások fogalmi magyarázatán túlmenően nem kívánok kitérni azok főbb alkotóelemeire, a velük szemben támasztott követelményekre, hanem összefüggéseket próbálok meg felállítani a fogalomkör egységes keretbe, egy közös rendszerbe történő integrálása érdekében.

Kulcsszavak: *negyedik generációs hadviselés, információs műveletek, számítógép – hálózati hadviselés, hálózatközpontú hadviselés, hálózat nyújtotta képesség*

Abstract

In my evaluative analysis I would like to sum up and to systematize the main fundamental concepts, the examinations and interpretations of my research topic. My research topic is: The effect of the digitalization onto the modernization of the filed communication. The modernization, „digitization" of the CIS force I think that one of the determining parts and essential point of the research of a given topic is to clarify the occurent concepts. I wish to examine it according to this, with an uniform general looking out the definitions of the fourth generation warfare, information operations, computer network operations, network centric warfare and network enabled capability. Except the conceptual explanation of the single definitions, I do not wish to deviate their main components and requirements made on them, but I try to set up contexts into an uniform framework.

Keywords: *fourth generation warfare, information operations, computer network operations, network centric warfare, network enabled capability*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.04.

BEVEZETÉS

Korunk modernkori hadviselése egy hosszas, több lépcsőt magába foglaló fejlődési, átalakulási folyamaton ment keresztül, mígnem eljutott jelenlegi formájába. Ennek a változásnak az eredményeképpen nem csak a hadászati, hadműveleti, harcászati elvek, a hadelmélet alapvetései, a szembenálló felek és erőviszonyok, hanem az alkalmazott eljárások és eszközök tárháza, valamint az információcsere célját szolgáló különböző kommunikációs eljárások, megoldások, lehetőségek és eszközök is megváltoztak. Számos esemény zajlott le a világban, mely az egyes generációk kialakulását indukálta, és meghatározta legfontosabb jellemzőiket. Ezen események között egyrészt megemlíthetünk akár a világ számára pozitív hozadékkal bíró olyan kiemelkedő történéseket is, mint például az ipari forradalom időszaka és befolyásoló hatása, a globalizáció és ezáltal az egyes folyamatok, történések világméretű elterjedése és következményei. Másrészt sajnos szót kell ejtenünk olyan sajnálatos, számos emberéletet követelő vagy az emberiségre veszélyt jelentő momentumokról is, mint például a polgárháborúk, világégések kora. A negatív befolyásoló tényezők sorát akarva-akaratlan ki kell egészítenünk a terrorizmus retteget időszakával is, melynek történései közül a teljesség igénye nélkül megemlíthetjük például az Oszama bin Laden terroristavezér által irányított Al-Kaida radikális iszlamista terrorszervezet nevéhez fűződő, 2001. szeptember 11-én kivitelezett terrortámadást az Egyesül Államok ellen, a World Trade Center Világkereskedelmi Központ ikertornyainak és egyéb célpontoknak a megtámadása által.

Az első generációs hadviselés korszaka nagyjából a tizenhetedik és a tizenkilencedik század közepe közötti időszakra tehető, amely még egy klasszikus értelemben vett, nemzetállamok között kialakuló konfliktusok által gerjesztett, hadseregek által megvívott, merev szabályokat követő, az élőerő jelentőségére összpontosító hadviselési forma volt. Korszakolásának kezdő eseményeként a vesztfáliai békekötés, míg záróeseményeként az amerikai polgárháború időszakát jelölhetjük meg. [1] Az alkalmazott eszközök alapvetően a korra jellemző hagyományos fegyverek voltak. A háborúk célja pedig elsősorban a területi uralom megszerzése, az esetleges béketárgyalásokon az irányító szerepe megragadása, döntési pozíció megszerzése volt. Jelen-tős és alapvető hatást gyakorolt ezen időszak hadviselésére a közben végbemenő ipari forradalom is. A korszak jelentős személyiségei között olyan neveket kell megemlítenünk, mint Raimondo Montecuccoli, Bonaparte Napóleon vagy Karl von Clausewitz. [2]

Az ezt követő *második generációs hadviselés* időszaka az 1861-1865 között lezajlott amerikai polgárháborúval vette kezdetét, és alapvetően az első világháború 1914-1918 közötti időszakának történéseivel zárult. Kiteljesedésének olyan események adtak lökést, mint még az ipari forradalom továbbra is érezhető hatása vagy a francia forradalom eseményei. A korábbi generáció élőerő koncentrálásának elvétől eltérően itt már jellemzően a tűzerő koncentrálására, összpontosítására tevődött át a hangsúly. Az első generációban alkalmazott muskéta és vonalharcászat helyett ennek a korszaknak legfontosabb jellemzője a tüzérség, a géppuska, géppisztoly, a harckocsik és harci repülőgépek, valamint a tengeralattjárók által megvívott harc, az ipari forradalom vívmányaiként megemlíthető vasút és gőzhajók által megvalósított csapatmozgások, szállítások és utánpótlások biztosítása volt. Előtérbe került az egyes fegyvernemek közötti együttműködés szorosabbra fűzése, a fegyveres küzdelmek legfontosabb célkitűzése pedig a katonai potenciál, az élőerő felőrlése, teljes megsemmisítése volt. Ez az a momentum, mely a következő generációra jellemző hadviselés során átalakult, hiszen az erre az időszakra jellemző, az erőt és eszközöket érintő teljes megsemmisítésére irányuló törekvéseket felváltja az élőerő demoralizálásának, harctól való elállási szándékának erősítésére irányuló elképzelés. A második generációs hadviselés kiemelkedő személyei között kell szót ejtenünk többek között Erwin Rommel tábornokról vagy Helmuth Johannes Ludwig von Moltke vezérezredesről. [1] [2]

Minden egyes generációt a rá jellemző sajátosságok alapján egy jól beazonosítható jelzővel illettek. Addig, amíg az első generációt a muskéta és vonalharcászat, a második generációt az összpontosított tűzerő jelzővel illették, addig a *harmadik generációs hadviselésre* a mobilitás jelzőt ragasztották. Korszakolása a II. világháború és az I. Öböl-háború közötti időszakra datálható. Sajátosságaira legnagyobb hatást Heinz Guderian, Mikhail Tukhachevsky, John Frederick Charles Fuller vagy Basil Liddell Hart elképzelései gyakoroltak. A harci siker kivívása legfontosabb eszközének a gyors mozgások végrehajtását, az erők és eszközök meglepetésszerű alkalmazását, a mélységi hadműveletek végrehajtását, a bombázókkal felszerelt gépesített hadseregek alkalmazását, a totalitás elvének követését, a hátország háborúba történő bevonását és támadását tartották. A harc megvívásának legfontosabb célkitűzése részben az ellenség erejének megsemmisítése mellett harci kedvének megtörése, az erők és eszközök ellátásának, valamint az információcserének a megakadályozása volt. Utóbbi célkitűzésre már csak azért is fokozott hangsúlyt helyeztek, mert ebben a korszakban már egyre nagyobb jelentőséggel bírt a különböző híradó eszközök alkalmazásával megvalósított híradás, kommunikáció, információcsere végrehajtása. [1] [2]

Ezen folyamatok eredményeképpen jutunk el a *negyedik generációs hadviseléshez*, mely korunk jellemző hadviselési formája. Kibontakozása egészen a Szovjetunió szétesésének időpontjára nyúlik vissza, és napjainkban is újabbnál újabb formában ölt testet a megjelenő új fenyegetések, kihívások, szembenálló felek, alkalmazott eszközök, technológiáknak- és technikák következményeképpen. Olyan jellemzőkkel írhatjuk le leginkább, mint az asszimetrikus hadviselés, mely elsősorban az egymással szemben álló felek erőviszonyaira, irreguláris mivoltukra, az általuk alkalmazott harceljárások és harceszközök sajátosságaira utal. Meg kell említenünk a felsorolásban az állami és nem állami szereplők együttes megjelenését a modern kor átértékelődött vagy a technológiai- és technikai fejlődésnek köszönhetően kialakuló digitális hadszínterein, a nem csupán katonai célpontok ellen intézett támadásokat, a rettegés, megfélemlítés, a biztonság hiányára utaló érzés kialakítását az emberekben, melyek főleg a globális, sejtszerű, szélsőségesen radikális, elvakult vallási, etnikai vagy egyéb ideológiákat követő csoportok megjelenésének köszönhetőek. Nem feledkezhetünk meg olyan közkeletű kifejezésekről sem, mint a hibrid, hálózatközpontú vagy kiberhadviselés, és hálózat nyújtotta képesség sem. Ezek eredményeképpen az ilyen jellemzőkkel bíró hadviselésnek az egyik legfontosabb célkitűzése az információs fölény megszerzése. Somkuti Bálint A negyedik generációs hadviselés-az érdekérvényesítés új lehetőségei című PhD értekezésben az alábbi definíciót adja a negyedik generációs hadviselésre: „*Ez a módszer pontosan meghatározott politikai célok érdekében végzett, gyakran több szervezet ideológiai közösségén alapuló általában nem-katonai tevékenység, mely szakít a hagyományos hadviselés szabályaival és hatását több, egymást kiegészítő és felerősítő területen végrehajtott katonai és nem-katonai műveletek eredményképpen fejti ki.*" [2; 6. o.] Jellemzői között pedig olyan tényezőket sorolt fel, mint például a [2]:

- clausewitzi „szentháromság" megszűnése;
- a nem állami szereplők részvétele a háborúkban, harcokban, fegyveres konfliktusokban, terrorista akciókban;
- a hagyományos, ipari alapú konfliktusok háttérbeszorulása;
- a népi (ideológiai, vallási) háborúk újjáéledése;
- a propaganda központú hadviselés;
- kizárólag katonai eszközökkel nem megnyerhető;
- nem haditechnika centrikus;
- totális;
- a fegyveres konfliktus alacsony intenzitású, térben és időben korlátozott;
- asszimetrikus;
- valamint a modern és üzleti megoldások egyöntetű alkalmazása.

A negyedik generációs hadviselés elméletét elsőként William S. Lindt fogalmazta meg A Háború változó arca: A negyedik generáció felé című tanulmányában, melyben rámutatott többek között arra a fontos tényre, hogy ebben a jellegű hadviselési formában a szembenálló felek decentralizált logisztikai, szervezeti és vezetés-irányítási rendszerek kialakítására fognak törekedni. [1]

INFORMÁCIÓS MŰVELETEK (INFOOPS)

A XXI. század társadalma az információs társadalom. Ezt az újfajta társadalmi szerveződést, struktúrát több tényező együttes hatása befolyásolja, határozza meg, és alakítja fejlődési irányvonalát. Ezek között beszélhetünk egyrészt a konvergencia, a telematika, az új technológiák- és technikák térhódítása, az IoE és IoT világának kérdéséről. Másrészt egy másik megközelítésből megvilágítva a kérdéskört, említést kell tennünk az új típusú hadviselés, ellenség, hadszíntér és a modernkori háborúk megvívásához szükséges számtalan újfajta harceljárás, harcmód és harceszközről is, hiszen az információs társadalom vívmányai és ezzel párhuzamos negatív velejárói a védelmi szférát sem hagyják érintetlenül. Mindezek mindegyikét alapvetően meghatározó építőeleme pedig nem más, mint az információ, mely az új kor viszonyai között jelentős mértékben át- és felértékelődött, mely hatalommal bír, melynek megszerzése vagy valamilyen formában történő befolyásolása, az információs fölény megszerzése alapvető célkitűzése az új típusú hadszíntéren, új típusú hadviselési elveket követő, új típusú szembenálló felek harcának. Ebben a keretben kell elhelyeznünk és meghatároznunk az információs műveletek lényegét is, melyek korunk negyedik generációs hadviselésének meghatározó és alapvető részét képezik. Somkuti Bálint PhD értekezésében is erre találhatunk utalást, amikor is a negyedik generációs hadviselés öt fő részterületének egyikeként ezt az újfajta hadviselési módot is azonosítja. A részterületek az alábbiak [2; 72. o.]:

- „globális gerilla hadviselés, ideértve a kritikus infrastruktúra elleni és terrortámadásokat;
- információs hadviselés, ezen belül kiberhadviselés;
- gazdasági manipuláció, pénzügyi manőverek;
- ideológiai, emberi jogi illetve egyéb percepción alapuló médiaműveletek;
- valamint ezek egyesítése államok és nem-állami szereplők részéről.”

A Magyar Honvédség Információs Műveletek Doktrínája (Ált/57) 2014. évi I. kiadása alapján az információs műveletek, mint egyfajta speciális, újkori, korszerű katonai műveletetek elsősorban a stratégiai kommunikáció (STRATCOM)[1] [3; 13. o.] részeként, mint más képességekkel összehangoltan az adott stratégiai cél elérése érdekében alkalmazott képesség értelmezhetőek. A doktrína megfogalmazása szerint az „*INFOOPS az információs környezet elemzéséhez és a hatástervezéshez kapcsolódó törzsfunkció. Tervezi, koordinálja, majd értékeli az információs tevékenységeket*[2]*, integrálja azokat a katonai műveletek sorába annak érdekében, hogy elérje a kívánt hatást a célközönség akaratában, megértésében és*

[1] Stratégiai kommunikáció: „a NATO/adott nemzet kommunikációs tevékenységek és képességek, úgy-mint a nyilvános diplomácia (PD), a tömegtájékoztatás, Civil PA (Public Affairs), katonai tájékoztatás (MPA), információs műveletek (INFOOPS) és Lélektani Műveleti (PSYOPS) összehangolt és megfelelő használata a stratégiai célok elérése érdekében.”

[2] Információs tevékenység: „azok az akciók/cselekmények, illetve bevezetett rendszabályok, melyek célja, hogy hatást gyakoroljanak az információra és/vagy az információs rendszerekre az információs környezetben, a kívánt változás elérése érdekében.”

képességeiben a küldetés célkitűzéseinek teljesítéséhez. A célközönséget a szemben álló felek, a lehetséges szemben álló felek és más, a politikai szint által jóváhagyott személyek és meghatározott csoportok alkotják." [3; 17. o.]

Az információs műveletek folyamán, melyek egyaránt megjelenthetnek stratégiai, hadműveleti és harcászati szinten is, az információs célkitűzések elérésére, támogatására különböző képességeket, eszközöket és eljárásokat alkalmaznak. Ennek képezik szerves és integráns részét többek között a számítógépes hálózatokkal végrehajtott műveletek, a számítógép-hálózati hadviselés. Az egyéb képességek eljárások és eszközök a következőek [3]:

- lélektani műveletek (PSYOPS[3]);
- megjelenés, viselkedés és arculat (PPP[4]);
- műveleti biztonság (OPSEC[5]);
- információs biztonság (INFOSEC[6]);
- megtévesztés (Deception);
- elektronikai hadviselés (EW[7]);
- fizikai megsemmisítés;
- kulcsfontosságú vezetőkkel való érintkezés (Key Leaders Engagement);
- valamint a civil-katonai együttműködés (CIMIC[8]).

SZÁMÍTÓGÉP – HÁLÓZATI HADVISELÉS (CNO)

Az általam ismertetett, rendszerezett fogalmak elemzése, felvonultatása során nyilvánvalóvá válik az a gondolat, hogy ezek egymástól markánsan nem különíthetőek el, egyik a másiknak valamilyen formában, de szerves részét képezi, velejárója, vagy legalábbis hatást gyakorol arra. Nincs ez másként a számítógép-hálózati hadviselés esetében sem, mely, mint az az iménti felsorolásából mindenki számára nyilvánvalóvá válik, szerves és meghatározó részét képezi az információs műveleteknek, valamint végső soron ezáltal a negyedik generációs hadviselésnek is.

A számítógép-hálózatok felhasználásával végrehajtott hadviselés egy összetett forma, mely „*magában foglalja a számítógépes hálózatok struktúrájának feltérképezését, a forgalmi jellemzőik alapján hierarchikus és működési sajátosságainak feltárását, a hálózaton folytatott adatáramlás tartalmának regisztrálását, a célobjektum programnak és adattartalmának megváltoztatását, megsemmisítését, valamint a szemben álló fél hasonló tevékenysége elleni védelem kérdéseit.*" [3; 29. o.] A számítógép-hálózatok felhasználásával vagy éppen az azok ellen irányuló hadviselés műveletei három fő területre bonthatóak szét, melyek az alábbiak [3; 29. o.]:

- „számítógépes-hálózati felderítés (CNE[9]);
- számítógépes-hálózati támadás (CNA[10]);
- számítógépes-hálózati védelem (CND[11])."

[3] Psychological Operations
[4] Presence, Posture, Profile
[5] Operational Security
[6] Information Security
[7] Electronic Warfare
[8] Civil-Military Cooperation
[9] Computer Network Exploitations
[10] Computer Network Attack
[11] Computer Network Defence

A számítógép-hálózati hadviselés összetettségére utal, hogy napjainkban számos különböző elnevezéssel hivatkoznak rá, például informatikai hadviselés, de az egyik talán legközkedveltebb és széles körben elterjedt megnevezése napjainkban a kiberhadviselés. A kiberhadviselés rendszerbe történő elhelyezése érdekében beszélhetünk ezzel kapcsolatban számos más közkeletű fogalomról is, melyek megjelenhetnek a szakirodalomban, s melyek mindegyike szerves részét képezi annak az gyűjtőkategóriának, melyre kiberfenyegetésként hivatkozhatunk. Ennek részeként, a kiberhadviselés mellett az alábbi fenyegetéstípusokat említhetjük meg:

- kiberbűnözés[12];
- hacktivitizmus[13];
- kiberterrorizmus[14];
- kiberkémkedés[15].

Bárhogyan is nevezzük ezt a fajta hadviselést, egyik legfontosabb célja az egymással valamilyen hálózati infrastruktúrán, átviteli közegen egy rendszerbe kapcsolt számítógépek által alkotott hálózat, annak eszközeinek, erőforrásainak megbénítása vagy éppen egy végrehajtott támadás hatásainak csökkentése, a megtámadott hálózat, infrastruktúra, rendszer, erőforrások működőképessé tétele, szolgáltatások biztosítása, stb.

Ennek megfelelően az alkalmazott eszközök tárháza is elég széles körű lehet, mely alatt érthetjük a különböző kártékony programok, alkalmazások (vírus, féreg, trójai, backdoor, malware, spyware, csomagvizsgáló, nyomkövető alkalmazások, DOS[16], DDOS[17], stb.) segítségével végrehajtott alapvetően szoftvereken alapuló támadásokat, de alkalmazhatóak különböző hardveres eszközök is (illetéktelen, jogosulatlan hálózati eszközök, erőforrások, stb.). [4]

HÁLÓZATKÖPONTÚ HADVISELÉS (NCW)

Az Észak-atlanti Szövetség Szervezetének mindennapjait a bipoláris világrend megszűnését követően tulajdonképpen a folyamatos útkeresés jellemzi, mely köszönhető többek között a hagyományos, klasszikus értelemben vett szembenállás átértékelődésének, az állandóan változó biztonsági környezetnek, a megjelenő új kihívásoknak, valamint a folyamatosan átalakuló, változó hadviselési elveknek. Ezen útkeresést igazolják az egyes NATO csúcstalálkozók döntései is. A modern kor haderejének ilyen keretek között kell a tevékenységét végrehajtania, és kell megfelelnie számos kritériumnak annak érdekében, hogy az újabbnál újabb és változatosabbnál változatosabb kihívásokra hatékony és korszerű elveket

[12] A bűnözők célja leginkább a profitszerzés például különböző kártékony szoftverek alkalmazásával (ransomware vírusok, malware, darkweb, stb.). A végrehajtott támadások irányulhatnak akár magánemberek, de ugyan így állami, önkormányzati vagy a védelmi szféra szereplői ellen is

[13] Célja szinte megegyezik a kiberterrorizmus céljával, amikor is különböző hackercsoportok hajtanak végre támadásokat valamilyen ideológia képviselése, terjesztése, népszerűsítése, figyelemfelhívás, az információszabadság elvének biztosítása céljából. Kiemelkedő példaként említhetnénk meg a WikiLeaks botrányt.

[14] Lásd hacktivitizmus

[15] Legfontosabb célkitűzése az információk megszerzése, mely tevékenységet egyaránt kifejthetik magánemberek, vállalatok, szervezetek vagy állami szereplők is. Olyan kifinomult technikák alkalmazásával hajtható végre többek között, mint például a social engineering.

[16] Denial of Service: Szolgáltatás megtagadás támadás, melynek legfőbb célja a jogosult felhasználók és eszközök hozzáférésének megakadályozása, megbénítás a hálózat eszközeihez, erőforrásaihoz.

[17] Distributed Denial of Service: A DOS támadás egy speciális módja, melynek során ugyan azzal a céllal, de nem egy eszközt, hanem eszközök egy csoport használják fel a támadás kivitelezésére.

követő megoldásokkal, válaszlépésekkel, ellencsapásokkal legyen képes reagálni. Ennek a folyamatos változások által indukált környezetnek a következménye sok más tényező közepette a hálózatközpontú hadviselés elvének és gyakorlatának megszületése is, mely kutatások, elemzések alapján elválaszthatatlan fogalom a hatásalapú műveletek megközelítéstől, együttesen alkotva ezáltal a negyedik generációs hadviselés meghatározó összetevőit, jellemzőit.

A hatásalapú műveletek fogalmára Prof. Dr. Szternák György alapul véve a vonatkozó szakirodalom meghatározásait, az alábbi megfogalmazást adta: „*A mértékadó hazai és külföldi szakirodalom szerint a többnemzeti, összhaderőnemi katonai műveletek hatásalapú megközelítése azt jelenti, hogy a rendelkezésre álló katonai- és más erőket, eszközöket átfogó, egymást kiegészítő módon alkalmazzuk a kitűzött célok (súlypontok, végállapot) megvalósítása érdekében. Ez a megközelítés filozófiai változást jelent a katonai műveletek végrehajtásának formájában és módszerében.*" [5]

Egy rendszerszemléletű gondolkodási elvet követve megállapíthatjuk, hogy a hatásalapú katonai műveletek elképzelése magával hozta a hálózatközpontú hadviselés koncepciójának megalkotását is. A korszerű, modernkori katonai műveletekben különböző rendszerek és alrendszerek állnak kapcsolatban egymással, és természetesen hatnak is egymásra úgy, mint a kommunikációs, információs, vezetési, valamint pusztító rendszerek, alrendszerek. Prof. Dr. Szternák György szerint ezek a hálózatközpontú hadviselés alapvető összetevői, melyre az alábbi fogalmi meghatározást adja: „*A hálózatközpontú katonai művelet lényege, hogy egy rendszert alkot a felderítés, a döntés és a cél pusztítása a katonai műveletek végrehajtása teljes időtartamában. A katonai műveletek hálózatközpontú módon történő megvívása kiváló képzettségű katonákat követel, akik a különböző információs, számítógépes eszközöket kezelik. A hálózatközpontú katonai művelet sem helyettesíti viszont a parancsnokok és a katonák szakmai (katonai) tudását valamint felkészültségét. Más szóval, annyi információt továbbíthatunk csak a döntéshozóknak, hogy pontosan megértsék a kialakult helyzetet, nem többet. A hálózatközpontú katonai műveletek a szárazföldi haderőnem számára lehetővé teszik számítógépen keresztül az információcserét a többi haderőnemmel és más erőkkel. A parancsnokok állandóan valós képet kapnak a hadszíntéren folyó tevékenységekről, ez alapján a felderítés-célkiválasztás-csapás ideje lényegesen csökkenthető.*" [5; 5. o.]

Szeretném felhívni ezen megfogalmazás egyik alapvető momentumára a figyelmet, mely alátámasztja témaválasztásom indoklását, miszerint a modern kor körülményei között egy olyan korszerű haderőre van szükség, mely a megváltozott hadviselési elveknek megfelelően, a technológiai- és technikai fejlődés vívmányaival lépést tartó, azt eredményesen alkalmazni képes, infokommunikációs ismeretekkel felvértezett szakmai állomány meglétét feltételezi és követeli meg. Ennek hiányában nem valósítható meg a különböző rendszerek együttműködése, a vezetés és irányítás összhangja, az új szemléletű gondolkodásnak megfelelő haderő kialakítása, valamint az új kihívásokra modern, korszerű eszközökkel, eljárásokkal, elvekkel történő reagálás képessége.

Annak ellenére, hogy negyedik generációs hadviselésről, modernkori, korszerű elvekről, eljárásokról teszünk említést, sok esetben jóval régebbre kell, hogy visszanyúljon vizsgálódásunk gyökere, hiszen ezek a jelenségek már sokkal korábbi háborús események folyamán teret nyertek, felszínre törtek. Nincs ez másként a hálózatközpontú hadviselés esetében sem. Gondoljunk csak vissza a negyedik generációs hadviselés korszakolásának kezdő momentumára, melynek a Szovjetunió összeomlását említettem meg. A hálózatközpontú hadviselés estében ez a visszatekintés egészen a második öbölháborúig kell, hogy érjen, amikor is Dr. Resperger István ezredes úr kutatásai alapján „*a Szövetségesek a XXI. századi haderőt, a „hálózatközpontú hadviselést" (Network Centric Warfare-NCW), a korlátlan légi uralmat, az információs hadviselést, a pszichológiai hadviselést, a speciális összhaderőnemi (joint) hadviselést testesítették meg, amihez az ellenség valós időben, minden*

év és napszakban elérhető helyzetképe járult hozzá, amivel az ellenség minden tevékenységét nyomon követhették. Az amerikai haderő a „képesség alapú" hadviselésről áttért a „hatás alapú" hadviselésre. Ebben a háborúban a bevetett fegyverek 85%-a már precíziós vezérlésű, az NCW lehetővé teszi a törzsek számára a leghatásosabb és leghatékonyabb haderőnem, fegyverhordozó, valamint fegyvertípus kiválasztását. Az ellenség helyzetének valós idejű ismerete lehetővé tette a csapások koordinálását, a megfelelő válaszlépések végrehajtását." [6]

Ezen a ponton szeretnék visszacsatolni publikációm számítógép-hálózati hadviselés fogalmi vizsgálódásának részéhez, nevezetesen a kiberhadviselés kérdésköréhez, mely ugyancsak nem annyira új keletű jelenség, mint azt megítélésem szerint a fogalom használatának kezdete sugallná. A kibertámadások vonatkozásában is legalább a 2007. évi esztendő történéseiig vissza kell tekintenünk, ha nem korábbi időszakra, amikor is pl. feltételezhetően Oroszország kibertámadást intézett Észtország ellen a két ország között egy Tallinban található szovjet hősi emlékmű eltávolítása miatt kialakult pattanásig feszített diplomáciai helyzetben. Láthatjuk tehát, hogy illessük is bármilyen jelzővel a folyamatosan változó környezetnek megfelelni törekvő hadviselési elveket, csíráikban, valamilyen kezdetleges formában, a jelen kor körülményei között is helytálló, jól körülhatárolható, beazonosítható célkitűzések elérése érdekében már jóval korábban jelen voltak, mint az őket leírni próbáló fogalmak a köztudatba kerültek volna.

HÁLÓZAT NYÚJTOTTA KÉPESSÉG (NEC)

Közleményem témaválasztásának alátámasztása, indoklása miatt szükségesnek ítélt fogalmi okfejtések sorát a hálózat nyújtotta képesség rövid, tömör vizsgálatával szeretném zárni.

2011. szeptember 11-ét követően valami markánsan megváltozott a világban. Mindenkinek rá kellett döbbennie arra, hogy a terrorizmus és a hozzá hasonló új típusú kihívások és fenyegetések fogják meghatározni ebben az új korszakban nem csak az emberek, hanem az országok, politikai rendszerek, az egész világ, és ennek következtében a védelmi szféra, valamint a különböző szövetségesi rendszerek mindennapjait, további fejlődésük, stratégiai elképzeléseik főbb irányvonalát, az Észak-atlanti Szerződés Szervezetének esetében a már oly sokat emlegetett folyamatos útkeresés főbb mérföldköveit. Mint azt már korábban említettem volt, a terrortámadást követő időszak szinte minden egyes NATO csúcstalálkozóján született valamilyen döntés a modern kor új típusú kihívásaira választ adni, reagálni képes korszerű elvekkel, eljárásokkal, eszközökkel, rendszerekkel, összességében a negyedik generációs hadviselést érintő alaptézisekkel kapcsolatban. Ennek részeként értelmezhető a *hálózat nyújtotta képesség* megjelenése is.

A csúcstalálkozók sorából a hálózat nyújtotta képességet illetően, mint kiindulási alapot, a terrortámadást követő első, 2002. november 21-22. között Prágában megrendezésre került NATO tagállamok állam és kormányfőinek egyeztetését emelném ki, mely a hidegháború lezárását követő időszak ötödik soron következő fóruma volt, elsőként egy olyan ország területén, amelyet Magyarországgal egy időben vettek fel a NATO tagországok sorába 1999-ben. Mint arra Dr. Tóth András százados úr A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében című PhD értekezésében rávilágított, ekkor született döntés először a NATO Tanácsadó, Vezetés-irányítási Tanácsa (NC3B[18]) által egy, a NATO reagáló erő mindennemű tevékenységének támogatásához szükséges, kommunikációs háttér kiépítésének célját is szolgáló, az amerikai hálózatközpontú

[18] NATO Consultation, Command and Control Board

hadviselés elvére megszervezett képesség kialakításának tervéről. [7; 18-20. o.] Ez maga a hálózat nyújtotta képesség, mely a prágai képesség-felajánlási dokumentum részeként értelmezhető. [6] Mindezek mellett az alábbi határozatok, döntések születtek a NATO tagországok állam és kormányfőinek ezen a találkozóján, melyek meghatározó jelentőséggel bírtak a soron következő egyeztetések megtárgyalandó kérdései vonatkozásában:

- NATO Reagáló Erő (NRF[19] [8; 2. o.]) felállítása;
- elfogadták a prágai képesség-felajánlási dokumentumot (PCC[20] [8; 2. o.]);
- a szövetség parancsnoki struktúrájának megújítása;
- véglegesítették a hidegháborút követő második bővítési folyamat által érintett részvevőket tartalmazó listát.

A százados úr a hálózat nyújtotta képességet külföldi forrásokra hivatkozva az alábbiakban határozta meg. „*A hálózat nyújtotta képesség magába foglal minden olyan eszközt, amely szükséges az ellenőrzött és precíz katonai hatások gyors és megbízható szállításához. Az alapját három elem biztosítja: az érzékelők (információgyűjtés), a hálózat (biztosítani, kommunikálni és felhasználni az információt), és a csapásmérő eszközök, amelyek biztosítják a katonai hatást. A kulcsa az a képesség, hogy összegyűjti, biztosítja és terjeszti a pontos, időszerű és releváns információkat jelentős gyorsasággal (néha csak percek alatt, vagy akár "valós időben"), hogy segítséget nyújtson a parancsnokok részére a közös helyzetkép kialakításában minden szinten.*" Továbbá leszögezte azt, hogy „*A hálózat nyújtotta képesség kellő időben a megfelelő helyen képes biztosítani az információkat, felderítési adatokat, ezzel támogatva a parancsnoki döntéshozatali folyamatokat és tevékenységeket. Ennek kialakításához szükséges a rendelkezésre álló eszközök, szoftverek, eljárásmódok, struktúrák és személyzet fejlesztése alátámasztva egy biztonságos, robosztus, kiterjedt hálózattal.*" [6; 26. o.]

Meglátásom szerint a hálózat nyújtotta képesség ezen meghatározása által ugyancsak alá tudom támasztani, meg tudom indokolni, és értelmet nyer közleményemnek a személyi állományt érintő modernizációjára, digitalizációjára törekvő elképzelés szükségszerűsége, korszerű hálózati ismeretekkel történő felvértezésük által. Nem is lehetne ez másként, hiszen Magyarország és hadereje, mint NATO tagország ebben a működési környezetben kell, hogy tevékenykedjen, ugyanazoknak a kritériumoknak kell, hogy megfeleljen, ugyanazokra a kihívásokra kell, hogy választ adjon, és legfőképpen képes kell legyen együttműködésre akár honi, akár országhatáron kívül több nemzeti kötelékben végrehajtott műveletek folyamán más NATO tagországok haderejével, ami alatt akár a szakmai állomány, akár a különböző infokommunikációs hálózatok és rendszerek együttműködését is kell értenünk. Már csak azért is, mert a NATO Reagáló Erő felállítása a Magyar Honvédségre is kötelezettséget ró azáltal, hogy készenléti szolgálat jelleggel alegységeket kell biztosítani, felajánlani e kötelékbe.

---

[19] NATO Reaction Force: „*Az NRF olyan, technológiailag magas szintű, rugalmas, bevethető és fenntartható erő, amely szárazföldi, haditengerészeti és légierő csapatokból, valamint különleges műveleti erőkből áll, s amely bárhol alkalmazható.*"

[20] PCC: Prague Capabilities Commitment: „*Ennek keretében az állam- és kormányfők kötelezettséget vállaltak arra, hogy négy képességterületen fejlesztik haderejüket: a vegyi, biológiai, radiológiai és nukleáris támadás elleni védelemben; a vezetésirányítási, kommunikációs és információs fölény biztosításában; a telepített erők interoperabilitásának és harci hatékonyságának fejlesztésében; illetve a csapatok gyors telepíthetőségében és működőképességük fenntartásában.*"

KÖVETKEZTETÉSEK

Jelen publikációmat egy korábbi cikkem folytatásaként – mely a Híradás, hírrendszer, vezetés-irányítási rendszer. Fogalmi kitekintő címet viseli – ajánlom az érdeklődők figyelmébe. Azon cikkem témájához hasonlóan, jelen írásom alaptéziseit is alapvetően a XXI. század, korunk legmeghatározóbb jelentőséggel bíró társadalmi szerveződése, az információs társadalommal kapcsolatos alapgondolatok mentém fűztem fel.

Láthatjuk tehát, hogy a történelem folyamán hogyan alakultak, bontakoztak ki a különböző hadviselési elvek, milyen események hatások befolyásolták azokat, melyek eredményeként minden egyes generációnak egy jól beazonosítható célkitűzése, hadviselési elképzelése, és az ezek elérését, megvalósítását szolgáló módszer és eszközrendszere alakult ki az idők folyamán, mígnem eljutottunk korunk jellemző hadviseléséhez, a negyedik generációs hadviseléshez. Ez utóbbi azonosulva a kor újszerű és változatosabbnál-változatosabb kihívásaival, fenyegetéseivel és lehetőségeivel egy folyamatos és állandó átalakuláson és megújuláson megy keresztül, melyre legnagyobb hatást ennek az új keletű társadalomnak a technológiai- és technikai vívmányai gyakorolják függetlenül a szembenálló felektől. Gyakorlatilag a kezdetektől fogva ezek a befolyásoló tényezők hatják át az Észak-atlanti Szövetség Szervezetének szinte minden egyes csúcstalálkozóját, ahol az egyes tagországok állam és kormányfői folyamatosan azon munkálkodnak, hogy a jövőben milyen irányba formálják a nemzetközi katonai-politikai közösség kollektív védelemről szóló elképzelését. Ennek jegyében természetesen az egyik legnagyobb kihívást jelentő és legnehezebb feladat a szövetséges haderők ennek megfelelő átalakítása. Bárhogyan is vélekednek ezzel kapcsolatban a NATO tagországok felelős, kompetens vezetői, egy biztos, ennek az átalakítási folyamatnak az alapját kell, hogy képezze egy modern, digitális, a kor technológiai- és technikai trendjeinek, színvonalának megfelelni képes haderő kialakítása, melynek megvalósítása elképzelhetetlen egy korszerű ismeretekkel felvértezett személyi állomány kiképzése, felkészítése nélkül. Ezen követelményeknek való minél gyorsabb és minél hatékonyabb megfelelés által lesznek csak képesek megfelelő módon reagálni az új típusú kihívásokra és fenyegetésekre, melyek a klasszikus hadszíntér helyett egyre inkább a digitális hadszíntéren öltenek testet.

FELHASZNÁLT IRODALOM

[1] BALOG F.-FEKETE Cs.-NÉMETH A.-NÉMETH J. L.: A hibrid hadviselés különös tekintettel a mobil kommunikációra; Hadmérnök X. 4. (2015) 127-137. o.

[2] SOMKUTI B.: A negyedik generációs hadviselés-az érdekérvényesítés új lehetőségei; Doktori (PhD) értekezés; Budapest 2012.

[3] Ált/57 Információs Műveletek doktrína 1. kiadás; A Magyar Honvédség Kiadványa 2014.

[4] HAIGH Zs.: A számítógép-hálózati hadviselés rendszere az információs műveletekben; Bólyai Szemle 15. 1. (2006) 54-73. o.

[5] SZTERNÁK Gy.: Gondolatok a hatásalapú- és a hálózatközpontú katonai műveletekről; Hadtudományi szemle 1. 3. (2008) 1-7. o.

[6] TÓTH A.: A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében; Doktori (PhD) értekezés; Budapest 2015.

[7] FARKAS T.: A válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében; Doktori (PhD) értekezés, Budapest 2010.

[8] TÁLAS P.-MOLNÁR F.: NATO-csúcstalálkozók Washingtontól Prágáig; ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (2006/6) 1-9. o.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

AZ ELEKTRONIKAI HADVISELÉS JELENE ÉS LEHETSÉGES JÖVŐJE

TODAY'S ELECTRONIC WARFARE AND ITS POSSIBLE FUTURE

KOVÁCS László

(ORCID: 0000-0002-6403-0650)

kovacs.laszlo@uni-nke.hu

Absztrakt

Az ukrajnai válságban és az azt övező fegyveres konfliktusban, valamint a szíriai háborúban az elektronikai hadviselés hagyományos értelmezése újra előtérbe került. Jelen tanulmány azt a kérdés vizsgálja, hogy melyek azok az elektronikai hadviselési elvek, eljárások és eszközök, amelyek egy 21. századi, de hagyományos fegyverekkel vívott konfliktusban hatékonyan alkalmazhatóak az egyre inkább kibertéri műveletek előretörése mellett.

Kulcsszavak: *elektronikai hadviselés, kiberhadviselés, Ukrajna, Szíria*

Abstract

The pragmatic use of Electronic Warfare has emerged again in the Ukrainian crisis and in the Syrian war. This study focuses on the tactics, techniques and procedures of Electronic Warfare in a 21th Century's military crisis where the parties use conventional weaponry beside the emerging of operations in the cyber sphere.

Keywords: *electronic warfare, cyber warfare, Ukraine, Syria*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.31.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.02.17.)

BEVEZETÉS

Az elektronikai hadviselés mind eljárásaiban, mind eszközeiben komoly fejlődésen ment keresztül története során. Mint minden hadviselési elem, így az elektronikai eszközök felfedésére, az azokkal szembeni ellentevékenységre, illetve a saját elektronikai eszközök és rendszerek védelmére alkalmas megoldások folyamatosan alkalmazkodtak a korszak aktuális technikai és eljárásbeli kihívásaihoz. Ezek a kihívások elsőként technikai válaszokat igényeltek, de mindezek mellett megjelentek azok a kérdések is, amelyek elsősorban az eljárások és műveleti megoldások területén bekövetkező változásokat jelentették. A hagyományos nagyméretű fegyveres összecsapások helyett (leszámítva az olyan műveleteket, mint Irak 1992, vagy 2003) az aszimmetrikus, vagy a 2010-es években a hibrid hadviselési elvekhez kellett, illetve a legutóbbi időben csak kellett volna alkalmazkodnia az elektronikai hadviselésnek is.

A hidegháborút követő időszakban azonban a biztonságpolitikai szakértők egyöntetű véleménye alapján elterjedt nézet szerint, a nagy, hagyományos fegyveres konfliktusok (háborúk) esélye minimális volt. A nehéz fegyverzetű, ebből következően nehezen mozgó, lassan reagáló, hagyományos fegyveres erők ideje leáldozni látszott. Ugyanakkor Irak, Afganisztán, vagy éppen Líbia némileg ellentmondott ezeknek a megállapításoknak, hiszen például a 2003-as Öböl-háborúban a szövetséges erők igen komoly hagyományos légi-, illetve szárazföldi fegyverzettel vettek részt. Ez a vélekedés, valamint a nyugati országok folyamatos védelmi kiadásainak csökkenő tendenciája összességében negatívan hatott az egyébként is méregdrága – egyes elemzések szerint a légierő fejlesztési kiadásaival összemérhető –, olyan elektronikai hadviselés eszközrendszerek fejlesztésére, amelyek a hagyományos háborús műveletekben lennének alkalmazhatóak. Ez alól talán csak a légierő egyes eszközei és rendszerei voltak kivételek, hiszen a repülőgépek (elektronikai) önvédelmi berendezései komoly fejlődésen mentek keresztül. Ennek persze nagyon is nyomós oka volt, mégpedig az, hogy a légierő alkalmazási területein megkövetelt a maximális védelem az elektromágneses spektrumban is. Összességében megállapítható, hogy a szárazföldi erők klasszikus elektronikai hadviselési képességei, illetve azok fejlesztése számos országban messze elmaradt az elvárható szinttől.[1]

Mindezeken túl, az elmúlt évtizedben a számítógépek és számítógép-hálózatok katonai műveletekben való elterjedése, valamint a polgári számítógép-hálózatok célpontként való megjelenése egyre többször és egyre nagyobb átfedést jelent az elektronikai hadviselés, valamint a kibertérben folyó műveletek között.

Maga az elektronikai hadviselés – főleg annak eszközei és eljárásai – a legszenzitívebb, legtitkosabb tényezők minden ország hadseregén belül. Az általános elvek azonban nem titkosak, sőt számos publikációt találunk az elektronikai hadviselésről évtizedek óta.

Jelen írás arra keresi a választ, hogy hol történt képesség csökkenés, és hol történt esetleg képesség növekedés az elektronikai hadviselés területén az elmúlt időkben. Ugyanakkor az elemzés nem kíván teljes és átfogó képet adni a területről, de néhány tényező felvillantásával bepillantást kíván engedni az egyébként meglehetősen szenzitív és minden ország által rendkívül titkosan kezelt elektronikai hadviselés néhány konkrét jellemzőjébe.

[1] Ez alól az egyik kivétel a rádió távvezérelt improvizált robbanóeszközök elleni védelemben elengedhetetlen zavaró eszközök fejlesztése volt.

AZ ELEKTRONIKAI HADVISELÉS JELLEMZŐI

Az elektronikai hadviselés összetevői és feladatai

Definíciószerű megfogalmazás szerint az „*elektronikai hadviselés: a műveleti (hadműveleti, harc-) támogatás fajtája. Azon tevékenységek összessége, amelyek az elektromágneses spektrum ellenség által történő felhasználásának meghatározására, felderítésére, csökkentésére vagy megakadályozására, illetve az elektromágneses energia és az irányított energia felhasználására, az elektromágneses spektrum saját célú felhasználására, valamint az ellenség vezetési és irányítási rendszerei támadásának támogatására, a saját csapatok védelmére irányulnak.*" [1]

Ez a meglehetősen bonyolult és hosszú meghatározás azonban nem jelent mást, mint az elektromágneses spektrumban működő elektronikai eszközök működésének felderítését, az így megszerzett adatokból az elektronikai eszközök helyére, együttműködéseikre következtetések levonását, valamint a kisugárzások lehallgatásából információk megszerzését, az elektronikai eszközök működésének akadályozását, illetve nyilvánvalóan a saját elektronikai eszközeink védelmét. Az elektronikai hadviselés legfontosabb tartománya az elektromágneses spektrum, és mivel elektronikai eszközöket a hadseregek minden tevékenységük során használnak, így az elektronikai hadviselés jelen van a szárazföldi csapatok, a légierő, valamint a haditengerészet műveleteiben is. [2]

Hazánkban az elektronikai hadviselés külön dedikált doktrínával rendelkezik, amely szerint e tevékenység fogalma: „*olyan hatás-alapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését."* [3]

A fogalmi meghatározásokból is kitűnik, hogy az elektronikai hadviselés három nagy területre osztható: elektronikai támogatásra (angol terminológiában: Electronic Support Measures – ESM), elektronikai ellentevékenységre (Electronic Counter Measures – ECM)[2] és elektronikai védelemre (Electronic Protection – EP)[3]. Ugyanakkor a NATO elektronikai hadviseléssel foglalkozó doktrínájához hasonlóan a hazai szabályozási környezet is területekre és funkciókra osztja az elektronikai hadviselést, amely elektronikai támadás, elektronikai védelem és elektronikai megfigyelés területeket, valamint elektronikai támogatási, elektronikai ellentevékenységi és elektronikai védelmi funkciókat különböztet meg. [3]

Mindezekből a meghatározásokból le lehet vezetni az elektronikai hadviselés konkrét és kézzelfogható feladatait. Az elektronikai támogatás feladata alapvetően az elektromágneses spektrumban történő veszélyjelzés, az ISTAR (Intelligence Surveillance Target Acquisition Reconnaissance – felderítés és célazonosítás) képességekhez való hozzájárulás, valamint a SIGINT (Signals Intelligence – rádióelektronikai felderítés) tevékenység támogatása. Az elektronikai ellentevékenység hadviselési dimenziók szerinti feladata alapvetően két részre osztható: légierő-, valamint szárazföldi feladatok[4]. A légierő tevékenysége során az elektronikai hadviselés többek között a repülőgépek önvédelmi elektronikai hadviselési feladatait, kötelékoltalmazást (zavarást), az ellenséges légvédelem lefogását (SEAD -

[2] Az elektronikai ellentevékenységet egyre többször, főleg az amerikai terminológiában elektronikai támadásnak (EA - Electronic Attack) hívják.

[3] Korábban az elektronikai védelmet elektronikai ellen-ellentevékenységnek (Electronic Counter-Counter Measures – ECCM) is nevezték.

[4] Természetesen ezek a dimenziók a haditengerészettel rendelkező országok esetében a tengeri dimenziót is jelentik.

Suppression on Enemy Air Defenses) valamint a szárazföldi (ide értve a légideszant, különleges műveleti, stb.) erők számára elektronikai támogatási feladatokat végez. [4] A szárazföldi feladatok során az elektronikai ellentevékenység feladatai lehetnek a szembenálló fél kommunikációs eszközeinek, radarjainak, vagy akár a navigációs eszközeinek zavarása vagy megtévesztése. Az elektronikai védelem feladata elsősorban a saját csapatok elektronikai eszközeinek a védelme, közvetlen vagy közvetett módon a csapatok oltalmazása, valamint az elmúlt időszakban kiemelt feladatként a vezeték nélküli távirányítással[5] működő improvizált robbanóeszközök zavarását (counter RC-IED).

Ezekből a feladatokból világosan látszik, hogy az elektronikai hadviselés rendkívül összetett, komplex feladatrendszerrel rendelkezik. Ezek a feladatok mindegyike hatalmas technikai eszközparkot feltételez úgy, hogy ezeknek a technikai eszközöknek és rendszereknek fejlettségben folyamatosan követniük kell a „másik oldal" technikai fejlődési trendjeit, hiszen anélkül rendkívül gyorsan devalválódnak, azaz korlátozottan vagy teljesen használhatatlanná válnak a saját oldali eszközök. Ennek megfelelően a terület tudományos igényű kutatása nélkülözhetetlen. Ezeket a kérdéseket természetesen hazánkban is kiemelt területként kezelik a tudományos kutatások és mind a hadtudományi mind a katonai műszaki kutatások egyik meghatározó irányaként definiálják. [5] [6]

Az elektronikai hadviselés a NATO szövetségi szintjén is jelen van. A NATO legfontosabb elektronikai hadviselési szerve a NATO Elektronikai Tanácsadó Testület (NATO Electronic Warfare Advisory Committee - NEWAC). Ez a szervezet felelős a NATO elektronikai hadviselési politikájának, doktrínájának, utasítási és ellenőrzési koncepcióinak kialakításáért, valamint az elektronikai hadviselési támogatás NATO-műveletekben való megjelenésének biztosításáért. [7]

Az elektronikai hadviselés története dióhéjban

Az elektronikai hadviselés, bár magával a hadviseléssel természetesen nem lehet egyidős, mégis viszonylag régen jelen van a fegyveres küzdelmekben. Amióta az első komolyabb elektronikai eszköz, nevezetesen a harctéri rádió megjelent a katonai műveletekben, azóta beszélhetünk annak felderítési, lehallgatási, később pedig zavarási igényéről.[6] A Marconi féle rádió volt az első olyan vezeték nélküli híradást megvalósító eszköz, amely forradalmasította a harctéri kommunikációt. Ugyanakkor az első elektronikai hadviselési elveknek megfelelő katonai tevékenység az 1905-ös japán-orosz háborúban jelent meg először.[7] [8]

Mind az 1. mind a 2. világháború hatalmas fejlődést hozott az elektronikai hadviselés területén. Az 1. világháborúban, majd a két háború közötti időszakban a rádiók lehallgatása, a kisugárzás helyének a meghatározása, valamint az üzenetek tartalmának a megfejtése volt a fő feladat[8].

---

[5] A vezeték nélküli távirányítású eszközök közül is elsősorban a rádióhullámok tartományában működő eszközök ellen lehet hatékony az elektronikai ellentevékenység.

[6] Ugyanakkor a vezeték nélküli kommunikáció megjelenése előtt a vezetékes híradást lehetővé tevő Morse távíró vonalak lehallgatása vagy akár annak rombolása volt az első, klasszikus „elektronikai hadviselési" eljárás. *„A közlemények egyszerű vezetékre való csatlakoztatással lehallgathatóvá váltak, amin a különféle rejtjelezési módszerek, kódtáblázatok és más eljárások némiképpen segíthettek. Egyszerűen megvalósítható volt a megtévesztő közlemények bejuttatása a hálózatba, hiszen az adókészülék helyére egy ugyanolyan készülékkel rácsatlakozva fizikailag helyettesíteni lehetett az igazi felhasználókat. A vezetékek elvágásával, a távíróoszlopok kidöntésével a vonalak fizikailag is könnyen támadhatóak voltak."* [9]

[7] A japán-orosz háborúban jelent meg először a szembenálló fél rádióinak lehallgatási igénye. [8] [10]

[8] Itt meg kell említeni Pokorny Hermann nevét, aki az Osztrák-Magyar Monarchia tisztjeként kiváló orosz nyelvtudása miatt először az orosz rádió-táviratok feldolgozását, majd később – 1916-ig – a rádiólehallgatás megszervezését is feladatul kapta. [11]

A 2. világháborúban az elektronikai eszközök, mint például a repülőgép-fedélzeti rádiók és radarok egyre gyorsuló ütemű elterjedése az elektronikai hadviselési eszközök és erők fejlődését is magával hozta.

Ezt követően a helyi háborúk – koreai háború, az arab-izraeli háborúk, a vietnámi háború, később az Öbölháború 1991-ben – a harctéren megszerzett tapasztalatokkal támasztották alá és erősítették meg azokat a véleményeket, melyek szerint az elektronikai hadviselés elengedhetetlen része a korszerű fegyveres küzdelemnek.

Nem túlzás azt állítani, hogy ezt követően az elektronikai eszközök robbanásszerűen nyertek teret a 20. század közepén a hadviselésben. Minden ország fegyveres ereje egyre több és egyre komplexebb elektronikai eszközt alkalmazott és alkalmaz ma is a vezetés és irányításra, a felderítésre és információszerzésre, a fegyverrendszerek vezérlésére, a kommunikációra, az adatátvitelre, vagy a navigációra. Mindezek mellett olyan eszközök jelentek meg, mint a pilóta nélküli repülőgépek (angol terminológiában: Unmanned Aerial Vehicle – UAV), vagy a szárazföldi robotok (angol terminológiában: Unmanned Ground Robot – UGR), amelyek már nem csak „egyszerű" felderítésre, hanem a fedélzeti fegyvereiknek köszönhetően nagyon gyakran csapásmérésre is alkalmasak. Ezek az eszközök feladataik ellátása során, bár már sokszor önálló döntéshozatalra is képesek, de mégis egyelőre alapvetően elektronikai eszközökkel történő irányításuk a döntő.

Ezek a változások az elektronikai hadviselés képességeinek fejlődését és alapvető változását igényelték, mind eszközrendszer, mind eljárások tekintetében. Ez a hidegháború befejeződéséig nyomon követhető is volt. Ezt követően azonban – ahogy arra később részletesen szó lesz –, az alapvető biztonságpolitikai enyhülés, valamint az olyan egyéb kihívásoknak – pl. terrorizmus, aszimmetrikus fenyegetések, stb. – köszönhetően nagyon sok ország fegyveres ereje nem fordított kellő figyelmet az elektronikai hadviselési eszközök, rendszerek és képességek fejlesztésére. Ez természetesen nem minden területre igaz, de pl. a szárazföldi csapatok elektronikai hadviselési képességeinek sokszor még a szinten tartása is elmaradt.

ELEKTRONIKAI HADVISELÉSI KÉPESSÉGEK

Elektronikai hadviselési képességvesztés: Egyesült Államok

A hidegháború utáni időszakban, azaz az elmúlt több mint 25 évben a nyugati nagyhatalmak közül sokan – és ezzel párhuzamosan a kisebb országok[9] is – mintha elfelejtették volna azt a tényt, hogy mind a hadsereg vezetése, mind az ahhoz elengedhetetlen kommunikáció és felderítés elektronikai eszközökre épülnek, és ezek az elektronikai eszközök, hasonlatosan a számítógépekhez, illetve a számítógép-hálózatokhoz sérülékenyek. Ráadásul ez a tény ma már egy bizonyos szintű függőséget is jelent az elektronikai rendszerekkel szemben. Ugyanakkor az ezeket lehallgatni, az ezekbe az elektronikai eszközökbe beavatkozni képes, vagy az ezeket zavarni tudó – elektronikai hadviselési – eszközöket és rendszereket nem, vagy csak alig fejlesztették.[10]

Ezt támasztják alá azok a nagyon súlyos megállapítások, amelyeket az Amerikai Egyesült Államok Védelmi Minisztériumának úgynevezett Védelmi Tudományos Testülete (Defense

[9] Az elmúlt időben hazai kutatók is utaltak erre a problémára Magyarország vonatkozásában. [12] [13]

[10] Ez természetesen nem jelenti azt, hogy ne történt volna elektronikai hadviselési eszközfejlesztés. De maga az elektronikai hadviselési képesség, amellyel egy-egy ország rendelkezik messze alul maradt attól a képességtől, amelyet a hidegháború utáni technikai és technológiai fejlődés megkövetelt, illetve prognosztizálható lett volna.

Science Board of Department of Defense - DSB)[11] 2015 nyarán született jelentésében tett. A DSB jelentése, amelyben a 21. század katonai tevékenységeit a komplex elektromágneses környezetben vizsgálják, leszögezi, hogy az Egyesült Államok nagyon komoly hiányosságokkal küzd az elektronikai hadviselés területén.[12] A tanulmány három fő okra vezeti vissza ezen hiányosságok meglétét, illetve azok kialakulását:

- a hidegháborút követő 25 évben az USA elhanyagolta az elektronikai hadviselés területét, amely elsősorban az elektromágneses spektrumban rejlő veszélyek negligálása miatt következett be;
- a második ok abban keresendő, hogy a fejlett szoftver vezérelt elektronikai eszközök kutatás-fejlesztése, azok előállítása már nem csak az USA privilégiuma, számos feltörekvő ország képes ma már ilyen high-tech elektronikai eszköz és rendszer gyártására;
- világossá vált, hogy a potenciális ellenfelek, amelyek folyamatosan figyelték az Egyesült Államok harctéri elektronikai dominanciáját, olyan eszközöket és rendszereket állítottak hadrendbe, amelyek ezt a dominanciát megtörik és ezzel az USA számára a lépéselőny megszűnik.

Mindezek alapján az elemzés három olyan területre mutat rá, amelyek elengedhetetlenül szükségesek ahhoz, hogy a feltárt hiányosságok megszüntethetőek legyenek. Az első: szükség van az elektromágneses spektrum dinamikus használatára. Ez jelenleg egy olyan technikai kihívás, amely megnehezíti a helyzetismeret kialakítását, a spektrum hatékony kihasználását, valamint a szembenálló fél spektrumhasználatának akadályozását. A második: el kell érni az elektronikai rendszerek közel valós idejű adaptációját. Az a sebesség, amellyel a korszerű digitális elektronikára épülő technológia a működési üzemmódjai között vált drámai módon megnőtt. Ehhez alkalmazkodnia kell az USA elektronikai hadviselési eszközeinek is. A harmadik terület: az Egyesült Államok nem engedheti meg magának, hogy alárendelt szerepet játsszon az elektronikai hadviselés bármely területéről legyen is szó. Ennek érdekében olyan nagyarányú elektronikai fejlesztések szükségesek, amelyeket nem, vagy csak nehezen tudnak követni a potenciális vetélytársak. Ez egyrészről technológiai fölényt eredményez, másrészt a harctéren elektronikai fölényt fog jelenteni. [15]

Ezeket a megállapításokat támasztja alá Laurie Buckhout, az Egyesült Államok Szárazföldi Erők korábbi elektronikai hadviselési főnökének nyilatkozata: "*A legnagyobb probléma az, hogy évtizedek óta nem harcoltunk úgy, hogy a kommunikációnkat zavarták volna, így nem tudjuk, mit kell tenni ilyen helyzetben. Ráadásul nem csak az eljárásaink hiányoznak ilyen esetekre, hanem kiképzésünk sincs a zavar alatt álló kommunikációs környezetben való tevékenységre*." [16]

Ugyanebből a nyilatkozatból az is világosan kiderül, hogy az Egyesült Államok szárazföldi hadereje (US Army) az elektronikai ellentevékenység (zavarás) terén is hiányosságokkal

[11] A DSB-t 1956-ban hozta létre az amerikai Védelmi Minisztérium azzal a céllal, hogy a Testület révén olyan tudományosan magalapozott tanácsokat biztosítsanak a fegyveres erők számára, amelyek alapján azok megfelelnek a változó világrend egyre nagyobb kihívást jelentő rakéta technológiájával, az információs hadviseléssel, a biológiai, kémiai és nukleáris fegyverekkel, valamint egyéb hidegháború fenyegetésekkel szemben. A testület munkájára napjainkban ugyanolyan szükség van, mint korábban, hiszen a fegyveres erőkkel szembeni kihívások a hidegháború elmúltával nem, hogy csökkentek volna, hanem éppen ellenkezőleg: drasztikusan nőttek. [14]

[12] A tanulmány több területen vizsgálta az elektronikai hadviselés műveleti támogatásban betöltött szerepét és jellemzőit: műholdas kommunikáció, harcászati kommunikáció, precíziós navigáció és felderítés. Ezt a négy tényezőt megvizsgálták a legjellemzőbb három műveleti formában: harcászati légiharc, haditengerészeti védelem, valamint szárazföldi harcászati műveletek. [15]

küzd. "*Nagyszerű rádióelektronikai felderítésünk*[13] *van, egész nap tudunk lehallgatást végezni, de egytized részben sem tudjuk őket zavarni, összehasonlítva azzal, amit ők*[14] *tudnak. Nagyon védtelenek a hálózataink az ő támadásaikkal szemben.*" [16]

Számos elemzés ezeknek a hiányosságoknak a kialakulását paradox módon éppen Irakra és Afganisztánra vezeti vissza. 1999 óta, azaz az afganisztáni műveletek megkezdése óta, az USA szárazföldi ereje alapvetően az itt, valamint később Irakban tapasztalt kihívásokra koncentrált. Ennek megfelelően a US Army jelenlegi elektronikai hadviselési eszközeinek, illetve képességeinek a jelentős része a gyorsreagálású képességek biztosítása érdekében született. [17] Ezek a képességek pedig mind minőségben, mind (eszköz) mennyiségben nagyon messze vannak attól, amelyet egy hagyományos háborúban a szárazföldi erőknek teljesíteniük kellene.

Az afganisztáni és iraki kihívásokra adandó válaszok ad-hoc fejlesztésekhez és beszerzésekhez vezettek. Többek között olyan eszközök beszerzése történt meg, mint pl. a C-12-es repülőgépé, amely az úgynevezett CEASAR[15] (Communications Electronic Attack with Surveillance and Reconnaissance – kommunikációs zavaró és felderítő) függeszthető elektronikai hadviselési konténert alkalmazza. Ugyanakkor ez a konténer is alapvetően a felkelők elleni műveletek céljából, a gyorsreagálású képességek biztosítása érdekében került alkalmazásra.

Hasonló fejlesztés a GATOR (Ground Auto Targeting Observation/Reactive – földi automatikus célmeghatározó/zavaró) elektronikai hadviselési rendszer. (1. kép) Ez szintén abból az igényből származtatható, hogy nagyon gyors iránymérés és helymeghatározás szükséges az RCIED-k elleni tevékenységek esetén. [17] Ugyanakkor a rendszer ennél szélesebb körű felhasználással rendelkezik – hiszen a zavaró képesség a szembenálló fél kommunikációs rendszerei ellen is alkalmazható lenne –, de a korlátozott számban rendelkezésre álló berendezések miatt a felhasználhatóság itt is erősen limitált. [16]

---

[13] Rádióelektronikai felderítés: SIGINT (Signals Intelligence): alapvetően passzív eljárásokra épülő, az elektromágnes spektrumban működő felderítési fajta. Két részre osztható: COMINT (Communication Intelligence), azaz kommunikációs felderítés (magyar terminológiában: rádiófelderítés), valamint ELINT (Electronic Intelligence), azaz nem kommunikációs felderítés (magyar terminológiában rádiótechnikai felderítés). [2]

[14] Az orosz fél.

[15] A CEASAR a C-12 Beechcraft King Air repülőgépre, mint hordozóra kifejlesztett elektronikai felderítő és zavaró konténer. Fő feladata a felkelők elleni műveletekben (counter-insurgencies operations) a kommunikáció felfedése és zavarása. A fejlesztést alapvetően az US Army gyorsreagálású erői (U.S. Army Quick Reaction Capability Effort) számára készítették. [18] A C-12-es repülőgép, mint hordozó ugyanakkor számos más feladatban is szerepet kapott már korábban is (pl. futárgép, felderítőgép, stb.), és erre a típusra épült RC-12N Guardrail Common Sensor típusnévvel gyártott SIGINT repülőgép, amely az afganisztáni műveletekben is részt vett 2015-ig. [19]

A CEASAR alapjaira épült a szintén a Raytheon cég által gyártott NERO (Networked Electronic Warfare, Remotely Operated – távirányítású, hálózati elektronikai hadviselési) rendszer, amely alapvetően a US Army MQ-1C Gray Eagle típusú pilóta nélküli repülőgépéhez készült konténer. Fő feladata a kommunikációs felderítés és zavarás. Ez a konténer nagy előrelépés a fejlesztésben, hiszen egy (közvetlen) kezelőt nem igénylő, és így pilóta nélküli repülőgépen is alkalmazható rendszert jelent. [20]

1. kép. A GATOR elektronikai hadviselési rendszer. [21]

Mindezekhez a technikai kérdésekhez hozzájárul az elektronikai hadviselési szakemberek helyzete is. Az egyébként is kevés létszámú elektronikai hadviselési tiszt és altiszt alapvetően elméleti képzésben részesült, ráadásul békebeosztásuk sokszor más, párhuzamos feladat ellátását is jelentette, így gyakorlatban, harci körülmények között is alkalmazható szakmai ismereteik erősen korlátozottak. [16]

A problémák és a hiányosságok felismerése megtörtént. Ennek megfelelően az olyan elektronikai hadviselési rendszerek, mint pl. a CEASAR, NERO, GATOR további fejlesztése mellett újabb elképzelések is születtek. Ilyen például az MFEW (Multifunctional Electronic Warfare – multifunkcionális elektronikai hadviselés) fejlesztése. Az MFEW olyan elektronikai ellentevékenységi képességekkel fog rendelkezni, amely a mobil telefonok zavarásától, a GPS rendszerek zavarásán át, a harctéri rádiórendszerek zavarásáig széles spektrumot fed le[16]. Ugyanakkor ennek rendszerbeállítása csak 2023-ban, a teljes műveleti képesség elérése pedig csak 2027-re várható. [16] [21]

[16] Az eredeti elképzelések szerint az MFEW nem csak elektronikai támadó (zavarási) hanem elektronikai támogatási (ESM) képességekkel is rendelkezik, valamint mind szárazföldi, mind légi komponense is van. A rendszer hálózatos kialakítású, valamint valós idejű át- és újraprogramozási (új feladatszabási) lehetőségekkel is bír. [21]

Elektronikai hadviselési képesség növekedés: Oroszország

Az ukrajnai konfliktus során az Egyesült Államok katonai kiképzői folyamatosan segítik az ukrán hadsereg felkészítését és kiképzését. E tevékenység során az amerikai fél is nagyon sok hasznos tapasztalatra tesz szert, mert számos olyan ukrán csapat vesz részt a kiképzéseken, akik korábban Kelet-Ukrajnában az orosz barát felkelők elleni műveletekben harcoltak.

Így az ukrán hadsereg harcban szerzett tapasztalatait az USA feldolgozza, amely során elemzi többek között az orosz elektronikai hadviselési eszközök fajtáit, működési filozófiájukat, képességeiket, valamint ezen eszközök hatótávolságát. Mindezt segíti az is, hogy bár az ukrán fél elektronikai hadviselési képességei messze alul múlják az orosz félét, mégis a korábban a Szovjetunió részeként kiképzést kapott idősebb katona generáció még – részben – emlékszik azokra az elvekre és eljárásokra, ahogy az orosz fél elektronikai hadviselése felépül és működik.

Az így kapott eredmények arra engednek következtetni, hogy az orosz fél komoly fejlesztéseket hajtott végre a fegyveres erejének modernizációja terén, amely során az elektronikai hadviselési képességek is hatalmas fejlődést mutatnak. Az orosz hadsereg megtartotta, sőt fejlesztette a hagyományos elektronikai hadviselési erőit, ezen belül kiemelt figyelmet fordítottak a rádiózavaró, navigációs zavaró, illetve egyéb szárazföldi elektronikai eszközök, valamint rádiólokációs zavaró képességeik fejlesztésére.

A fentiekből levonható további következtetés, hogy – hasonlóan az amerikai haderőhöz – az ukrán hadsereg elektronikai zavarás esetén történő feladatellátásra való felkészülése teljesen hiányzik. Ez visszavezethető az ukrán hadsereg ilyen típusú kiképzésének, szimulációs gyakorlatainak, valamint az ilyen helyzetek kezelésére megfelelő eljárásrend kidolgozásának és begyakorlásának a teljes hiányára. Ez azzal a következménnyel jár, hogy a nagyarányú elektronikai zavarás a vezetés (C2 – Command and Control) megbontását eredményezi, azaz végső soron a masszív elektronikai hadviselés vezetési fölényt eredményez.[17] A katonai vezetés technikai eszközeinek elektronikai zavarás miatti kiesését – akár átmenetileg is – polgári kommunikációs eszközökkel, pl. GSM telefonokkal történő helyettesítése, pótlása szintén nehéz feladat, mert a területen a polgári rendszerek, így a GSM rendszerek zavarása is folyik. Egy másik – nem kevésbé veszélyes – következmény, hogy a tüzérségi felderítő radarok zavarása miatt nem lehetséges a tüzérségi tűz kiváltási helyének a meghatározása, így nem lehetséges pontos válasz-tűzcsapást vezetni a szembenálló fél tüzérségi eszközeire. [16] [22]

A fentieken túl az elektronikai hadviselési eszközök nem kinetikus energiájú „fegyverek”, hatásaik nem látszanak a médiában, így például Ukrajna keleti részében is gyakorlatilag láthatatlanul, vagy csak az avatott szemek számára látható módon képesek tevékenységet folytatni. Ez óriási előny az orosz félnek, hiszen anélkül képes vezetési fölényt biztosítani, hogy a jelenlétére utaló áruló technikai eszközök explicit módon megjelennének a hírekben. „*Az ukrán erők félelmetes orosz elektronikai hadviselési képességekkel szemben küzdöttek, amely elemzők szerint még az amerikai szárazföldi erők számára is megdöbbentő. Az amerikai hadsereg is használ zavarást a felkelők kommunikációja ellen a levegőből és a*

[17] Az elektronikai hadviselés az információs műveletek (IO – Information Operations) egyik alap összetevője (katonai képességként értelmezett módon). Az információs műveletek kiemelt célja az információ fölény, és ezen keresztül a vezetési fölény kivívása. Ennek értelmében megállapítható, hogy az orosz fél az információs műveletek területén is kiemelkedő sikereket ér el azzal, hogy az elektronikai hadviselés révén vezetési fölényt biztosít a maga számára. A vezetési fölény többek között a harcban azért is bír nagy fontossággal, mert birtoklója számára biztosítja a kezdeményezés, valamint a harctéren való dominancia előnyét.

szárazföldről egyaránt, de ez csak korlátozottan áll rendelkezésre, és a zavaró rendszerek fejlesztése nem is várható 2023-ig." [16]

Mindezek alapján jelen írás néhány olyan orosz elektronikai hadviselési eszközt kíván bemutatni, amelyek fejlesztése az elmúlt évtizedben történt, és amelyek szerepet kaptak Kelet-Ukrajnában, vagy akár Szíriában.

Az első ilyen eszköz egy új elektronikai hadviselési helikopter: az Mi-8MTPR-1, amely fedélzetén a Rychag-AV nevű zavaró állomás helyezkedik el. Az állomás fő rendeltetése a radarok zavarása, valamint radar rávezetéssel rendelkező föld-levegő és levegő-levegő rakéták elleni tevékenység, alapvetően azok zavarása[18]. Az eszközt a moszkvai központú Kret[19] nevű orosz, rádióelektronikai ipari vállalati egyesülés gyártja és forgalmazza[20].

A Mi-8 helikopterre szerelt zavaró rendszer látható a Kret cég hivatalos weblapján közzétett képen (2. kép). Ezen azonban valószínűsíthetően csak a mikrohullámú tartomány egyik antennája látszik a törzs hátsó harmadában.

2. kép. A Mi-8MTPR1 helikopterre szerelt Rychag-AV a Kret hivatalos fényképén [23]

Ugyanakkor amennyiben a fedélzeti rendszer kommunikációs zavaró képességgel is rendelkezik, akkor az szükségessé teszi URH antennák alkalmazását is. Ez a teljes antenna rendszer a 3. sz. képen látható módon nézhet ki (egy másik típus esetében).

[18] A Kret cég hivatalos képein és filmjein az is látható, hogy az állomás valószínűleg infravörös hullámtartományban is képes zavarásra.

[19] Kret: http://oblik.msk.ru/en/

[20] A Kret cég 2015-ben 9 db Moszkva-1 elektronikai felderítő állomást, 10 db Rychag-AV helikopter fedélzeti zavaró állomást, 8 db Krasukha-2 és 15 Krasukha-4 elektronikai hadviselési komplexumot, valamint 20 Rtut-BM elektronikai felderítő és zavaró állomást szállított az orosz hadseregnek. [24]

3. kép. Az orosz légierő Mi-8 típusú helikopterre szerelt elektronikai hadviselési eszköze. [25]

Érdemes megjegyezni, hogy a korábban a Varsói Szerződés több tagországában, így Magyarországon is rendszeresített Mi-17PP elektronikai hadviselési helikopter, amely hasonló feladatokkal és hasonló rendeltetéssel bírt (URH zavarás), antenna rendszerének elhelyezése és kialakítása sok hasonlóságot mutatott a 3. számú képen látható eszközzel. (4. kép)

4. kép. Az 1990-es évek közepéig a Magyar Honvédségben (korábban Magyar Néphadseregben) rendszerbe állított Mi-17PP elektronikai hadviselési[21] helikopter. [26]

[21] Az akkori terminológia szerint az elektronikai hadviselés rádióelektronikai harc kifejezésként volt használatos.

A Rychag-AV zavaró állomásról – csakúgy, mint az többi orosz elektronikai hadviselési eszközről – meglehetősen kevés, és csak általános technikai információ érhető el nyílt és nem utolsósorban megbízható forrásból. Egyes források a Rychag-AV eszközt az 1970-es években gyártott Szmalta zavaró állomás utódjának tartják. Az elől 100 km-es zavarási hatótávolsággal rendelkezett, ezzel szemben ennél az állomásnál ezt már több száz kilométerre teszik[22]. Fázisrács-vezérelt antennájának köszönhetően egyszerre több célpont zavarását is el tudja végezni. Magát a zavaró állomást nem csak helikopter fedélzetére lehet elhelyezni, hanem akár haditengerészeti vagy szárazföldi platformokra is. A gyors jelfeldolgozásnak, illetve a fedélzeti adatbázisnak köszönhetően önvédelmi elektronikai hadviselési feladatokat is képes ellátni az állomás. [27]

Vladimir Mikheev a Kret vállalat egyik vezetőségi tanácsadójának nyilatkozata alapján ezt a rendszert 2017-ben a Rychag-AVM zavaró rendszer fogja követni, amely még nagyobb hatótávolsággal és megnövelt funkcionalitással fog rendelkezni. [24]

A következő bemutatni kívánt orosz elektronikai hadviselési eszköz, illetve eszközök a Kraszuha-2/4 elektronikai hadviselési komplexumok. A két egymást kiegészítő változatban gyártott és rendszerbe állított elektronikai hadviselési komplexum az 1RL269 Kraszuha-2 és az 1RL257 Kraszuha-4 típus nevet viselik. Ezeket az eszközöket a szintén a Kret vállalathoz tartozó Bryansk Electromechanical Plant nevű cég gyártja. (5. és 6. kép). [28]

5. kép. Kraszuha-2 elektronikai hadviselési komplexum. [29]

A Kraszuha-2/4 alapvető feladata az AWACS (Airborne Warning and Control System – fedélzeti korai előrejelző és vezetési rendszer) felderítése és zavarása 250-300 km-es hatótávolságig. A komplexumok további elektronikai ellentevékenységi feladatai lehetnek az olyan fedélzeti radarok zavarása, mint például az amerikai Joint STARS[23] repülőgépen lévő

[22] A Rychag-AV zavarási hatótávolságát a Kret cég hivatalos bemutató filmje földi célok ellen 50-200 km-ben, a légi célok ellen 300 km-ben, az egyidejűleg lefogható célok számát pedig maximum 8 db-ban adja meg. [30]

[23] A Joint STARS (E-8C) repülőgép fedélzetén elhelyezett SAR radarjával mind a légierő, mind a szárazföldi csapatok számára biztosít felderítési adatokat, valamint harcvezetési rendszerének köszönhetően célinformációkkal támogatja a támadó műveleteket. [31]

SAR (Synthetic Aperture Radar – szintetikus apertúrájú radar), vagy akár a pilóta nélküli repülőgépek zavarása (pl.: RQ-4 Global Hawk, MQ-1 Predator). A rendszer korlátozott mértékben, de képes műholdak zavarására (pl.: az USA Lacrosse és Onyx típusú műholdjai) is, valamint alkalmas radar rávezetésű rakéták zavarására és hamis cél imitációra. A komplexum olyan nagy fontosságú célok védelmét is feladatul kaphatja, mint pl. az Iskander (9K720 Iskander SRBM).[24]

6. kép. A Kraszuha-4 elektronikai hadviselési komplexum. [32]

Szintén érdemes megjegyezni, hogy a Kraszuha-4 állomás antennarendszere kísértetiesen hasonlít a korábban a Varsói Szerződés számos tagországában – így hazánkban is – az 1980-as években rendszeresített SZPN-30 repülőgép-fedélzeti rádiólokátor zavaró állomás antennáihoz[25].

[24] Iskander (9K720 Iskander SRBM): ballisztikus rakéta. (NATO kódneve SS-26 Stone) Alapvető rendeltetése a harcászati csapásmérés a nagyértékű és nagyfontosságú célokra. Hatótávolsága 500 km. Ebből következően ez a komplexum elsődleges cél lehet egy adott fegyveres konfliktusban, így a védelme kiemelt fontosságú. [33]

[25] Ugyanakkor a gyártó hivatalos videóin jól látszik, hogy az állomás elektronikai eszközei a kor színvonalának megfelelő, számítógép vezérlésű eszközök.

7. kép. Az SZPN-30 repülőgép-fedélzeti rádiólokátor zavaró komplexum. [34]

Az SZPN-30 fedélzeti rádiólokátor zavaró állomás fő feladata a 3 cm-es hullámtartományban működő repülőgép-fedélzeti radarok zavarása zajzavarral, illetve válasz-impulzus zavarral volt. Az állomás egyszerre 5 cél lefogására volt képes közel 300 km-es hatótávolságig.

Az orosz katonai intervenció Szíriában szükségszerűen a korszerű orosz haditechnikai eszközök bevetését is igényelte. Ennek egyik példája többek között a Kraszuha-4 alkalmazása a szíriai háborúban. Erről tanúskodik a szíriai Latakia mellett telepített állomásról készített kép. (8. kép).

A fenti eszközökön kívül is számos olyan elektronikai hadviselési berendezést fejlesztett vagy modernizált az orosz haderő[26], amelyek a hagyományos fegyveres konfliktusokban sikerrel alkalmazhatóak, de mindezek mellett rendelkeznek az olyan képességekkel is mint a korábban említett RC-IED-k elleni elektronikai ellentevékenység, illetve védelem. Ilyen eszköz például az Infauna K1Sh1 UNSh-12 elektronikai felderítő és zavaró állomás, amely egy BTR-80-as alvázon került elhelyezésre, vagy például a Tigr-M MKTK REI PP állomás, amely Tigr típusú terepjáró személygépkocsi alvázára szerelt Leer-2 típusú iránymérő és zavaró berendezést jelent. [36]

További hasonló elektronikai hadviselési berendezés az MTLBU[27] alvázra épített Borisoglebsk-2 nevű RH és URH frekvenciatartományban működő elektronikai felderítő és zavaró állomás. Ez az új állomás annak az elektronikai hadviselési fejlesztési programnak a

[26] Az orosz haderő modernizációja az említetteken kívül is számos haditechnikai eszközt érintett. Ilyenek például a korszerű páncélozott harcjárművek irányított rakéták elleni védelmét lehetővé tevő ellentevékenységi rendszerek (többek között a Drozd-2, Sthora-1, Arena, stb.) [39]

[27] Az MTLBU oroszul МТ–ЛБу – многоцелевой транспортёр легкобронированный универсальный, azaz többcélú könnyű páncélozott szállító járművek korábban a Magyar Néphadseregben, illetve a Magyar Honvédségben is rendszeresítve voltak. Többek között az R-330P zavaró állomás is ilyen hordozó eszközön került elhelyezésre.

része, amely az orosz hadsereg gépesített lövész dandárjainak ilyen irányú képességei növelését célozta 2014-től kezdődően. [37]

8. kép. Kraszuha-4 komplexum a szíriai Latakia[28] közelében. [35]

Meg kell jegyezni, hogy ezek az állomások – azaz az Infauna, a Tigr-M MKTK REI PP, illetve a Borisoglebsk-2 is – mindegyike harcászati szintű, nagy páncélvédettséggel rendelkező, és nagy terepjáró képességekkel bíró olyan eszköz, amelyek elsősorban gépesített lövész egységek és alegységek, illetve légideszant csapatok[29] támogatására kerülnek alkalmazásra. Ebből egyértelműen levezethető, hogy alkalmazásuk – rendeltetésüknek megfelelően –, leginkább hagyományos háborúban a legvalószínűbb. Ez pedig intő jel kell, hogy legyen a számunkra.

AZ ELEKTRONIKAI HADVISELÉS LEHETSÉGES JÖVŐJE

Az eddig bemutatottak alapján jól látszik, hogy az elektronikai hadviselésnek a sikeres harc megvívása érdekében eszközeiben és eljárásaiban is alkalmazkodnia kell (a fentiek alapján számos országban csak kellene) azokhoz a körülményekhez, amelyek a korszerű fegyveres küzdelmet jellemzik.

Az elektronikai hadviselés a 20. század kezdetétől a 21. század kezdetéig az elektromágneses spektrum minél hatékonyabb sajátoldali felhasználását, valamint a szembenálló fél spektrum használatának az akadályozását jelentette. A 21. század elejére azonban már az elektromágneses spektrumban is megjelent egy sor olyan technikai kihívás, amely komoly dilemma elé állította az elektronikai hadviselési szakembereket. Egyrészt a hatalmas ütemben fejlődő digitális technika és az általuk biztosított új kommunikációs

[28] Latakia városa mellett van az orosz légierő Szíriába települt erőinek egyik legfontosabb légibázisa. Ennek megfelelően természetesen szükséges a bázis, illetve az onnan felszálló repülőgépek védelme. Így a Kraszuha-4 telepítése nem meglepő. A zavaró állomás mellett Sz-300 légvédelmi rakétakomplexumokat is telepítettek a légibázis, illetve az innen nem messze lévő tengeri kikötő védelmi érdekében. [38]

[29] A légideszant csapatok orosz hivatalos megnevezése: ВДВ – Воздушно-десантные войска.

módok[30] jelentik ezt a kihívást, másrészt a korábban említett biztonságpolitikai változásokból eredő kihívások is megmaradtak, sőt fokozódtak. Az olyan fegyveres konfliktusokon kívül, mint például Irak vagy Afganisztán, az orosz-ukrán válság rávilágított, hogy a hagyományos háborús eszközkészletre továbbra is, de modernizált, a 21. század technikai színvonalát elérni képes módon, de szükség van, hiszen sok helyen (pl.: Oroszország, Kína) nem csak megmaradtak a hagyományos fegyverzettel rendelkező hadseregek, hanem ezek tudatos és tervszerű modernizációja miatt hatalmas potenciált jelentenek. Ennek megfelelően a jövőben az elektronikai hadviselésnek mind eszközeiben, mind eljárásaiban nem csak a gyorsreagálású képességek támogatására, nem csak békekikényszerítő és béketámogató műveletekben[31], hanem nagy intenzitású háborús műveletekre is készen kell állnia.

Mindezeken túl a látható és nem látható fény tartományában, technikai eszközökkel végzett információszerzési tevékenységek és ezzel együtt a képi felderítés (Imagery Intelligence – IMINT) hatalmas fejlődése is nyomon követhető az elmúlt 10-15 évben, amely egyrészt a képi felderítő szenzorok hordozóinak (pl. UAV-knek), másrészt maguknak a képalkotó szenzoroknak és eljárásoknak a fejlődése miatt következett be. Az elektronikai hadviselésnek pedig egyrészt erre a spektrumtartományra (a látható és nem látható fény tartományára), a képi felderítő eszközök adatátviteli, adatfeldolgozó, kommunikációs és vezérlő rendszerei elleni tevékenységre, valamint az ezeket az eszközöket hordozó berendezések (sok esetben az említett UAV-k) elleni harcra is fel kell készülnie.

Ugyanakkor a 20. század végén, a 21. század elején számos más, egészen új kihívás is jelen van. Az egyik ilyen kihívást a kibertér és az abban folyó tevékenységek és műveletek jelentik. A kibertér, valamint az elektromágneses spektrum és a kibertéri elektromágneses műveletek meghatározásai, valamint azok összefüggéseinek a feltárása megtörtént az elmúlt években. [40] [41] [42]

A kibertérben megjelenő új technológiák, valamint az új, egyre inkább mindennapos eljárások és szolgáltatások összessége az elektronikai hadviselés számára is több alternatív, de mindenképpen párhuzamos jövőt feltételez. Így a kibertéri elektronikai hadviselés szükségessége már ma jelen van a hadviselésben.[44] Az elektromágneses spektrum és a kibertér átfedése azt is jelenti, hogy az elektronikai hadviselésnek komoly szerepe lesz a számítógép-hálózati műveletekben[32] (pl. annak felderítési, információszerzési fázisában), mert ahogy korábban a katonai vezetés és irányítás a rádiókommunikációt, úgy ma a számítógép-hálózatokat használja alap képességként. Ennek megfelelően, ha a számítógép-hálózatok adatforgalma vezeték nélküli, azaz a rádióhullámok tartományára alapul (akár csak részben is), akkor abba az elektronikai hadviselés – megfelelő technikai eszközök megléte

[30] Olyan megoldások jelentek meg a digitális technikának köszönhetően, mint pl. a kiterjesztett spektrumú adásmódok, vagy például az SDR (Software Defined Radio – Szoftverrádió) technológia.

[31] Meg kell jegyezni, hogy az ilyen műveletekben megjelenő kihívások is komplexek. Új, nem hagyományos kommunikációs és vezetési eszközök jelennek meg az ilyen területeken (pl. a felkelők elleni műveletek), amely eszközök nem katonai, hanem polgári eszközöket, vagy azok bizonyos modifikációit jelentik. Ugyanakkor a nem hagyományos katonai műveletekben megjelennek a nem katonai ECM eszközök is (pl.: Irán által gyártott eszközök), amelyre az egyik legjobb példa Izrael 2006-os libanoni beavatkozása során történt. Ekkor a libanoni erők (elsősorban a Hezbollah), olyan elektronikai hadviselési eszközöket alkalmazott az izraeli hadsereggel szemben, amelyeket nagy valószínűséggel Iránban gyártottak. [43] Ebből levonhatjuk azt a következtetést, amelyet korábban az USA elektronikai hadviselési képességeinél említett DSB szintén elemzései eredményeként jelenített meg, hogy ma már nem csak fejlett országok privilégiuma a legkorszerűbb elektronikai hadviselési eszközök fejlesztése és gyártása.

[32] Számítógép-hálózati műveletek (Computer Network Operations CNO), amelyek az elektronikai hadviseléshez hasonlóan szintén az információs műveletek részét képezik, fő feladatuk a szembenálló fél számítógép-hálózatainak felderítése, onnan információk kinyerése, vagy akár annak működésbeli korlátozása, mindeközben a saját ilyen hálózatok működésének a biztosítása, védelme.

esetén – be tud avatkozni, onnan adatokat tud kinyerni, vagy akár működésében tudja azt akadályozni (pl. zavarással).

A kibertéri elektronikai hadviselési képességek mellett szükséges megőrizni és fejleszteni a hagyományos hadviselési elveknek megfelelő elektronikai hadviselési erőket és eszközöket, valamint az ehhez a képességekhez tartozó eljárásokat[33].[44]

Ennek megfelelően leegyszerűsítve azt is mondhatjuk, hogy az elektronikai hadviselés számára a célok hasonlóak, mint korábban, csak a tartomány (domain) bővült.

KÖVETKEZTETÉSEK

Az elektronikai hadviselés a hagyományos hadviselés összetevői közül napjaink és prognosztizálhatóan a jövő fegyveres konfliktusainak és háborúinak egyik meghatározó tényezője.

Az elmúlt évtizedek, valamint a közelmúlt háborúiban szerzett tapasztalatok arra engednek következtetni, hogy az elektromágneses spektrumban folyó küzdelem a hadviselés elengedhetetlen része. A vezetési fölény megszerzéséhez és így a siker kivívásához pedig szükség van az információs fölényre. Az ukrán konfliktus különösen élesen rávilágított arra a tényre, hogy napjainkban, legyen szó bár aszimmetrikus, vagy hibrid hadviselésről, a javarészt a hagyományos fizikai dimenzióban vívott fegyveres küzdelem lényeges összetevője az elektronikai hadviselés.

A nyugati országok, köztük az Egyesült Államok azonban leépítették, vagy nem az elvárható mértékben fejlesztették a szárazföldi erőik elektronikai hadviselési képességeit. Így az komoly képességvesztést eredményez számukra.

Az ukrajnai konfliktusban, illetve a szíriai háborúban megjelenő – az elmúlt másfél évtizedben hatalmas technikai fejlesztésen és korszerűsítéseken átesett – orosz elektronikai hadviselési eszközök és rendszerek, illetve az ezek által megtestesített képességek figyelmeztető jelzések a számunkra.

A jövő elektronikai hadviselése kettősséget mutat: megmaradnak a hagyományos fegyveres küzdelem során a szárazföldi erőket támogató, ott a vezetési fölény kialakításához nagymértékben hozzájáruló korszerű elektronikai hadviselési eszközök és rendszerek szükségessége, valamint a másik oldalról a kibertér elektromágneses műveleteire alkalmas elektronikai hadviselés eszközei, erői és képességei szintén jelen lesznek a hadseregek arzenáljaiban.

FELHASZNÁLT IRODALOM

[1] Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás. MH Vezetési és Doktrinális Központ kiadványa, 2012.

[2] HAIG Zs., KOVÁCS L., VÁNYA L., VASS S., NÉMETH A.(szerk.): Elektronikai hadviselés. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[3] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína, 2. kiadás, 2015.

[4] KOVÁCS L.: A légerő elektronikai hadviselése a terrorizmus elleni harcban. Repüléstudományi Közlemények. 20/1. 2008.

[33] Mindezeket ki kell egészíteni a korszerű elektronikai hadviselési elvek szerinti kiképzéssel és felkészítéssel, valamint a felmerülő új technikai igényeket tudományos alapossággal kell megjeleníteni és transzformálni az ipar (haditechnikai ipar) számára, ahhoz, hogy valóban megfelelő – a kihívásokra választ adni képes – elektronikai hadviselési eszközök kerüljenek gyártásra.

[5] BODA J., BOLDIZSÁR G., KOVÁCS L., OROSZ Z., PADÁNYI J., RESPERGER I., SZENES Z.: Fókusz és együttműködés: A hadtudomány kutatási feladatai. Honvédségi Szemle 144/3. 2016.

[6] BLESZITY J., FÖLDI L., HAIG Zs., NEMESLAKI A., RESTÁS Á.: Műszaki kutatások és hatékony kormányzás. Hadmérnök 11/3. 2016.

[7] Electronic Warfare; http://www.nato.int/cps/en/natohq/topics_80906.htm [1] (letöltve: 2016.12.18.)

[8] GORDON, D. E.: Electronic Warfare: Element of Strategy and Multiplier of Combat Power, Pergamon Press, New York, 1981.

[9] HAIG Zs., KOVÁCS L., MUNK S., VÁNYA L.: Az infokommunikációs technológia hatása a hadtudományokra. Nemzeti Közszolgálati Egyetem, Budapest, 2013.

[10] BOKOR I., PAPP I., VÁRHEGYI I.: Elektronikus hadviselés. Műszaki Könyvkiadó, Budapest 1992.

[11] BAKONYI P. (szerk.): Pokorny Hermann vezérezredes: Emlékeim. A láthatatlan hírszerző. Hadtörténelmi Levéltári Kiadványok. http://mek.oszk.hu/02000/02095/html/ (letöltve: 2017.01.05.)

[12] BALOGH P.: Az elektronikai támogatás és a SIGINT helyzete a Magyar Honvédségben. Felderítő Szemle 2013:(1), 2013.

[13] HORVÁTH J.: Elektronikai hadviselés a Magyar Honvédségben. Hadmérnök, 9/1. 2014. http://hadmernok.hu/141_17_horvathj.pdf (letöltve: 2017.01.05.)

[14] Defense Science Board: About DSB: http://www.acq.osd.mil/dsb/index.htm (letöltve: 2017.01.05.)

[15] Report of the Defense Science Board: Study on 21st Century Military Operations in a Complex Electromagnetic Environment, Washington D.C., 2015. http://www.acq.osd.mil/dsb/reports/DSB_SS13--EW_Study.pdf (letöltve: 2017.01.05.)

[16] GOULD, J.: Electronic Warfare: What US Army Can Learn From Ukraine, Defense News, 2015. augusztus 2. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/ (letöltve: 2017.01.05.)

[17] ACKERMAN R. K.: Consolidation Is the Course for Army Electronic Warfare. Signal, 2013. április 1. http://www.afcea.org/content/?q=consolidation-%E2%80%A8the-course-army-%E2%80%A8electronic-warfare (letöltve: 2017.01.14.)

[18] NSWC Crane Electronic Warfare Center Fact Sheet. http://www.navsea.navy.mil/Portals/103/Documents/NSWC_Crane/EW%20Air%20Fact%20Sheet%20(no%20mark).pdf (letöltve: 2017.01.05.)

[19] United States Army Acquisiton Support Center: Guardrail Common Sensor (GR/CS). http://asc.army.mil/web/portfolio-item/guardrail-common-sensor-grcs/ (letöltve: 2017.01.05.)

[20] Raytheon News Release: Raytheon delivers electronic jamming capability for Gray Eagle UAS. http://investor.raytheon.com/phoenix.zhtml?c=84193&p=irol-newsArticle&ID=1819171 (letöltve: 2017.01.05.)

[21] Program Executive Office Intelligence Electronic Warfare & Sensors: Electronic Warfare & Cyber, Multi-Function Electronic Warfare – MFEW https://peoiews.army.mil/electronic-warfare-cyber (letöltve: 2017.01.05.)

[22] MCLEARY, P.: Russia's Winning the Electronic War. Foreign Policy, 2015. október 21. http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/ (letöltve: 2017.01.05.)

[23] Kret News Release: http://oblik.msk.ru/en/news_and_media/ (letöltve: 2017.01.05.)

[24] Kret News Release: http://oblik.msk.ru/en/news/10246/ (letöltve: 2017.01.05.)

[25] VASILESCU, V.: Sistemul de bruiaj rusesc Richag-AV vs drona americana RQ-170 Sentinel. Ziarul de Garda, 2015. április 15. http://www.ziaruldegarda.ro/sistemul-de-bruiaj-rusesc-richag-av-vs-drona-americana-rq-170-sentinel/ (letöltve: 2017.01.05.)

[26] ILLÉS Z.: Mi-8 Hip, a forgószárnyas mindenes. http://www.hunaf.hu/rovatok/fegyverek/mi8/hip/ (letöltve: 2017.01.19.)

[27] Deagel: Rychag-AV. http://www.deagel.com/Ship-Protection-Systems/Richag-AV_a003124001.aspx (letöltve: 2017.01.05.)

[28] Kret: Kraszuha. http://www.kret.com/en/product/12/ (letöltve: 2015.11.14.)

[29] Defense Blog: New Russian Electronic Warfare System «Krasukha» at TVM-2014. http://defence-blog.com/news/new-russian-electronic-warfare-system-krasukha-at-tvm-2014.html (letöltve: 2017.01.05.)

[30] КРЭТ передал армии секретное оружие https://www.youtube.com/watch?v=wdzI1iK4xxI (letöltve: 2017.01.05.)

[31] US Air Force: Popular Fact Sheets: E-8C Joint Stars. http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104507/e-8c-joint-stars.aspx (letöltve: 2017.01.05.)

[32] Pakistan Defense: Russia Displays Innovative Asymmetric Counter Stealth Systems at MAKS-2015. http://defence.pk/threads/russia-displays-innovative-asymmetric-counter-stealth-systems-at-maks-2015.395964/ (letöltve: 2017.01.05.)

[33] GlobalSecurity.org: 9K720 Iskander-M (SS-26 Stone) http://www.globalsecurity.org/wmd/world/russia/ss-26.htm (letöltve: 2017.01.05.)

[34] Valka.cz: http://en.valka.cz/topic/view/38028/SOV-SPN-30-prostredek-REB (letöltve: 2017.01.05.)

[35] The Boresight Air Power Focus. http://theboresight.blogspot.hu/2016/07/the-end-of-primacy-russian-federation.html (letöltve: 2017.01.05.)

[36] Army Recognition: Army in the world - Russia Electronic Warfare units. http://www.armyrecognition.com/armies_in_the_world_analysis_focus/russian_airborn

e_troops_are_ready_to_use_electronic_warfare_ew_vehicles_infauna_and_leer-2_0410124.html (letöltve: 2017.01.05.)

[37] Kret News Release: http://rostec.ru/en/news/4516361 (letöltve: 2017.01.05.)

[38] BBC News: Syria conflict: Russia sends missile system to Tartus base. 2016. október 4. http://www.bbc.com/news/world-middle-east-37557138 (letöltve: 2017.01.05.)

[39] VÁNYA L.: Российские средства и способы радиоэлектронной борьбы в интересах защиты бронетанковых машин. Hadmérnök. 9/2 (2014). http://hadmernok.hu/142_32_vanyal.pdf (letöltve: 2017.01.05.)

[40] HAIG Zs.: Információ - társadalom – biztonság. NKE Szolgáltató Kft., Budapest, 2015.

[41] FM 3-38: Cyber Electromagnetic Activities. Headquarters Department of Army, 2014. https://fas.org/irp/doddir/army/fm3-38.pdf (letöltve: 2017.01.05.)

[42] POMERLEAU. M.: DoD could declare the spectrum a domain of warfare. Defense Systems, 2015. december 10. https://defensesystems.com/articles/2015/12/10/dod-could-declare-spectrum-an-operational-domain.aspx?s=ds_141215 (letöltve: 2017.01.05.)

[43] ESHEL, D.: Hezbollah's Intelligence War: Assessment of the Second Lebanon, Defense Update, 2007. http://defense-update.com/analysis/lebanon_war_1.htm (letöltve: 2017.01.05.)

[44] VÁNYA L.: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. Doktori (PhD) értekezés. ZMNE, Budapest, 2003. http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf (letöltve: 2017.01.05.)

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

E-KÖZIGAZGATÁSI RENDSZEREK INTEROPERABILITÁSÁNAK ÉRETTSÉGE

INTEROPERABILITY MATURITY OF E-GOVERNMENT SYSTEMS

LAPOSA Tamás

(ORCID: 0000-0002-4809-5796)

tamas.laposa@gmai.com

Absztrakt

Az Európai Bizottság az informatikai rendszerek együttműködésre való képességét, azaz interoperabilitását, az európai elektronikus közszolgáltatások jövőbeli fejlesztésének egyik kritikus tényezőjeként kezeli. Az interoperabilitási képesség szervezetenként és rendszerenként heterogén, különböző (jogi, szervezeti, technológiai és szemantikai) tényezők határozzák meg, minősége ún. érettségi modellek segítségével mérhető.

A határon átnyúló európai elektronikus közszolgáltatások interoperabilitásának értékelése és fejlesztésének támogatása céljából a Bizottság megalkotta az Interoperability Maturity Model-t (IMM). Az IMM specifikus érettségi modell, azonban a transznacionális közszolgáltatások összetettsége miatt az elektronikus szolgáltatások interoperabilitásának értékelése különböző nézőpontú modellekkel javasolt.

Jelen tanulmány célja az érettségi modellek elméleti hátterének áttekintése, valamint a tudományos diskurzusban elérhető több interoperabilitási modell IMM-mel történő összevetése, az elektronikus közszolgáltatások elemzési eszköztárának bővítése és esetleges további specifikus modellek kidolgozásának elősegítése érdekében.

Kulcsszavak: *interoperabilitás, érettség modell, elektronikus közszolgáltatások*

Abstract

The European Commission emphasizes that interoperability (i.e. the ability to exchange data and to enable information sharing) of information systems is a critical success factor of the development of electronic public services. The interoperability of different systems can be very heterogeneous and it is defined by a range of legal, organizational, technological and semantic factors. Its quality can be best measured by so-called maturity models.

The European Commission elaborated the Interoperability Maturity Model (IMM) to support the development and the evaluation of the interoperability of cross-border electronic public services. However IMM is tailored to the above domain, the complexity of cross-border services requires a multidimensional approach to evaluate the interoperability of electronic services.

This paper has two main aims. First, to review the theoretical background of maturity models. Second to compare the IMM with other maturity models used in the pertinent literature in order to methodologically support the evaluation of electronic public services and to pave the way for the elaboration of further specific models.

Keywords: *interoperability, maturity models, electronic public services*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.15.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.18.

BEVEZETÉS

Az Európai Bizottság felismerte, hogy az informatikai rendszerek együttműködésre való képessége, azaz interoperabilitása és a digitális közszolgáltatások bevezetése kritikus fontossággal bír a közszolgáltatások modernizálása és hatékonysága szempontjából. A következtetések alapján a Bizottság útjára indította az ISA2 (Interoperability Solutions for Public Administrations2) programot és célul tűzte ki az európai elektronikus közszolgáltatások interoperabilitásának előmozdítását és támogatását.

Mindemellett az információs technológia fejlődése, az ügyviteli folyamatok digitalizálása, az elektronikus közszolgáltatások körének bővülése növeli a lehetséges kapcsolódási pontok számát, s így az interoperabilitás jelentőségét.

Az informatikai rendszerek interoperabilitási képessége nem homogén, az együttműködési képességek minősége alapján az interoperabilitás különböző szintjei határozhatók meg. Ennek mérésére különböző ún. érettségi modellek állnak rendelkezésünkre. Az ISA program keretében a Bizottság kidolgozta az Interoperability Maturity Model-t (IMM), melynek célja az elektronikus közszolgáltatások interoperabilitási érettségének értékelése, valamint a kívánt képességek és minőségi szint eléréséhez szükséges támpontok meghatározásának támogatása. Az IMM segíti a szolgáltatás nyújtóját a szolgáltatás minőségének javításában, a költségek csökkentésében és az érintett rendszerek hatékony integrálásában. [1]

Az IMM a határon átnyúló elektronikus közszolgáltatások érettségének javítására fókuszál, azonban e szolgáltatások komplexitása miatt, az érettség vizsgálata több nézőpontból ajánlott, így további érettségi modellek áttekintése javasolt, hogy az IMM mellett megfelelő alternatív modellek legyenek alkalmazhatóak. Jelen tanulmány célja ezen eltérő szemléletű modellek módszertani összehasonlítása, különbségeik, hasonlóságaik elemzése, segítve az elektronikus közszolgáltatások elemzési eszköztárának bővítését, valami esetlegesen újabb specifikus modellek megalkotását.

AZ ÉRETTSÉGI MODELLEK MEGALKOTÁSÁNAK MÓDSZERTANA

A Carnegie Mellon Egyetem által alkotott definíció szerint*: „Az érettségi modell mutatók, attribútumok, karakterisztikák és sémák olyan készletét jelenti, amely segíti a vizsgált szervezet, ágazat fejlődésének és teljesítményének felmérését*." [2; 3.o.]

Az érettségi modellek lehetővé teszik egy szervezet működésének, folyamatainak és alkalmazott módszereinek értékelését, valamely világosan definiált referenciaérték (jó gyakorlat, szabvány, az adott ágazat meghatározó módszertanai) használatával. Segítségükkel felmérhető a szervezet aktuális állapota, meghatározhatók képességei, valamint a modellek támogatják a kívánt változások, tervezését, megvalósítását.

A modellek szabványos mérési módszereivel a szervezet meghatározhatja jelenbeli helyzetét és a jövőbeni céljait. A módszert az egyes szervezeti egységek is használhatják teljesítménymérési összemérésként, különösen akkor, ha az egyes részlegek hasonló funkciójú tevékenységeket végeznek. A modellben alkalmazott jó gyakorlatok felhasználhatók a teljesítményproblémák orvoslását célzó tervek kidolgozásához is.

Tágabb értelemben véve, az érettségi modellek segítik a szervezetek (piaci, ágazati, iparági) pozícióinak meghatározását és mutatóik más szervezetekkel való összevetését. Más megközelítésben, a szervezetek teljesítményének értékelésén keresztül a modellek lehetővé teszik az ágazat teljesítményének mérését, egy ún. ágazati teljesítményprofil megalkotását, így a modellek az ágazati teljesítmény javításának katalizátoraként használhatók. A profilalkotás segítheti az ágazati problémák hatékonyabb, közösségi szintű kezelését is. [2; 6.o.]

A modellek fő típusai

Az érettségi modellek hozzájárulnak egy közös ágazati nyelv kialakulásához, egységes fogalmi gondolkodást és kommunikációt biztosítanak, ezzel segítve a tervezhetőbb ágazati teljesítmény elérését.

Az érettségi modellek használata a képességek és folyamatok fejlesztésének fontos eszköze, a modellek alapvetően az alábbiak szerint csoportosíthatók: fejlődési modellek, képességi modellek, hibrid modellek.

A *fejlődési érettségi modellek* egy jellegzetes tulajdonság, mutató, vagy attribútum fejlődését mérik, ahol a szintek közti elmozdulások a vizsgált vonások érettségének növekedését fejezik ki. Rendszerint független modellek, melyek a vizsgált tulajdonságra, a fejlődés nyomvonalára összpontosítanak és nem a szervezeti érettség általános modellezésére. E modellekben, a szintek elnevezése jellegzetesen az adott tulajdonság egyes fejlődési szakaszaihoz kötődik.

A *képességi érettségi modellek* fókusza összetettebb, a vizsgálat tárgyát valamely szervezeti képesség képezi, mely különböző minták, folyamatok mentén valósul meg. Tágabb értelemben véve a szervezeti képességek vizsgálata a szervezeti kultúra érettségét tükrözi. A szintek itt a szervezet érettségét mérik a vizsgált folyamatok tekintetében. E modelleket gyakran nevezik „folyamatmodelleknek" is, s általános jellegük miatt, rendszerint több területen is alkalmazhatók.

A *hibrid érettségi modellek* ötvözik a fejlődési és képességi modellek jellegzetességeit. A modellek specifikus területekre fókuszálnak, azonban az érettség vizsgálatának fő szempontját az ágazati szabványok és jó gyakorlatok szervezeti képességekkel való összevetése képezi. A hibrid modellek viszonylag könnyen alkalmazhatók, jól használhatóak az érettségi szintlépést célzó fejlesztési tervek meghatározásához. [2; 7.-8..o.]

A modellek fő alkotóelemei

Az eltérő modellalkotási megközelítések ellenére, a modellek közös strukturális alapokra épülnek, melyek összekapcsolják az elérni kívánt szervezeti célokat, az ágazati szabványokat, a szervezeti képességeket, valamint a fejlesztés tervezett irányait. A modellek strukturális alkotóelemei a következők:

Az érettségi modellek legjellegzetesebb építőelemei a kitűzött célok által meghatározott fejlődési skálák mentén elhelyezkedő *érettségi szintek*, melyek között az elmozdulás mindig mérhető viszonyítási pontokhoz köthető. Mindez segíti a kiinduló állapot felmérését, a kívánt állapot meghatározását, s az annak eléréséhez szükséges attribútumok azonosítását. A modell típusától függően, a szintek fejlődési fokozatokat, kívánt képességeket, vagy további attribútumokat reprezentálhatnak.

A *célterületek* olyan osztályozási eszközök, melyek segítik a modell attribútumainak a vizsgálat szempontjából fontos tényezők szerinti csoportosítását az egyes szinteken belül. [2]

Az *attribútumok* a modellek elemi építőkövei, melyek modellen belüli helyzetét a célterületek és szintek határozzák meg. A modellek által vizsgált tényezők elemzése és érettségi szintek szerint történő besorolása az attribútumokon keresztül történik. Jellemzően szakértői ismereteken, szabványokon alapszanak, s általában mutatók, jó gyakorlatok, jellegcsoportok formájában jelennek meg.

A modellekkel kapcsolatos egyik legfontosabb elvárás, hogy a szintek közti elmozdulás mérhető viszonyítási pontokhoz köthető legyen. A *mérés módszerének* gyakorlatban kipróbáltnak, megalapozottnak és empirikus adatokon nyugvónak kell lennie.

A mérések elvégzése jellemzően pontozási és becslési módszerekkel történik. Használatuk lehet formális, informális, szakértő által végzett, vagy önbevallásos. A méréshez szükséges adatgyűjtés lehet valamely bevett mérési módszer eredménye, vagy akár kérdőíves felmérésen is alapulhat. A mérési eljárás összetettségét és szigorúságát a vizsgálat céljai, a vizsgált terület

sajátosságai határozzák meg.

Az érettségi modellek a szervezetek összehasonlítása mellett szervezetfejlesztési céllal is alkalmazhatóak. Számos modell tartalmaz olyan módszereket, melyek a helyzetfelmérést, a *fejlődési irányvonalak* meghatározását, valamint a kívánt változások tervezését és megvalósítását támogatják. [2; 8.-9.o.]

INTEROPERABILITÁSI ÉRETTSÉGI MODELLEK

Az érettségi modellek felhasználásának egyik speciális területe az interoperabilitási képesség vizsgálata. Ehhez elsőként tisztázni szükséges az interoperabilitás definícióját. Tekintettel arra, hogy a tanulmány célja a modellek összevetésének tapasztalatainak hasznosítása az elektronikus közszolgáltatások terén, így az *Európai Interoperabilitási Keretrendszerben (European Interoperability Framework – EIF)* található fogalom-meghatározást idézem.

A dokumentum szerint: „*Az európai közszolgáltatások vonatkozásában az interoperabilitás az a képesség, mely révén az egymástól eltérő szerkezetű, különböző szervezetek együtt tudnak működni kölcsönösen előnyös, konszenzuson alapuló, közös célok érdekében, ami magában foglalja a szervezetek egyedi munkafolyamatait követő, saját adatátviteli IKT-rendszereiken keresztül bonyolított ismeret- és információátadást is.*” [3; 3.o.]

Az EIF szerint az interoperabilitás különböző rétegei (*jogi, szervezeti, szemantikai, műszaki*) azonosíthatók ily módon az interoperabilitás is különböző nézőpontokból vizsgálható. Az EIF alapvetéseiből kiindulva, az Európai Bizottság elkészítette az *Interoperability Maturity Model-t (IMM)*, az elektronikus közszolgáltatások interoperabilitási érettségének értékelése céljából.

Az IMM jelen tanulmányban öt, a tudományos irodalomban elérhető, további modellel (*Information System Interoperability Maturity Model, Smart Grid Interoperability Maturity Model, LISI Interoperability Maturity Model, Governmenet Interoperability Maturity Model, Organisational Interoperability Maturity Model*) kerül összevetésre. A szelekció elsődleges szempontja olyan modellek kiválasztása volt, melyek lehetővé teszik az elektronikus közszolgáltatások interoperabilitásának több szempontú elemzését, így különböző szakterületek (*katonaság, közszolgálat, rendszerfejlesztés*), eltérő célú és típusú modelljei kerültek a mintába.

A továbbiakban a hivatkozott modellek ismertetése következik a következő fejezetben elvégzendő összehasonlító elemzés szempontjai mentén. Terjedelmi szempontból a modellek nem kerülnek minden alkotóelem mentén összevetésre, az elemzés elsődlegesen a modellalkotás céljaira, a modellek attribútumaira, szintjeire és azok tartalmára fókuszál. A szintek tartalmának precízebb megragadhatósága érdekében, az elnevezések angol eredetije is feltüntetésre kerül.

Interoperability Maturity Model (IMM; Interoperabilitási Érettségi Modell)

Az IMM célja, egy olyan módszertani útmutató biztosítása, mely segíti az európai elektronikus közszolgáltatások interoperabilitásának értékelését és iránymutatást ad az érettség szintjének növeléséhez, folyamatos fejlesztéséhez.

Az IMM elsődleges célcsoportját a szolgáltatásgazdák képezik, akiknek biztosítani kell az elektronikus közszolgáltatások interoperabilitását. [1; 3.o.]

Az IMM vizsgálati célja, hogy az adott közszolgáltatást nyújtó szervezet, milyen mértékben képes más szervezetekkel való interakciókra az EIF-ben meghatározott interoperabilitás definíció tartalmát figyelembe véve. Ekképpen a modell a külső szervezetekkel való interakciók mentén, valamint szervezeti, technikai, szemantikai és jogi tényezők szerinti jó gyakorlatok alapján értékeli az interoperabilitási érettségét. A modellben szereplő attribútumok a következők:

- *Szolgáltatás-nyújtás tényezői*: a végső felhasználók felé biztosított szolgáltatás fő összetevői (szolgáltatási csatorna, platformfüggőség, adatok újrahasznosítása, többnyelvűség, kereszthivatkozások, szolgáltatás-katalógus)
- *Szolgáltatás igénybevétel tényezői*: rendszerek közti szolgáltatás-igénybevétel és újrafelhasználás összetevői (igénybe vett külső szolgáltatások, igénybe vétel módja, szolgáltatás újrahasznosítása, feldolgozás módja, lekérdezési mechanizmusok, közös protokollok, publikus infrastruktúra használata, szemantikai egyezés, kivételkezelés, tanúsítás, specifikálás folyamata).
- *Szolgáltatás-menedzsment tényezői*: a külső interakciók és a szolgáltatásnyújtás folyamatának biztosítása (költség-haszon elemzés, nyújtott szolgáltatások száma, közbeszerzési előírások, automatizáció mértéke, státuszkövetés, eljárásrendek, folyamat-fejlesztési szabványok, architektúrális keretrendszer, architektúrális rugalmasság, specifikálás folyamata). [4; 5.-26.o.]

A modell az ágazati jó gyakorlatok szemszögéből közelíti meg az érettség vizsgálatát. Az IMM, a bevált modellalkotási gyakorlatot követve öt szintet állapít meg a szolgáltatások érettségnek besorolására. Az IMM szintjei a következők:

- *1 – Eseti (Ad hoc):* korlátozott interoperabilitás, a szolgáltatás csekély számú eleme rendelkezik interoperabilitási képességgel.
- *2 – Alkalmi (Opportunistic):* mérsékelt interoperabilitás, a szolgáltatás kialakítása során ágazati jó gyakorlatok alkalmanként kerülnek felhasználásra.
- *3 – Lényegi (Essential):* lényegi interoperabilitás, a szolgáltatás lényegi elemei ágazati jó gyakorlatokra épülnek.
- *4 – Fenntartható (Sustainable):* jó minőségű interoperabilitás, a releváns jó gyakorlatok teljes köre alkalmazásra kerül.
- *5 – Hézagmentes (Seamess):* mintaszerű interoperabilitás, a szolgáltatás ágazati jó gyakorlatként szolgál más szolgáltatásgazdák számára. [1; 5.o.]

Smart Grid Interoperability Maturity Model (SGIMM; Smart Grid Interoperabilitási Érettségi Modell)

Az SGIMM megalkotásának célja egy objektív módszer kidolgozása, mely biztosítja az egymással kapcsolatba lépő szervezetek interoperabilitási érettségének értékelését. A modell pillanatfelvételt ad az interoperabilitási képesség aktuális állapotáról, mely segít a rendszerek közti interoperabilitás várható eredményességének megítélésében. Kiemelendő, hogy az SGIMM elsődlegesen helyzetértékelésre fókuszál, s nem célja a jövőbeni fejlődési irányok tervezése.

Az SGIMM statikus modell, az interoperabilitás követelményeinek jelenbeli teljesítésére fókuszál, s azt részletes elemzés alá veti, a következő szempontok szerint.

- *Hatékonyság növelése*: az elektronikus szolgáltatásnyújtás hatékonyságának és teljesítményének javítása.
- *Interoperabilitási érettség*: a modell különlegessége, hogy egyik attribútumaként egy másik modell (GridWise Interoperability Framework) érettségi skálát is felhasználja. A skála 8-szintű és a technikai, szemantikai és szervezeti interoperabilitás minőségét méri.
- *Technikai architektúra és design*: a technikai interoperabilitás támogatása a folyamatok menedzsmentje, nyomon követése és a szolgáltatásnyújtás terén.
- *Üzleti architektúra és design*: szervezeti interoperabilitás támogatása az üzleti alkalmazásokban.

- *Interoperabilitás szervezeti támogatása*: bevett iparági szabványok és csereszabatos megoldások alkalmazása a külső rendszerekkel való kommunikációban érintett rendszerkomponensek tekintetében.
- *Biztonság*: a biztonsági szempontok magas szintű érvényesítése az interfészek és a kommunikációban érintett komponensek tekintetében.
- *Konzekvens tervezés*: az interoperabilitás biztosítása az iparági szabványok és protokollok korábbi verzióit használó alkalmazások esetében, a rendszerbeli interfészek kompatibilitásának biztosítása a külső interfészekkel.
- *Kritikus funkciók szeparációja*: kommunikációs protokollok és üzleti logika elkülönítése, jogosultságkezelés és adatkezelés szeparációja. [5; 1.-3.o.]

Az SGIMM célja az interoperabilitási képesség részletes feltárása, ennek érdekében a fenti attribútumok alapján a következő szinteket határozza meg:

- *1 - Nem átjárható (Non-interoperable):* a rendszerkomponensek többsége egyedi, integrációjuk jelentős tesztre szabást igényel. A fejlesztések során ritkán követnek ágazati szabványokat, vagy következetlenül teszik azt.
- *2 - Kezdetleges (Initial):* a rendszerek összekapcsolása magas erőforrás igényű integrációs projektek lévén lehetséges. A projektek a működés fenntarthatóságára (támogatás, frissítések) nem fókuszálnak. A megoldások jellemzően belső, nem piaci szabványokon alapszanak, belső hitelesítésükre gyakran nincsenek belső folyamatok, külső tanúsítás ritkán történik.
- *3 - Erősödő (Emerging):* a rendszerek összekapcsolása kisebb terjedelmű integrációs projektekkel megoldható, a projektek kiterjednek a működés fenntarthatóságára, azonban a tervezett folyamatok közepes hatásfokúak. A piaci szabványok használata gyakori, de a belső hitelesítési eljárások sokszor hiányoznak. Esetenként a megoldás tanúsítatása is megtörténik.
- *4 – Minősített (Certified):* az integrációs projektek iránti igény csekély, a rendszerkapcsolatok a meglévő interoperabilitás mellett jól megvalósíthatók, a fenntarthatóság erőteljes hangsúlyt kap. A komponensek kialakítása ismert szabványokon alapszik, külsőleg tanúsított, de a tanúsítás nem mindig éri el az elvárt szintet.
- *5 – Kompatibilis (Plug and play):* az új komponensek, technológiák rendszerbe illesztése nem igényel speciális szakértelmet és nem erőforrás-intenzív. A rendszerkapcsolatok robusztus támogatással és frissítési eljárásokkal támogatottan kerülnek kiépítésre, melyet követően a tanulságok és jó gyakorlatok megosztására is sor kerül az ágazati szabványok minőségének további javítása érdekében. [5; 4.-5.o.]

Levels of Information System Interoperability Maturity Model (LISI; Információs Rendszerek Szintjei Interoperabilitási Érettségi Modell)

A LISI katonai modell, melynek célja a közös hadműveletek irányításának és levezénylésének metodológiai támogatása. E hadműveletek gyakran előre nem tervezhető módon, korábban egymással kapcsolatban nem álló és speciális rendszereket használó szervezetek között jönnek létre, így az interoperabilitási képesség e műveletek megvalósításának egyik kulcstényezőjévé válik.

A LISI célja, a műveleti együttműködéshez szükséges interoperabilitási igények azonosítása, az információs rendszerek képességeinek felmérése és a szervezetek támogatása interoperabilitási képességeik fejlesztésében.

- *Folyamatok*: az attribútum az információs rendszerek fejlesztésével, integrációjával kapcsolatos belső iránymutatásokat (működés, funkcionalitás, architektúra) és szervezeti kontrollokat öleli fel.
- *Alkalmazás*: az információs rendszer fejlesztésnek célja, a rendszer kialakításának funkcionális követelményei.
- *Infrastruktúra*: a rendszerek architektúrája, a rendszerek közti kapcsolat kialakításának technológiai háttere.
- *Adat*: a rendszerben feldolgozott információkkal kapcsolatos követelmények, szintaktika és szemantika.

A LISI a következő érettségi szinteket határozza meg:

- *0 – Elszigetelt (Isolated):* izolált rendszerek, melyek nem képesek elektronikus adatcserére. Az adatok kinyerése manuálisan történik.
- *1 - Kapcsolódó (Connected):* a rendszerek képesek az elektronikus adatcsere egyszerű formáira, ami jellemzően munkaállomások között történik és homogén formátumok (egyszerű szöveg, hang, e-mail) átadását jelenti.
- *2 - Funkcionális (Functional):* magasabb komplexitású adatok cseréje helyi hálózatok között. Heterogén adattípusok cseréje közös logikai adatmodell alapján. [
- *3 – Szakterület-alapú (Domain-based):* adatcsere azonos funkciójú szervezetek, független alkalmazások között, szakterületi-alapú (fizikai és logikai) adatmodellek alapján. A rendszerek képesek adatbázisok közti közvetlen műveletek végrehajtására és üzleti szabályok alkalmazására.
- *4 – Vállalati szintű (Enterprise-based):* az adatcsere globálisan, különböző szakterületek adatbázisai között, egységes adatmodell alapján. A közös adatbázisok és a kölcsönösen elérhető alkalmazások az együttműködés magasabb szintjét biztosítják. [6; 20.-35.o.]

Organisational Interoperability Maturity Model (OIMM; Szervezeti Interoperabilitási Érettségi Modell)

Az OIMM szintén katonai modell, célja a LISI-hez hasonlóan a közös hadműveletek megavalósításának módszertani támogatása. E hadműveletek megindításában kiemelten fontos szerepet játszik a résztvevők közötti kooperáció minősége és hatékonysága. A modell a LISI-et veszi alapul, azonban annak folyamat és adatkezelési attribútumait bontja ki részletesen, célja a szervezet interoperabilitási képességének vizsgálata, értékelése és a kooperáció támogatása.

Az OIMM a szervezeti interoperabilitás hatékonyságát vizsgálja, attribútumai az együttműködés mielőbbi és hézagmentes kialakításának tényezőire koncentrálnak:

- *Felkészültség*: a szervezet felkészültsége az együttműködésre (eljárások, tapasztalatok, gyakorlat).
- *Ismeret*: tudás- és információ-megosztás, információ-felhasználás a szervezeten belül.
- *Irányítási stílus:* a szervezetek vezetési és irányítási stílusa (döntéshozatal, felelősségek meghatározása).
- *Etosz*: szervezeti kultúra és értékrend, a bizalom szintje a szervezeten belül.

Az OIMM a következő érettségi szinteket határozza meg:

- *0 – Független (Independent):* a szervezetek között korábban nem volt interakció, esetlegesen működési céljaik sem azonosak, az együttműködés igénye előre nem tervezett módon merül fel. A szervezetek a hagyományos kommunikációs csatornákon (telefon, fax, email, értekezletek) keresztül lépnek kapcsolatba.

- *1 – Eseti (Ad hoc):* a szervezetek magas szintű működési céljai azonosak, korlátozott mértékű szervezeti útmutatás áll rendelkezésre, mely az interoperabilitás általános formáinak kialakítását biztosítja, a specifikus formák kialakítására nincs írott protokoll.
- *2 – Közreműködő (Collaborative):* a szervezetek magas szintű céljai azonosak, az együttműködéshez szükséges szerepkörök és felelősségek a normál ügymenetben is megtalálhatók. A szervezetek között rendszeres tudás-csere van.
- *3 – Integrált (Integrated):* a szervezetek céljai és értékrendje azonos, az interoperabilitás biztosítására begyakorolt folyamatok és részletes eljárásrendek állnak rendelkezésre. Az együttműködés ugyanakkor nem mindennapos.
- *4 – Egyesített (Unified):* a szervezetek céljai, értékrendje és szervezeti kultúrája azonos, az együttműködés mindennapos gyakorlat. [7; 1.-8.o.]

Government Interoperability Maturity Model (GIMM; Kormányzati Interoperabilitási Érettségi Modell)

A Government Interoperability Maturity Matrix (GIMM) megalkotásának célja, hogy egyszerű, önértékelésre alkalmas modellt biztosítson a közszféra szervezetek számára, mely felhasználható elektronikus szolgáltatásaik interoperabilitási szintjének értékelésére, s a kívánt szolgáltatási színvonal eléréséhez szükséges lépések megtervezésére.

Az GIMM attribútumai az EIF-ben meghatározott interoperabilitási rétegekre épülnek, a következőképpen:

- *Szervezeti interoperabilitás:* az együttműködésben érintett közszféra szervezetek működési céljainak, folyamatainak és eljárásrendjeinek összehangolása.
- *Műszaki interoperabilitás*: az informatikai rendszerek összekapcsolásának műszaki kérdései (interfészek, adatintegráció, adatcsere, hozzáférés, biztonság).
- *Szemantikai interoperabilitás*: az átadott adatok, információk más alkalmazások általi feldolgozhatósága, értelmezhetősége.

A GIMM az elektronikus közszolgáltatásokat biztosító szervezetek együttműködési képességeit méri, az EIF rétegei mentén. A szintek tartalmának kialakítása során az OIMM szintjeinek elemei és logikája fedezhető fel.

- *0 – Független (Independent):* interakció egymástól független szervezetek között.
- *1 – Eseti (Ad hoc):* a szervezetek eljárásrendjei csekély mértékben terjednek ki a más szervezetekkel való interakciók kezelésére, mely eseti együttműködések kialakítását teszi lehetővé.
- *2 – Közreműködő (Collaborative):* jól definiált szervezeti eljárásrendek az interoperabilitás biztosítására, azonos szervezeti célok, de a szervezetek elkülönülten működnek.
- *3 – Integrált (Integrated):* azonos szervezeti célok és értékek, teljes felkészültség az együttműködésre, elkülönült szervezetek között.
- *4 – Egyesített (Unified):* azonos célok, értékek és irányítási struktúra, közös tudásbázis. [8; 1.-4.o.]

Information System Interoperability Maturity Model (ISIMM; Információs Rendszer Interoperabilitási Érettségi Modell)

Az ISIMM alkotóinak célja egy gyakorlatias megközelítésű érettségi modell kidolgozása volt, mely az információs rendszerek közti interoperabilitás műszaki aspektusainak értékelését támogatja. Az ISIMM a LISI és a GIMM modelleken alapszik.

Az ISIMM az információs rendszerek technológiai interoperabilitását vizsgálja, célja a komplexitás részletesebb feltárása, az összefüggések mélyebb értelmezése. Ennek érdekében

az interoperabilitás alábbi dimenzióinak minőségét vizsgálja:

- *Adatszintű interoperabilitás*: eltérő rendszerek és alkalmazások adatainak szemantikai és szintaktikai értelmezése.
- *Szoftver interoperabilitás*: az szervezeti alkalmazások közti különbségek áthidalása az adatcsere lebonyolítása érdekében.
- *Kommunikációs interoperabilitás*: közös protokollok használata a rendszerek összekapcsolására és a kommunikáció megvalósítására.
- *Fizikai interoperabilitás*: hardware, hálózati eszközök és perifériák összekapcsolása.

Az ISIMM a következő érettségi szinteket határozza meg:

- *1 – Kézi (Manual):* az információs rendszer nem kapcsolódik más rendszerekhez, az adatcsere manuális úton történik.
- *2 – Eseti (Ad hoc):* nem szabványos adatok elektronikus cseréje rendszerek között, ad hoc jelleggel. A szervezetek alkalmazásai és adatbázisaik szeparáltak.
- *3 – Közreműködő (Collaborative):* a szervezetek egyes szigetszerű alkalmazásai összekapcsolódnak, az adatcsere harmonizált logikai adatmodellek alapján zajlik. A szervezetek további alkalmazásai és adatbázisai szeparáltak.
- *4 – Integrált (Integrated):* az adatbázisok egy része közös használatú, a szigetszerű alkalmazások közti adatcsere közös adatmodelleken alapszik. Szakterületi együttműködés, a szervezetek integrálják egyes szolgáltatásaikat és rendszereiket.
- *5 – Egyesített (Unified):* a szervezeti adatbázisok és alkalmazások közös használatúak, az adatmodellek teljesen egységesek. Vállalati szintű együttműködés, folyamatos és magas minőségű interoperabilitás. [9; 1.-3.o.]

A MODELLEK ÖSSZEHASONLÍTÓ ELEMZÉSE

A tanulmány záró részében a bemutatott modellek komparatív elemzését végzem el, a modellalkotás általános jellemzői, a szintek tartalma, attribútumai és a modellek felhasználhatósága szempontjából, az elektronikus közszolgáltatások érettségének több szempontú vizsgálata érdekében.

Modellek általános jellemzőinek elemzése

Elsőként a modellek alkalmazási- és fókuszterületét (a modell mely tényezőkre összpontosítva vizsgálja az érettséget), típusát (fejlődési, képességi, hibrid), valamint esetleges referenciamodelljeit vetem össze.

Modell	Felhasználási terület	Fókusz	Modelltípus	Hivatkozott más modellek
IMM	közszolgáltatás	jó gyakorlatok	hibrid	-
SGIMM	szakterülettől független	szervezetek integrációs képességei	képességi	-
LISI	katonai, rendszerfejlesztés	adatbázisok és alkalmazások integrációs képessége	képességi	-
OIMM	katonai	együttműködési képességek	képességi	LISI
GIMM	közszolgáltatás	szervezeti interoperabilitás	képességi	LISI, OIMM
ISIMM	rendszerfejlesztés	adatbázisok és alkalmazások integráltsága	fejlődési	LISI, GIMM

1. táblázat: érettségi modellek összevetése a modellalkotás általános jellemzői szerint (a szerző szerkesztése [1,5,6,7,8,9] alapján)

A modellek között szerepelnek szakterület specifikusak és általánosan alkalmazhatóak is. A modellek fókuszterületeit tekintve, az IMM külső tényezőkre (ágazati jó gyakorlatok) összpontosít, míg a többi modell belső nézőpontú (képességek, architektúra).

A korábban alkalmazott tipológiák szempontjából az IMM hibrid érettségi modell, mivel alapvetően az ágazati jó gyakorlatok alkalmazásának mértékéhez viszonyítja az érettség fokát. A további érettségi modellek szervezeti és technológiai képességekre fókuszáló ún. képességi modellek, az ISIMM kivételével, mely fejlődési érettségi modellként különböző architektúrális, alkalmazás és adatbázis szintű attribútumok fejlettségét méri. A vizsgált érettségi modellek egy része hivatkozik más referenciamodellekre, több esetben egymás elveit veszik alapul.

Megállapítható, hogy az IMM e mintában egyedinek számít, így a további modellek eltérő természetük miatt (általános alkalmazhatóság, nem hibrid jelleg, belső fókusz) számos új és praktikus nézőpontot biztosítanak az elektronikus közszolgáltatások interoperabilitási érettségének vizsgálatához, így megfelelő alapot biztosítanak a tanulmány céljainak teljesítéséhez.

Érettségi szintek elemzése

A továbbiakban az érettségi modellek szintjeit, azok tartalmát és a szintek által megjelenített fejlődési íveket vizsgálom.

1.

Modell	0.szint	1.szint	2.szint	3.szint	4. szint	5. szint
IMM		eseti	alkalmi	lényegi	fenntartható	hézagmentes
SGIMM		nem átjárható	kezdetleges	erősödő	minősített	kompatibilis
LISI	elszigetelt	kapcsolódó	funkcionális	szakterület alapú	vállalati szintű	
OIMM	független	eseti	közreműködő	integrált	egyesített	
GIMM		független	eseti	közreműködő	integrált	egyesített
ISIMM		kézi	eseti	közreműködő	integrált	egyesített

2. táblázat: érettségi modellek szintjeinek összevetése (a szerző szerkesztése [1,5,6,7,8,9] alapján)

A modellek mindegyike követi a bevált módszertani gyakorlatot és öt érettségi szintet határoz meg. A szintek kialakításának specifikuma, hogy a LISI és az OIMM esetén a szintek számozása 0-val kezdődik.

A szintek elnevezése alapján megfigyelhető, hogy az önálló modellalkotók (IMM, LISI, SGIMM) sajátos, a modell specifikumait jól megragadó elnevezéseket választottak, ez alól egyedi kivétel az eseti (ad hoc) jelző visszatérő használata. A más referenciamodelleket alapul vevő modellek (OIMM, GIMM, ISIMM) esetén a szintek elnevezése erős összhangot mutat.

Az OIMM – GIMM esetében, valamint az ISIMM-LISI esetében a szintek tartalmában nagyfokú összhang mutatkozik, az első modellpár hangsúlyos szervezeti, míg a második esetben erőteljesen technikai fókusszal.

Az azonos szintek könnyebb áttekintése és összevethetősége érdekében a szinteket egységes struktúrában is megjelenítem.

Modell	Kiinduló szint	Köztes szint I.	Köztes szint II.	Köztes szint III.	Zárószint
IMM	eseti	alkalmi	lényegi	fenntartható	hézagmentes
SGIMM	nem átjárható	kezdetleges	erősödő	minősített	kompatibilis
LISI	elszigetelt	kapcsolódó	funkcionális	szakterület alapú	vállalati szintű
OIMM	független	eseti	közreműködő	integrált	egyesített
GIMM	független	eseti	közreműködő	integrált	egyesített
ISIMM	kézi	eseti	közreműködő	integrált	egyesített

3. táblázat: érettségi modellek szintjei modellbeli dinamika szerint (a szerző szerkesztése [1,5,6,7,8,9] alapján)

A kiinduló szintekről a fent leírtak alapján megállapítható, hogy az interoperabilitási és az együttműködési képességek hiányát, vagy annak korlátozott létét ragadják meg. Az I. köztes szinten az interoperabilitás járulékos tényező, a szervezeti működésre, a napi ügymentre, irányelvekre csekély befolyást gyakorol (eseti, alkalmai felhasználás, belső szabványok meghatározóak, munkaállomások közti kapcsolat, korlátozott szervezeti iránymutatás).

A II. köztes szinten az interoperabilitás a normál ügyment részévé válik (piaci gyakorlatok és szabványok gyakori használata, szigetszerű alkalmazások, helyi hálózatok közti kapcsolat, meglévő szervezeti iránymutatás).

A III. köztes szinten az interoperabilitás a normál működést meghatározó tényezővé válik (piaci gyakorlatok és szabványok használata meghatározó, közös adatbázisok, szakterületi együttműködés, részletes szervezeti iránymutatás), a belső szabályozó tényezők és a külső szabványok használata között egyfajta egyensúly alakul ki.

A záró szint tekintetében az interoperabilitás teljes körű, de a fókusz itt nemcsak az együttműködés teljességére esik, hanem az általa kiváltott szinergiákra, a járulékos értékteremtésre is (mintaszerű piaci gyakorlat, hozzájárulás az ágazati szabványok tökéletesítéséhez).

Összességében megállapítható, hogy az IMM és a további modellek struktúrája és dinamikája nagy hasonlóságot mutat. Mindez segíti a tanulmány céljának megvalósítását, mivel az IMM-től eltérő nézőpontú, de hasonló szerkezetű, dinamikájú modellek lehetővé teszik az interoperabilitás vizsgálati eszköztárának bővítését.

Attribútumok elemzése

Az attribútumok az érettségi modellek elemi tényezői. A modellek attribútum-fókuszpontjainak összevetéséhez az IMM kidolgozását megalapozó EIF interoperabilitási rétegeit (jogi, szervezeti, szemantikai, műszaki) veszem alapul. Az egyes érettségi modellek attribútumait e rétegek szerint rendszereztem, melynek eredményét az alábbi táblázat jeleníti meg. Kiemelendő, hogy egy attribútum több réteghez is kapcsolódhat.

Modell	Attribútum	EIF rétegek
IMM	Szolgáltatás nyújtás	Technikai, szervezeti, szemantikai interoperabilitás
	Szolgáltatás igénybevétel	Technikai, szervezeti, szemantikai interoperabilitás
	Szolgáltatás menedzsment	Jogi, technikai, szervezeti, szemantikai interoperabilitás
SGIMM	Hatékonyság növelése	Szervezeti interoperabilitás
	Interoperabilitási érettség	Szervezeti interoperabilitás, technikai interoperabilitás, szemantikai interoperabilitás
	Technikai architektúra és design	Technikai interoperabilitás
	Üzleti architektúra és design	Szervezeti interoperabilitás
	Interoperabilitás szervezeti támogatása	Szervezeti interoperabilitás
	Biztonság	Technikai interoperabilitás
	Konzekvens tervezés	Technikai interoperabilitás
	Kritikus funkciók szeparációja	Szervezeti interoperabilitás
LISI	Folyamatok	Szervezeti interoperabilitás
	Alkalmazás	Technikai interoperabilitás
	Infrastruktúra	Technikai interoperabilitás
	Adat	Szemantikai interoperabilitás
OIMM	Felkészültség	Szervezeti interoperabilitás
	Ismeret	Szervezeti interoperabilitás
	Irányítási stílus	Szervezeti interoperabilitás
	Etosz	Szervezeti interoperabilitás
GIMM	Szervezeti interoperabilitás	Szervezeti interoperabilitás
	Technikai interoperabilitás	Technikai interoperabilitás
	Szemantikai interoperabilitás	Szemantikai interoperabilitás
ISIMM	Adatszintű interoperabilitás	Szemantikai interoperabilitás
	Szoftver interoperabilitás	Technikai interoperabilitás
	Kommunikációs interoperabilitás	Technikai interoperabilitás
	Fizikai interoperabilitás	Technikai interoperabilitás

4. táblázat: érettségi modellek attribútumai a szerző szerkesztése [1,5,6,7,8,9] alapján)

A modellek eltérő típusaiból, céljaiból fakadóan az attribútumok száma, elnevezése és tartalma eltér, hiszen a modellek elemi tényezőiként az attribútumok jelenítik meg a modellek specifikumait. A LISI-t referenciamodellként használó OIMM és ISIMM esetében az attribútumok száma azonos.

Az IMM attribútumok az EIF minden rétegéhez kapcsolódnak, e terjedelemben a további modellek egyike sem foglalkozik az interoperabilitással. A vizsgált modellek így olyan alternatív elemzési eszközként alkalmazhatók, melyek az interoperabilitás egy rétegének, vagy egyes rétegeinek célzott elemzésére szolgálnak.

Az elemzés eredményeinek felhasználhatósága a közszolgálatban

A tanulmányban az érettségi modellek számos strukturális, terjedelmi és tartalmi aspektusa került elemzésre. A továbbiakban a megszerzett tapasztalok, eredmények felhasználhatóságával, az elektronikus közszolgáltatások fejlesztését támogató modellalkotás terén való hasznosíthatóságával foglalkozom.

Az IMM vizsgált mintához viszonyított egyedisége miatt az eredmények felhasználásának elsődleges lehetőségeként a különbözőségek alternatív e-közszolgálati modellek kialakítása során való hasznosítása kínálkozik.

Az elektronikus közszolgáltatások összetettségét, folyamatos fejlődését és a sikerességüket meghatározó tényezők sokaságát figyelembe véve, alternatív elemzési nézőpontok biztosítása és az IMM mellett további érettségi modellek alkalmazása, esetlegesen kidolgozása javasolt. A szempontrendszer szélesítésének elsődlegesen javasolt iránya, hogy az elektronikus közszolgáltatások elemzése során a hibrid jellegű IMM mellett olyan más modelltípusok (fejlődési, képességi) is alkalmazásra kerüljenek, melyek hasonló felhasználási területre, vagy általános felhasználásra készültek.

E tekintetben hasznos kiindulópontot jelenthet az ISIMM, a GIMM és az SGIMM alkalmazása. Az ISIMM elsődlegesen a technikai tényezőkre koncentráló, általánosan alkalmazható fejlődési modell, amelyben a fejlesztések technikai oldala kellő hangsúlyt kap, valamint a modell eltérő típusa révén is alternatív nézőpontot biztosít. A képességi modellek tekintetében a GIMM megfelelő kiindulási pontot jelent, mivel célzottan a kormányzati rendszerek és szervezeti képességek érettségének értékelésével foglalkozik, kellő hangsúlyt adva a szervezeti tényezőknek. A vázolt elveket figyelembe véve megfontolandó az SGIMM alkalmazása is, mivel az interoperabilitás rétegeinek minden a téma szempontjából fontos dimenziójára reflektál, s azok részletes elemzését teszi lehetővé.

A LISI és az OIMM elsődlegesen a katonai műveletek szempontjából fontos képességek értékelésére került kidolgozásra, valamint alapelveik megjelennek a fent javasolt modellekben is (az ISIMM a LISI elveire, a GIMM pedig az OIMM alapjaira épül), így az IMM, GIMM és ISIMM együttes alkalmazása megfelelő módszertani eszköztárat biztosít az elektronikus közszolgáltatások fejlesztése terén alternatív elemzési nézőpontok kilapításához, valamint esetleges új modellek kidolgozásához.

KÖVETKEZTETÉSEK

A tanulmányban öt interoperabilitási érettségi modell került összevetésre az Európai Bizottság, határon átnyúló elektronikus közszolgáltatások interoperabilitási érettségét mérő modelljével (IMM). A minta kiválasztása során olyanok modellek szelekciójára törekedtem, melyek lehetővé teszik az interoperabilitási érettségének több szempontú elemzését, így különböző felhasználási területek (katonai, közszolgálat, rendszerfejlesztés) eltérő típusú (fejlődési, képességi) modelljei kerültek a mintába. A modellek összevetése a következő megállapításokra vezetett.

A modellek céljainak összevetése alapján megállapítható, hogy a jó gyakorlatok alkalmazását mérő IMM egyedinek számít a mintában, a további modellek az interoperabilitás specifikus képességeivel, vagy a rendszerek egyes tulajdonságaival foglalkoznak. Mindez azonban hasznos eszköztárat biztosít az elektronikus közszolgáltatások több nézőpontból történő elemzéséhez.

A szintek száma tekintetében minden modell a bevált módszertani gyakorlatot követi és ötszintű skálán méri az interoperabilitási érettségét. Összességében az IMM és a vizsgált modellek struktúrája, dinamikája nagy hasonlóságot mutat, azonban az alkotók a szintek elnevezésében erősen érvényre juttatják a modellek specifikumait.

A modellek attribútumai jól elkülöníthetők az EIF interoperabilitási rétegei (jogi, technikai, szervezeti, szemantikai) szerint, a rétegek teljes spektrumát egyedül az IMM fedi le, s azok mindegyikében értékeli a jó gyakorlatok alkalmazását. Tekintettel a további modellek specifikus jellegére, azok jellemzően az interoperabilitás egy, vagy egyes rétegeihez kapcsolódnak.

A határon átnyúló elektronikus közszolgáltatások interoperabilitását tényezők komplex együttese befolyásolja, így az érettség vizsgálatára az IMM mellett további alternatív

nézőpontú modellek alkalmazása javasolt. E célra a vizsgált minta megfelelőnek bizonyul, hiszen a modellek megközelítése kellően specifikus, de szerkezetük és dinamikájuk az IMM-hez hasonlatos és attribútumaik jól besorolhatók az EIF alapját képező interoperabilitási rétegek szerint. Az érettség alternatív vizsgálata elsődlegesen más típusú (fejlődési, képességi), de általánosan alkalmazható, vagy hasonló felhasználási területre készült modellekkel valósítható meg. E tekintetben, az IMM, GIMM és ISIMM modellek alkalmazása hatékony módszertani keretet nyújt az elektronikus közszolgáltatások interoperabilitásának alternatív elemzéséhez illetve esetleges új modellek kidolgozásához.

FELHASZNÁLT IRODALOM

[1] EURÓPAI BIZOTTSÁG.: Interoperability Maturity Model – IMM Guideline, Európai Bizottság, Brüsszel, 2016

[2] CARALLI, RICHARD, KNIGH M., MONTGOMERY T, A. .: Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, 2012

[3] EURÓPAI BIZOTTSÁG.: Európai Interoperabilitási Keretrendszer, Európai Bizottság, Brüsszel, 2010

[4] EURÓPAI BIZOTTSÁG.: Interoperability Maturity Model – IMM Full questionnaire, Európai Bizottság, Brüsszel, 2016

[5] MATER, J., DRUMMOND R..: A Smart Grid Interoperability Maturity Model Rating System Predicting “Plug and Play” Integration Probability, GridWise Architecture Council, Richland, USA, 2009

[6] C4ISR ARCHITECTURE WORKING GROUP.: Levels of Information Systems Interoperability (LISI), USA, 1998

[7] CLARK T., JONES, R.: Organisational Interoperability Maturity Model for C2, In Proceedings of the Command And Control Research And Technology Symposium (CCRTS), Newport, USA, 1999

[8] SARANTIS, D., CHARALABIDIS, X, PSARRAS, J.: Towards Standardising Interoperability Levels for Information Systems of Public Administrations, eJETA Special Issue on “Interoperability for Enterprises and Administrations Worldwide”, Athens, 2008

[9] VAN STADEN, S., MBALE, J.: The Information Systems Interoperability Maturity Model (ISIMM): Towards Standardizing Technical Interoperability and Assessment within Government, in: I.J. Information Engineering and Electronic Business, MECS Publisher, 2012.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

MOBILHÁLÓZATOK KAPACITÁSA VÉSZHELYZETBEN

CAPACITY OF MOBILE NETWORKS IN EMERGENCY CASE

MAROS Dóra; TEMESVÁRI Zsolt

(0000-0002-8600-9035); (0000-0001-8309-7992)

maros.dora@kvk.uni-obuda.hu; zsolt.temesvari@gmail.com

Absztrakt

A rádiós hálózatok használata mindennapjaink megkerülhetetlen részévé vált, ezért mobil termináljaink napról napra hangsúlyosabb szerepet kapnak életünkben, ezért egyre fontosabb, hogy az elérhető szolgáltatások folyamatosan és zavartalanul működjenek, legyen szó akár lakossági, akár nemzetbiztonsági felhasználásról. Vészhelyzet vagy katasztrófa sújtotta területen ezen infrastruktúrák folyamatos működése elengedhetetlen lenne a vészhelyzeti kommunikáció biztosítására, viszont számos nehézség merülhet fel, az ilyen helyzetben uralkodó felhasználási szokások megváltozása miatt. A cikk áttekintést ad a meglévő mobilhálózatok működéséről, a kapacitásról és annak bővítési lehetőségeiről, valamint az elérhető adatátviteli sebesség mértékéről. A téma aktualitása és fontossága a 2016-os brüsszeli terrortámadás elemzésével kap hangsúlyt. Az esettanulmány arra ad részben választ, hogy a forgalom-penetrációból miként alakulnak az esetleges kapacitásproblémák és milyen lehetőségek adódnak a torlódások kezelésére.

Kulcsszavak: *vészhelyzet, mobilhálózatok, kapacitás*

Abstract

The use of wireless radio networks takes part in our everyday life, that's why mobile terminals play greater and greater role in our life. Therefore the operation of these wireless services should be continous and uninterrupted whether it is public or national security use. On emergency or disaster affected area the operation of these infrastructures is especially necessary, but unfortunately several problems can be detected due to the changed user habits (caused by panic) because of the vis maior situation. This article can give an overview about capacity of available mobile networks and the data transfer rate limits. The topic of capacity problems can get a greater focus by the analysis of the terrorist attack of Brussels 2016. The case study could partly give answer about the traffic penetration and solution about the *possible capacity problems experienced in emergency situation*

Keywords: *emergency case, mobile networks, capacity*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.15.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.28.

BEVEZETÉS

A mobilhálózatok tervezésekor olyan szempontokat kell figyelembe venni, mint az adott terület domborzati tulajdonságai, beépítettsége, a várható felhasználók száma, a becsült forgalomeloszlás, az igénybe vett szolgáltatás jellege és sávszélesség igénye (adat, hang), valamint az aktív mobileszközök száma.

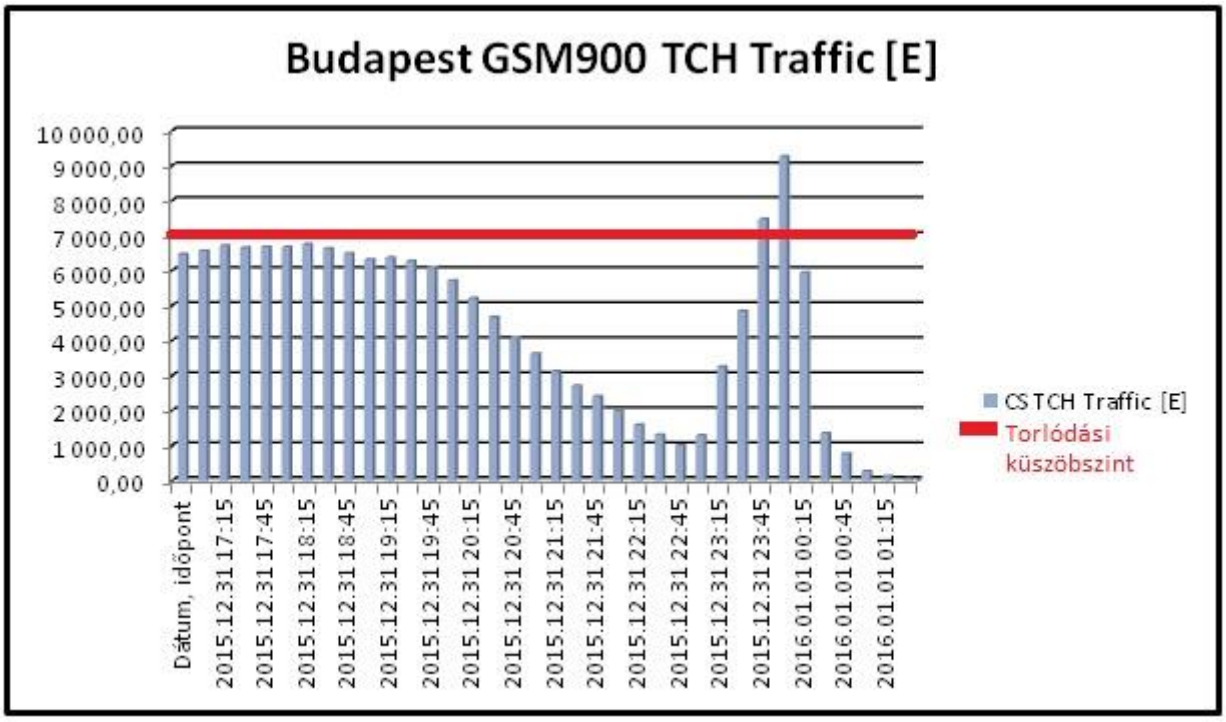
A fentieken felül - egyéb fontos szempont és kritérium mellett - a tényleges hangsúlyt a felhasználók legjobb minőségben történő kiszolgálására kell helyezni, hiszen a minőségi hálózatelérést és adatforgalmat a folyamatosan növekvő igények és az egyre több okostelefon használónak is biztosítani kell. Ezek alapján a mobilhálózat minősége általában tervezhetővé válik, legyen szó akár GSM[1], UMTS[2], LTE[3] technológiáról. Az említett elméleti tényezőkön túl számos másik, egyenértékű feltételnek is szükséges megfelelni a tervezés során, ezért fontos, hogy az eltérő technológiák egymástól függetlenül paraméterezhetők legyenek, és a már működő rendszerek működése folyamatosan legyen optimalizálva, annak érdekében, hogy a hálózat a felhasználói és egyéb változásokhoz minél rugalmasabban igazodjon.

Krízishelyzetekben a hálózattervezés hagyományos megoldásai nem nyújtanak kielégítő megoldásokat a jelentősen megnövekedett forgalom kezelésére. Ilyenkor olyan megoldások alkalmazása válik szükségessé, amelyeket a normál forgalmi elvárások esetére tervezett hálózatok már nem képesek kielégíteni. A probléma megoldását nem csupán technikai, hanem gazdasági szempontok és befolyásolják.

MOBILHÁLÓZATOK KAPACITÁSÁNAK HATÁRAI

Katasztrófa és vészhelyzet vagy egy terrortámadás esetén a mobilhálózatok használata olyan mértékben változik meg, hogy azt a hálózati rendszerek megfelelő optimalizálása mellett sem lehet minden esetben kezelni. Ilyen esetekben a felhasználószám hirtelen ugrásszerű növekedése miatt a mobilhálózatok elérhetik kapacitásuk korlátját, amely torlódási problémákhoz vezet. Egy ilyen valós helyzetet szemléltet az 1. ábra, amelyen a budapesti GSM forgalom változását láthatjuk Szilveszter éjjelén.

[1] GSM (2G): Global System for Mobile Communications - Globális rendszer mobil kommunikációhoz
[2] UMTS (3G): Universal Mobile Telecommunications System - Egyetemes mobil távközlési rendszer
[3] LTE (4G): Long Term Evolution - 4G mobilhálózat



1. ábra A budapesti GSM900-as forgalom alakulása 2015 szilveszter napján negyedórás mérésekre bontva Erlang[4]-ban megadva (a szerző szerkesztése)

Az ábrán látható, hogy december 31. éjfél közeledtével a GSM hálózat eléri maximális kapacitását és a forgalmi torlódás következik be.
Torlódás esetén a beszédhívás vagy adatforgalmazás kezdeményezés sikerességi aránya (Call Success Rate) drasztikusan lecsökken, a kapcsolateldobás (Call Drop) pedig emelkedik. A kritikus helyzetekben tapasztalható hirtelen forgalomnövekedés a rendszer kapacitásának határain lényegesen túlmutat. A publikus mobilhálózatok kritikus helyzetekben előforduló kapacitás problémáinak megértéséhez elengedhetetlenül szükséges, hogy a kapacitástervezés folyamatát hálózatokra bontva, röviden áttekintsük.

Magyarországon jelenleg három közcélú mobilhálózat működik, a GSM (2G), az UMTS (3G), és az LTE (4G). Ezen hálózatok egymástól függetlenek olyan értelemben, hogy saját cellákkal rendelkeznek, viszont az egyes technológiák közti átjárás biztosított. Várhatóan 2020 után kerülnek kereskedelmi alkalmazása az 5G hálózatok, amelyek lényeges kapacitás és sebességnövekedést tesznek majd lehetővé.

Kapacitástervezési szempontok különböző hálózatok esetén

GSM hálózat (2G)

A GSM hálózat egy frekvencia duplex (FDD) rendszer (900 és 1800 MHz-es tartományban), amely frekvencia és időosztásos hozzáférési technológiával (FDMA/TDMA) működik. A bázisállomás (BTS) TRX, azaz az adó-vevő egységében 8 db időrés konfigurálható egy vivőfrekvenciára uplink (feltöltés) és downlink (letöltés) irányban. Egy időrésben egyidejűleg egy hanghívás kezelhető, de további hálózat optimalizálási funkciók használatával ez a

[4] Erlang: Telekommunikációs forgalom jellemzésére szolgáló mértékegység. /1 Erlang: egy folytonos hívás, mely egy óra időtartamon keresztül tart/

kapacitás növelhető. A GSM rendszer is alkalmas adatforgalmazásra EDGE[5] szabvány segítségével (~384 kbit/s elvi maximum adatátviteli sebességet biztosít).

Minden TRX más csatornát kezel (egy csatorna 200KHz sávszélességű), amelynek pontos értékét a rádiós frekvencia tervezésekor határoznak meg. Az adott bázisállomásoknál alkalmazott TRX szám határozza meg az adott bázisállomás kapacitását. Az Erlang B tábla segítségével az előre meghatározott blokkolási arány, a várható forgalomeloszlás és adatforgalom mentén meghatározható az adott cella kapacitása.

A mobil szolgáltatók a kapacitás tervezéskor általában egy normál nap legmagasabb kalkulált forgalmú időszakára (óráira) számolnak, legtöbb esetben ez gazdasági szempontból valóban indokoltnak látszik. Egy adott cella kapacitásának maximuma a TRX-ek számától függ, ha további kapacitásnövelésre van szükség, erre az alábbi módokon van lehetőség:

- Hálózat optimalizálással és/vagy forgalomtereléssel más technológiákba:
  - Ez a központból a hálózatmenedzsment funkció segítségével bármikor megtehető.
- Cellaméret csökkentésével:
  - A cellaméret csökkentése az antenna kimeneti teljesítményének csökkenésével, vagy az antenna dőlésszögének megváltoztatásával (tilt) érhető el. Ezzel a megoldással ugyanaz a forgalom kisebb területre fókuszálható, és torlódás esetén a kapacitást meghaladó forgalmat a szomszédos cellák veszik át. Ez szintén a hálózatmenedzsment funkció segítségével kezelhető.
- További TRX-ek indításával:
  - A bázisállomások tervezésekor (gyártó specifikus) meghatározott a maximális TRX-ek száma A normál forgalmi időszakokban azonban nem szükséges az összes TRX-et aktív módban üzemeltetni, vagy gazdaságossági szempontból eleve nincs a maximális számú TRX a bázisállomáson telepítve. Ilyenkor két megoldás lehetséges:
    a) Az inaktív TRX-t aktiválni
    b) Új TRX elhelyezése a bázisállomáson és annak aktiválása.

Olyan esetekben, amikor egy bázisállomás fizikailag is megsérül, új bázisállomás gyors telepítése szükséges. Ilyenkor mozgatható, általában erre alkalmas például teherautóba szerelt bázisállomások használata a leggyorsabb és leghatékonyabb megoldás a kritikus helyzet megoldására.

UMTS hálózat (3G)

Az UMTS szélessávú kódosztás (WCDMA)[6] alapú rendszer, amely Magyarországon a 900 MHz-es, valamint a 2100 MHz-es sávon működik. A hálózatok optimalizálásakor a szolgáltatók meghatározzák, hogy milyen eloszlással alakuljon a forgalom az UMTS és GSM technológiák közt. Utóbbinak természetesen függvénye, hogy a mobilkészülék rendelkezzen 3G modullal.

A 3G technológia már szélessávúnak tekinthető, azaz nem elkülönített spektrumú keskenysávú vivőkön működik, mint a GSM, hanem azonos frekvenciájú szélessávú blokkokban üzemel (5MHz-es sávszélességben), így a klasszikus értelemben vett

[5] EDGE: Enhanced Data rates for Global Evolution - GSM rendszer csomagkapcsolt adatátviteli megoldásának továbbfejlesztése
[6] WCDMA: Wideband Code Division Multiple Access - Szélessávú kódosztásos többszörös hozzáférés

frekvenciatervezés itt már nem értelmezett. A cellák egymásra nem ortogonálisak, azaz a cellák között frekvencia interferenciák vannak, e miatt a jel/zaj viszony megfelelő mértéke sokkal hangsúlyosabb szerepet játszik a hálózatok tervezésekor. A mobil terminálok 3G hálózatokban az eltérő frekvenciablokkról nem ismerik fel a cellákat, mert azok azonos frekvencián működnek, ezért a cellák megkülönböztetésére az un. scrambling-kódokat (keverőkód) használják.

Az UMTS hálózatokon keresztül a hanghívások mellett már nagy adatforgalom is bonyolódik, így a cellák kapacitását egy adott időben tapasztalható adatforgalmi felhasználási igények is nagyban meghatározzák. Az ún. „dual carrier" alkalmazásával van lehetőség két egybefüggő UMTS frekvenciablokk összefogására, biztosítva ezzel a teoretikus maximális 42 Mbit/s-ot. Egy 3G cella elméletben maximum 128 hanghívást képes lekezelni szimultán, viszont az adatforgalom számára ekkor már nem marad szabad kapacitás. 3G cellák torlódása esetén, a leterheltség csökkentésére a GSM-ben alkalmazott megoldásokon túl a következő megoldások szolgálhatnak:

- Újabb frekvenciablokkok integrációja, valamint ezen blokkok összefogása. Ez a megoldás frekvenciasáv korlátos, tehát ez akkor valósítható meg, ha az adott szolgáltató rendelkezik elegendő frekvenciával (legyen az a 900MHz-es vagy a 2100MHz-es sávban), valamint csak egybefüggő blokkok esetén van lehetőség az összefogásukra.
- Új bázisállomás(ok) létesítésével
    - Például, mikro[7] vagy „small"[8] cellák indítása különállóan vagy nagyobb makrocellákon belül.

LTE hálózat (4G)

Az LTE rendszer OFDMA[9] alapú rendszer, mely jelenleg Magyarországon a 800 MHz-es, 1800 MHz-es, valamint a 2600 MHz-es sávban működik és egyelőre csak IP alapú adatszolgáltatás nyújt a felhasználók számára, hangszolgáltatást nem. Megjelenésével az eddigi két technológia leterheltsége az LTE képes telefonok elterjedésének köszönhetően egyre csökken. Az LTE rádiós hozzáférési technológia lényegesen különbözik a 2G és 3G hálózatokban alkalmazott technológiáktól. Az OFDM átvitel akár nem folytonos spektrum összefogására is lehetőséget ad, valamint a sávszélesség rugalmas megválasztását is megengedi.

Ennek köszönhetően különböző frekvenciasávok összefogásával (carrier aggregation) az elérhető adatátviteli sebesség tovább növelhető. Itt érdemes megemlíteni a térbeli multiplexálási technikát, elterjedtebb nevén MIMO-t[10], amellyel a frekvencia-összefogáshoz hasonlóan tovább emelhető a sebesség.

A MIMO átviteli mód több antennaút egyidejű használatát jelenti az adó és a vevő oldalon, az egyes antennákra különböző információt juttatunk azonos frekvenciasáv használata közben. A frekvenciasávok, valamint a MIMO használatából adódó lehetséges sebességnövekményt a következő (2.) ábrán láthatjuk.

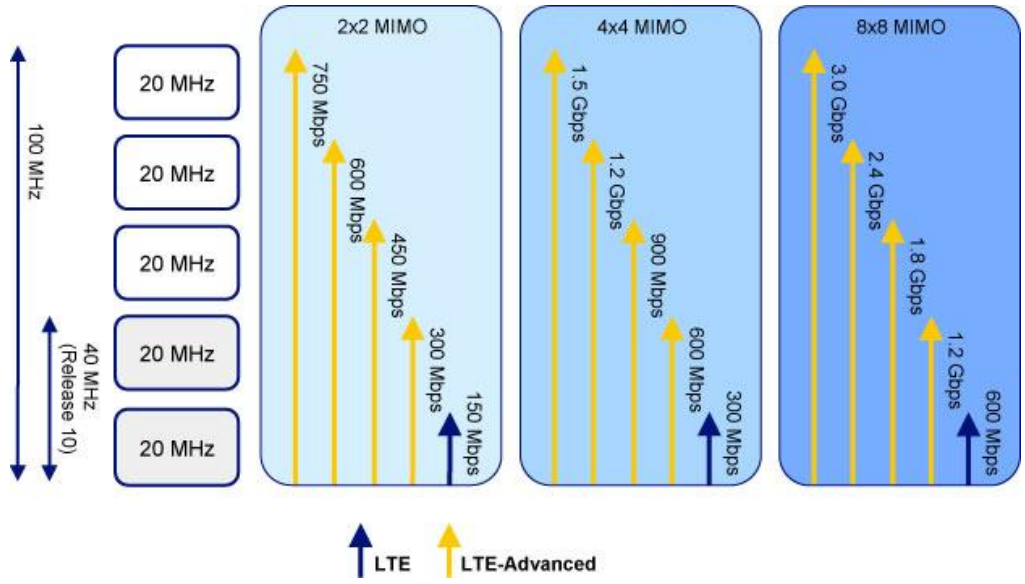
---

[7] Mikrocella: kültérben alkalmazandó, a makrocellánál alacsonyabb antennamagasságból sugárzott cella

[8] „Small" cella: kültérben alkalmazandó, a mikrocellánál alacsonyabb antennamagasságból sugárzott cella, forgalmas városrész, vagy eseti rendezvények ellátására alkalmas

[9] OFDMA: Orthogonal Frequency-Division Multiple Access - Ortogonális frekvencia-osztásos multiplexelés

[10] MIMO: Multiple-Input and Multiple-Output – Többszörös bemenet és többszörös kimenet



2. ábra. Az LTE és LTE-A[11] elérhető adatátviteli sebességének alakulása az összefogott spektrum és az alkalmazott MIMO függvényében [1]

Az LTE cellák kapacitását tekintve elmondható, hogy egy 5 MHz-es blokk szabvány szerint legalább 200 aktív mobil terminál átlagos forgalmát képes kiszolgálni [2].

A kapacitás növelésére szolgáló megoldások lényegében megegyeznek a 3G celláknál említettekkel, kiegészítve annyival, hogy a 3G technológia esetén eltérő hálózat optimalizálási lehetőségek vannak, mivel az adott hálózatot lehetőség van a felhasználás jellegére szabni,

- Ha a maximális adatátviteli sebesség elérése a cél, úgy az erőforrásokat a hálózat megpróbálja a szerint allokálni, hogy az aktív terminálok részére az elérhető adatátviteli sebesség a lehetséges maximum felé közelítsen. Ez a kapacitás csökkenését eredményezi az egy időben kiszolgálható terminálok tekintetében.
- Ha az aktív terminálok ellátása kerül fókuszba, úgy az adatátvitel minimalizálásával a kapacitás maximalizálására optimalizálunk. Hotspot-okban12, nagy forgalmú helyeken (pl. fesztiválok vagy katasztrófa sújtotta területek) lehet ez a beállítás nagyobb jelentőségű.

A mobilhálózatok túlterheltség kezelésének tapasztalatai krízishelyzetekben

A brüsszeli terrortámadás

2016. március 22-én több robbantásos merénylet történt Brüsszelben: kettő a repülőtéren, egy a Maelbeek metróállomáson, mely során több tucatnyi ember vesztette életét, illetve a sebesültek száma is 200 felett volt.

Az ember természeteses reakciója ilyen helyzetben, hogy azonnal segítséget hív (segélykérő számok hívása), vagy szeretteiket, ismerőseiket szeretnék mielőbb tájékoztatni, biztonságban tudni. Ilyenkor mobiltelefonjaikat veszik elsősorban igénybe, azaz hanghívást kezdeményeznek és/vagy SMS[13]-t küldenek, de már nagyon elterjedt a közösségi oldalakon

[11] LTE-A: Long Term Evolution Advance - Továbbfejlesztett 4G mobilhálózat
[12] Hotspot: Forgalmas terület
[13] SMS: Short Message Service - Rövidüzenet szolgáltatás

(Facebook[14], Twitter[15], stb.) történő kommunikáció is. Utóbbiak (főleg a video és képtartalom miatt) jelentősen leterhelik a mobilhálózatokat, különösen krízis helyzetekben. A brüsszeli események során a pánik okozta azonnali információcsere főként hanghívások formájában történt. Viszonylag rövid időn belül hatalmas torlódás keletkezett a cellánként egyidejűleg indított több ezer hívás miatt (2G, 3G, s 4G cellákat együtt értve), mely már túlmutatott a rendszerek kapacitásán.

A szolgáltatók a közösségi oldalaikon arra kérték az előfizetőket, hogy hanghívás helyett inkább az SMS szolgáltatást és az internet alapú közösségi oldalakat (Twitter, Facebook) vagy üzenetküldő szolgáltatásokat (Viber[16], WhatsApp[17]) vegyék igénybe, ezzel is csökkentve a beszédcsatornák leterheltségét és a sürgős segélyhívások lehetővé tételét [3]. A hálózati torlódások ennek ellenére továbbra is fennálltak, így a hálózatüzemeltetőknek és a hatóságoknak egyéb intézkedéseket kellett tenniük a probléma enyhítésére. A következő megoldásokat alkalmazták:

- a repülőtér és környezetében elérhető Wi-Fi hotspotokat 24 órán át bárki számára ingyenesen és jelszó megadása nélkül elérhetővé tették, ezzel csökkentve a mobilhálózatokon átjáró adatforgalmat.
- a katasztrófavédelemmel együttműködve a szolgáltatók egy információs telefonszámot hoztak létre, ahol bárki segítséget, információt és eligazítást kérhetett [4].

A fenti intézkedés ellenére a mobilhálózatok több mint 8 óra elteltével is akadoztak az óriási kihasználtság miatt, az aznapi forgalom ugyanis duplája volt egy átlagos napnak, mind a beszédhívásokat és az SMS-eket, mind pedig az adatforgalmat illetően.

Összességében a válságstáb a mobilszolgáltatókkal szorosan együttműködve a lehetőségekhez mérten jól kezelte a helyzetet és mindent megtettek annak érdekében, hogy a kommunikáció és információáramlás a lehető legsikeresebb legyen.

KÖVETKEZTETÉSEK

A mobilhálózatok szolgáltatásainak megbízható alkalmazása fokozottan fontos kritikus helyzetekben. Mivel a rádiós hálózatok kapacitása is véges, az átlagos legforgalmasabb órához viszonyított többszörös forgalmat már nem biztos, hogy képesek kezelni – hiába a legjobb hálózat optimalizálási stratégia vagy a maximális felhasználói számot bőven meghaladó kapacitásra történő tervezés.

A hálózati problémák, a túlterheltség, a beszéd és az adatforgalom kimaradása, lassulása vagy teljes megszűnése miatt az információvesztés a bekövetkezett krízishelyzet súlyosságával arányos, ebben az esetben a hálózati operátoroknak és hatóságoknak mindent el kell követniük annak érdekében, hogy a forgalmi problémákat minimalizálják. A brüsszeli eseményekre a szolgáltatók által adott reakciók bíztatóak és példaként kell, hogy szolgáljanak a jövőre nézve.

A GSM, UMTS és LTE hálózat különálló rétegenként üzemel mind az alkalmazott frekvenciasávok, mind pedig a rádiós technológiák tekintetében, ezért ezek krízishelyzetekben – az adott szituációtól függően – egymást kiválthatják, szükség esetén a kapacitásnövelés céljait szolgálva. A jövő várható vezetéknélküli technológiájának, az 5G-nek a megjelenése

[14] Facebook: Internetes közösségi oldal
[15] Twitter: Internetes közösségi
[16] Viber: Internet alapú VOIP hang-, szöveges üzenet és fájlmegosztó rendszer
[17] Whatsapp: Internet alapú VOIP hang-, szöveges üzenet és fájlmegosztó rendszer

az extrém forgalomnövekedés kezelésében további megoldást hozhat, hiszen különálló hálózat révén plusz kapacitást tesznek majd elérhetővé. A meglévő technológiák fejlesztése az 5G első kiadásáig nem áll meg, az egyre több optimalizálási mechanizmus bevezetésének hála a hálózatok erőforrás-menedzsmentje teljesen automatikusan, mindig a felhasználók igényeinek megfelelően történik majd.

Jelenleg a cellák nagyságát és az antennák sugárzási irányait a rádiós antennák fix beállításai határolják be, a jövőben azonban olyan teljesen önműködő heterogén hálózatokat fognak kialakítani a bázisállomások optimalizálásával foglalkozó cégek, melyekben a cellák teljesítményét, sugárzási irányát és karakterisztikáját annak megfelelően fogják adaptív módon szabályozni, hogy a rádiós erőforrást éppen hova (mely területre) szükséges csoportosítani a forgalomi igények függvényében. Ezen felül a tervezők gondolnak a fenntarthatóságra, energiahatékonyságra is. Jelenleg ugyanis a bázisállomások a nap 24 órájában működnek, de a közeljövőben előreláthatólag mindig a napszaknak és forgalomnak megfelelő teljesítményt fogják alkalmazni, mely az áramfogyasztás drasztikus csökkenését eredményezheti majd.

Cikkünkben a publikus mobilhálózatokkal foglalkoztunk érintve azok tervezését, paraméterezését, különösen krízishelyzetekben. Elemeztük az elérhető kapacitást és adatátviteli sebességet a 2G, 3G és 4G technológiákat illetően, hogy rávilágítsunk a hálózatok krízishelyzetekben tapasztalható gyenge pontjaira. Kitértünk a kapacitás korlátjaira, valamint a lehetséges bővítési lehetőségeket is bemutattuk.

Az ismertetett problémákon túl, olyan egyéb kutatási lehetőségeket rejt a téma, amelyek megoldása további segítséget nyújthatna a vészhelyzetben tapasztalható mobilhálózati problémák megoldása tekintetében. Egy robbantásos merénylet vagy terroresemény, egy katasztrófahelyzet általában lokálisan okoznak komolyabb teljesítmény-degradációt, vagy kapacitásproblémát az egyes szolgáltatók mobilhálózataiban. A hálózat előbb torlódhat, majd működésképtelenné válik. Amennyiben a szolgáltatók hálózatai összegződnének ilyen esetekben, úgy megfelelő kapacitás-menedzselés mellett az erőforrások szétosztásával tovább lehetne javítani a hálózati kapacitást, segítve ezzel a mentő- és nemzetbiztonsági egységek, illetve a bajbajutottak kommunikációját egyaránt.

FELHASZNÁLT IRODALOM

[1] http://www.artizanetworks.com/resources/tutorials/accelera_tech.html (letöltve: 2016.11.15)

[2] https://communities.theiet.org/blogs/426/444 (letöltve: 2016.05.10)

[3] http://www.politico.eu/article/belgian-phone-network-crashing-under-strain-terror-attacks-airport-mobile/ (letöltve: 2016.05.10)

[4] http://www.independent.co.uk/life-style/gadgets-and-tech/news/brussels-attacks-phone-networks-zaventem-airport-explosion-maelbeek-metro-live-updates-a6945571.html (letöltve: 2016.05.10)

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

EGYSÉGES EURÓPAI KIBERTÉR? AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI POLITIKÁJÁNAK FEJLŐDÉSE

SINGLE EUROPEAN CYBERSPACE? THE DEVEOPMENT OF THE EUROPEAN UNION'S CYBER SECURITY POLICY

MOLNÁR Dóra

(ORCID: 0000-0002-1476-5253)

molnar.dora@uni-nke.hu

Absztrakt

A kiberbiztonság a biztonság nagyon dinamikusan fejlődő olyan új területe, amely egyre veszélyesebb fenyegetéseket rejt magában. Ezidáig csak az egyes nemzetállamok próbálták meg saját kiber infrastruktúrájukat megvédeni – több-kevesebb sikerrel –, egységes, európai szintű szabályozás nem létezett. A tanulmány felvázolja, hogy az elmúlt évtizedben az Európai Unió milyen lépéseket tett a kiberbiztonsági szabályrendszer és az egységes európai digitális piac megteremtése terén, és röviden ismerteti a 2016-ban elfogadott két legfontosabb jogforrást, az adatvédelmi rendeletet és a hálózatbiztonsági irányelvet. Ezek előremutató lépések ugyan, de valójában a stratégiák és a szabályozók gyakorlati megvalósulása fogja tudni igazolni, hogy e lépések elegendőek-e ahhoz, hogy az Unió sikeresen meg tudjon birkózni a kibertérben jelentkező egyre nagyobb számú és egyre súlyosabb fenyegetéssel.

"A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Egyed István Posztdoktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Kulcsszavak: *kiberbiztonság, Európai Unió, adatvédelem*

Abstract

Cybersecurity is a very dynamic new sector of security that involves more and more dangerous threats. So far only national states themselves tried to protect their own cyber infrastructure – with more or less success –, a single, Europe-wide regulation has not existed. The study outlines what steps the European Union has taken in the creation of regulations and of a single European digital market in the past decade and briefly describes the two most important sources of law adopted in 2016, the General Data Protection Regulation and the NIS directive. Although, these are steps forward, but only practical implementation of strategies and sources of law will be able to verify if these measures are sufficient enough for the European Union to successfully cope with the growing number of more and more serious cyber threats.

„The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in (the) István Egyed Postdoctoral Program."

Keywords: *cyber security, European Union, data protection*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.31.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.02.30.

BEVEZETÉS

Az elmúlt évben számos olyan fejlemény következett be, amelyek az európai kiberbiztonságot új alapokra helyezték. Talán a 2016-os év volt az, amikorra az Európai Unió felkészültté vált arra, hogy tagállamai kezébe olyan iránymutatásokat legyen képes adni, amelyek segítségével mind a tagállamok önállóan, mind pedig az Unió mint egész képes a kibertérben jelentkező fenyegetések hatékony kezelésére.

A tanulmány célja az, hogy felvázolja az európai szabályrendszer legfontosabb pilléreit, amelyek kijelölik a tagállami kötelezettségeket és mozgásteret saját kiberbiztonságuk megteremtéséhez. Terjedelmi korlátok miatt kizárólag az Európai Unió keretei között megalkotott jogforrásokat mutatom be és elemzem, a többi szervezet szabályrendszerével egy későbbi részben foglalkozok.

TÁRSADALMI HÁTTÉR

Az Európai Unió és az uniós polgárok egyre növekvő mértékben vannak kitéve a kibertérből származó fenyegetéseknek. Ráadásul, egyre gyakrabban válnak a térség és polgárai kiszemelt célponttá, köszönhetően többek között annak, hogy ez európai számítógépes infrastruktúra igen fejlett, a számítógépes hálózatok valamennyi szektort átszövik, az azokon tárolt adatok köre és mennyisége fokozatosan növekszik, mindez pedig vonzó terepet kínál a számítógépes bűnözőknek. Ezért *egyre fontosabbá és sürgetőbbé válik egy összehangolt, komplex európai szabályrendszer megalkotása*, amely a gyakorlatban kész szcenáriókat kínál az államoknak mind a kibertámadások megelőzéséhez, mind pedig a bekövetkezett akciók következményeinek hatékony és gyors kezeléséhez. Államok elszigetelt, önálló szabályrendszerének megalkotása már nem elegendő, hanem olyan közös európai – és elsősorban uniós – fellépésre van szükség, amely az országhatárokon átnyúló hálózat- és információbiztonsági fenyegetések és incidensek kezelésére képes, mert az ilyen akciók képesek lehetnek akár az Unió egészére is kihatással bírni. Mindez pedig a lakosság biztonságérzetének nagymértékű (további) csökkenéséhez vezethet, és *a kiberfenyegetések a migráció jelentette fenyegetéssel hasonló szintre kerülhetnek.* Ugyanakkor nem szabad figyelmen kívül hagyni azt sem, hogy a kibertér egy határokat nem ismerő, szabad mozgást lehetővé tevő globális tér – hasonlóan magához az Európai Unióhoz -, amely működésének egyik alappillére a személyek szabad mozgásának biztosítása. Ezért *elengedhetetlen egy közös, biztonságos európai kibertér létrehozása*, amely nemzeti, közösségi és nemzetközi szinten történő stratégiai és operatív együttműködés további fejlesztésével érhető el.

Nem túlzás, ha azt állítjuk, hogy az európai lakosság még nincs teljesen sem felkészülve, sem felkészítve a kibertérből származó veszélyekkel szemben. Az Eurobarométer által publikált, kifejezetten a kiberbiztonsággal foglalkozó felmérés érdekes képet fest az európai piacról. Bár az internethasználat tagállamonként igen eltérő,[1] az uniós polgárok átlag 63%-a napi szinten használja az internetet és mindössze 24% annak a kisebbségnek aránya, amely egyáltalán nem használja (ki) a világháló adta lehetőségeket.[2] [1] Egész Európa internethasználata még ennél is magasabb, 73%-os. [2] Ez a világátlag (50%) felett van, de ne felejtsük el, hogy igen elmaradt térségek adatai is részét képezik a felméréseknek. Az a

[1] Az északi államok e területen is élen járnak, kiemelten Norvégia, Svédország, Dánia és Hollandia (94-94%), míg a legelmaradottabb államok között tartják számon Romániát és Bulgáriát e vonatkozásában is (alig 50%-kal).

[2] Érdekesség, hogy a világhálót használók számaránya tekintetében Izland vezeti az államok listáját, 96%-kal.

„mindössze" kifejezés tehát természetesen igen relatív, mert az uniós polgárok 24%-a is összesen 121 millió lakost jelent, tehát koránt sem beszélhetünk egy kis létszámú csoportról.

Az internethasználók magatartása azonban fokozatosan közelít afelé, amit *biztonságtudatosnak* nevezhetünk: 60%-uk legalább évente megváltoztatja a jelszavát, 61%-uk használ vírusirtó programokat, 49%-uk megnyitás nélkül törli az ismeretlen feladótól származó e-maileket és személyes adataikat is sokkal óvatosabban szolgáltatják internetes felületeken. Talán ennek is köszönhető az internethasználók körében igen elterjedt azon (tév)hit, hogy képesek saját magukat hatékonyan megvédeni a kibertérben – bár ezt leginkább a fejlett államok polgárai gondolják ekképp.

A SZABÁLYOZÁS SAROKPONTJAI

A szabályozás szükségességét már maga az Unió is felismerte, és mintegy 10 évvel ezelőtt megkezdte kiberbiztonsága kereteinek kiépítését. Mivel az EU számos fenyegetést elsősorban civil oldalról közelít meg – így a kibertérben jelentkező fenyegetéseket is –, a hangsúlyt a szabad, nyílt internet megteremtésére helyezi, amelyet elsősorban a nemzetközi együttműködés kiszélesítése, valamint a szabályozók megalkotása révén kíván elérni.

A kiberbiztonságot néhány más szakterület már megelőzte a szabályalkotás terén. Itt utalok a terrorizmus elleni uniós szabályokra, amelyek elfogadására a 2001. szeptember 11-i események következtében került sor a 2000-es évek elején, majd ehhez kapcsolódva és ezzel párhuzamosan jelentkezett az igény a kritikus infrastruktúrák és az infokommunikációs hálózatok védelme iránt,[3] végül pedig mindezek folyománya volt a digitális egységes piac megteremtése érdekében tett lépések sora.

A szabályozás legmagasabb szintjét a stratégiai szint képezi. Az Unió 2003 decemberében fogadta el első *biztonsági stratégiáját*, amely „Egy biztonságos Európa egy jobb világban. Az Európai Biztonsági Stratégia" címet viseli. [6] A dokumentum felsorolja a globális és a konkrétan Európát fenyegető kihívásokat, amelyek között ugyan nevesítve nem szerepel a kiberfenyegetések köre, azonban a nemzetközi terrorizmus és a társadalmak sebezhetőségének kiemelésével már utal a kritikus infrastruktúrára. A stratégia felülvizsgálatának hosszas folyamatában mérföldkő volt a 2008 decemberében kiadott jelentés, amely a kiberbiztonságot már mint fő kihívást nevesítette. A jelentés utal a modern társadalmak kritikus infrastruktúrától való nagyfokú függésére, amely – többek között – az internet világát is érinti. A 2003-as stratégia átdolgozása egyre sürgetőbbé vált a globális környezet gyors és nagyfokú megváltozásának köszönhetően. Az államok digitális technológiáktól való függése drasztikusan megnövekedett és az Unió számára stratégia érdekké vált, hogy polgárai számára biztosítani tudja a mindenki számára biztonságosan hozzáférhető internetet. A stratégiaalkotás folyamata lassan haladt, az Európai Uniónak mintegy 13 évébe telt az új dokumentum elfogadása. 2016 nyarán „Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitika stratégiája" címmel

[3] Az első jelentős lépés a 2004-ben kiadott „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" című bizottsági közlemény volt, amelyben a kibertámadást és a kiberterrorizmust első alkalommal hivatalos uniós dokumentumban megemlítették – még ha „csak" a kritikus infrastruktúrákkal kapcsolatosan is. [3] Ezt követte a Bizottság által 2006-ban elfogadott program a kritikus infrastruktúrák védelmére vonatkozóan (EPCIP) [4], majd a program végrehajtására vonatkozó Zöld Könyv. 2008-ban előbb egy irányelvben összegezték a kritikus infrastruktúrák védelmének kapcsolatos előrelépési lehetőségeket [5], majd felállítottak egy, a kritikus infrastruktúrák védelméért felelős európai hálózatot (European Reference Network for Critical Infrastructure Protection – ERNCIP), melynek fő feladata a tagállamok közötti információ-megosztás és a kutatás elősegítése, elsősorban a kutatóközpontokon keresztül. (Jelenleg mintegy 140 intézmény segíti a hálózat munkáját).

jelent meg az unió új biztonsági stratégiája [7], amelyben a kiberterület már nevesítve és kiemelt helyen szerepel a kihívások kezelésére szánt eszközök és szakpolitikák között.[4]

Az első dokumentumot, amely kifejezetten az információs rendszerek védelmével kapcsolatos, *2009*-ben adta ki az Unió. A *Bizottság közleménye* „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló-képesség fokozása" címmel jelent meg. A dokumentum a hiányosságok között kiemeli, hogy uniós szinten a kibervédelmi gyakorlatok még kezdetleges szinten állnak és a több országot átölelő gyakorlatok is igen ritkák. Ezért hangsúlyozza a más, e területen kialakult gyakorlattal rendelkező szervezetekkel – kiemelten az ENSZ-szel, a NATO-val, az OECD-vel és a G8-cal – való együttműködés fontosságát. Előremutató megállapítása volt a közleménynek, hogy szükségesnek tartotta olyan nemzeti számítástechnikai katasztrófaelhárító csoportok felállítását,[5] amelyek mind a korai előrejelzés, mind pedig az incidenskezelés terén megfelelő képességekkel rendelkeznek. A 2009-es közleményben foglaltak *felülvizsgálatára 2013*-ban került sor. A bizottsági munkacsoport jelentésében [9] már különválasztotta a kritikus infrastruktúra védelmével kapcsolatos tevékenységeket, és azokat a *megelőzés - felkészülés - következménykezelés hármas kategóriájába* osztotta. A kezdeti célok megvalósításának határidejét 2014. második felében jelölte meg.

Az Európai Unió kiemelt területként kezeli a *digitális vívmányok biztonságos használatá*nak elősegítését. Ennek elérésére előbb két ötéves programot indított (2000-2005.[6] és 2005-2010.[7]), jelenleg pedig a harmadik program fut, tízéves futamidővel (2010-2020.[8]). Az első ötéves program három célt tűzött ki annak érdekében, hogy Európa valamennyi államában létrejöhessen az információs társadalom: olcsóbb, gyorsabb és biztonságosabb internet biztosítása; szakemberek képzése; valamint az internethasználat fellendítése. A második ötéves periódusra megfogalmazott célok már jóval komplexebbek voltak: egy egységes európai információs tér megteremtése; az infokommunikációs szektor és a kutatások kiemelt támogatása,[9] valamint egy összeurópai információs társadalom megteremtése. A jelenleg érvényben lévő *tízéves program* fő célja a kibertér biztonságos használatának megteremtése. A menetrend felvázolja az olyan európai hiányosságokat, mint az interoperabilitás hiánya, a digitális piac töredezettsége, a kiberbűnözés növekvő mértéke, a befektetések hiánya vagy a szakképzett munkaerő hiánya, majd valamennyi probléma vonatkozásában megoldásokat javasol. A cél az volna, hogy 2020-ra az európai polgárok a lehető legszélesebb körben és a lehető legbiztonságosabb keretek között élvezhessék a digitális technológia nyújtotta előnyöket.

A Digitális Menetrend meghirdetését követően fellendült a kibertér iránti érdeklődés, és ez az uniós dokumentumokban is megmutatkozott. *2012*-ben az *Európai Parlament határozatot* fogadott el „Kritikus információs infrastruktúra védelme: a globális kiberbiztonság megteremtése felé" címmel. [13] Bár a dokumentum a tagállamokat kötelezni nem tudta, mégis olyan javaslatokat fogalmazott meg, amelyek mára ténylegesen is megvalósultak az uniós országokban. Ezek között szerepelt például a nemzeti kiberbiztonsági stratégia megalkotása, a kibervédelmi veszélyhelyzeti tervezés, az önálló kibervédelmi

[4] Részletesebben a stratégia elemzését lásd: [8]
[5] Ezek lesznek később a hálózatbiztonsági reagáló csoportok, a CERT-ek.
[6] eEurope Action Plan [10].
[7] i2010 – European Information Society for growth and employment [11].
[8] Európai Digitális Menetrend [12]
[9] A szektor kiemelt támogatására azért volt szükség, mert Európa nagy elmaradásban volt a világ vezető államaihoz képest. Míg az Egyesült Államok esetében infokommunikációs szektor a K+F költségvetés 34%-ából részesült, Japán esetében pedig 35%-ból, addig az EU vonatkozásában ez mindössze 18% volt.

szervezetrendszer felállítása vagy a vonatkozó nemzeti jogszabályok megalkotása. Innen már csak egy lépcsőfok volt az uniós kiberbiztonsági stratégia megalkotása, amelyre a következő évben sor is került. Az Unió *2013*-ban kiadta átfogó *kiberbiztonsági stratégiáját* „Nyílt, biztonságos és megbízható kibertér - Az Európai Unió kiberbiztonsági stratégiája" címmel. [14] A stratégia bemutatása és elemzése önálló tanulmány tárgya lehetne, ezért ezen a ponton csak a stratégiában megfogalmazott prioritásokat emelem ki. Ezek a következők:

- kibertámadások megelőzéséhez, feltárásához és kezeléséhez szükséges képességek kifejlesztése;
- a kiberbűnözés nagymértékű visszaszorítása
- önálló kibervédelmi politika és képességek fejlesztése az Unió közös biztonság- és védelempolitikáján belül;
- a szükséges ipari és technológiai kapacitások és feltételek megteremtése;
- önálló, uniós szintű kiberpolitika mint szakpolitika létrehozása az EU alapértékei mentén.

A stratégia megalkotása igen jelentős lépés volt az Unió részéről, a lefektetett prioritások pedig nagy ívű célokat állítanak a szervezet elé, amelyek elérése még a jövő zenéje. Ugyanakkor a stratégia csak az európai infokommunikációs rendszerek meghibásodásának és ellenük intézett támadások megelőzésére és a válaszlépésekre vonatkozik, s még az olyan kérdések is megválaszolatlanok maradnak, mint például az, hogy a Lisszaboni szerződés záradéka alapján az Európai Unió mint egész hogyan reagáljon egyik tagállamát ért kibertámadás esetén.

A kiberbiztonsági stratégiához szorosan kapcsolódik a *2015*-ben kiadott *európai digitális egységes piaci stratégia*, amely az európai társadalom átalakításáról szól. Cél az európai egységes digitális piac megteremtése, amely számos előnnyel jár: többek között az európai GDP-t 415 milliárd euróval növelné és számtalan új munkalehetőséget kínálna. A Bizottság közleménye szerint szükséges volna jobb fogyasztói és vállalkozói hozzáférést biztosítani az internetes szolgáltatásokhoz és termékekhez, amely a bizalom erősödéséhez, az indokolatlan – területalapú – korlátozások megszüntetéséhez, a digitális tartalomhoz való hozzáférés javításához és az (adó)terhek csökkenéséhez is vezetne. Azonban a digitális tér kiépülésének egyik nagyon fontos előfeltétele az uniós polgárok bizalmának elnyerése. Ehhez szükséges a kiberbiztonsági kapacitások fejlesztése úgy, hogy azokat valamennyi tagállamban azonos kondíciókkal használhassák a lakosok.

A stratégia kiemeli, hogy a digitális gazdaság óriási mértékben növekszik. A növekedés mértéke a big data ágazat esetében eléri az évi 40%-ot, amely hétszer gyorsabb, mint az informatikai piac éves növekedési üteme.

Ez utóbbi megállapítás már előrevetítette az uniós jogalkotás *új irányát*. Hosszas, mintegy négyéves egyeztetést követően 2016-ban fogadtak el két korszakalkotó jelentőségű jogi normát, az adatvédelmi rendeletet (General Data Protection Regulation – GDPR rendelet) [15] és a NIS irányelvet (Directive on security of network and information systems) [16]. A tanulmány második felében e két jogforrást fogom értékelő-elemző módon ismertetni, mielőtt azonban erre rátérnék, az európai keretek alapjaihoz hozzátartozik a szervezetrendszer rövid bemutatása is.

SZERVEZETRENDSZER

A szervezetrendszer kiépítése már az 1990-es években megkezdődött, előbb tagállami, majd uniós szinten. Azok az államok jártak élen, amelyek a legfejlettebb információs rendszerekkel rendelkeztek, mivel a bűnözők a meglévő rendszereket kezdték el támadni a kibertérben, s ezen támadások ellen kellett megfelelően felkészülniük az államoknak szervezeti értelemben

is. Létrehozták a *hálózatbiztonsági reagáló csoportokat* (computer emergency response team – CERT), országonként más és más szervezeti felépítéssel. Mára valamennyi uniós tagállamban működnek CERT-ek kormányzati szinten, de több állam esetében ágazati CERT-ek is működnek, és az unós intézmények mellett is létrehoztak CERT-eket.[10]

Az uniós szintű építkezés alapköveként *2014*-ben hozták létre az *Európai Hálózat- és Információbiztonsági Ügynökséget* (European Network Information and Security Agency – *ENISA*), amely az Európai Unió, a tagállamok és a magánszektor közötti együttműködést segíti az információ-megosztás, a tagállamok közötti koordináció és tanácsadás területén. 2012 óta minden év októberében megszervezi az *Európai Kiberbiztonsági Hónap*ot, amely egy nemzetközi tudatosító kampánysorozat. Célja a kiberbiztonsági tudatosság növelése és a kiberfenyegetések mind szélesebb körben történő megismertetése. Ennek keretében a civil és akadémiai szféra, valamint az illetékes helyi szervek Európa-szerte mintegy 450 program közül választhatnak – 2016-ban Magyarország 22 programmal kapcsolódott az eseménysorozathoz.[11] Másik jelentős éves programja a *Cyber Europe* elnevezésű pán-európai kiberbiztonsági gyakorlat, amelyet 2016-ban negyedik alkalommal rendezett meg. Célterületei az informatika, a telekommunikáció és az információbiztonsági iparágak voltak, és konkrét technikai incidenseket kellett megoldaniuk a játékosoknak.

Tágabb értelemben a szervezetrendszer részét képezik egyrészt a kiberbűnözés elleni küzdelemmel foglalkozó szervezetek (élén 2013 óta az Európai Rendőrségi Hivatal szervezetén belül létrejött Számítástechnikai Bűnözés Elleni Küzdelem Európai Uniós Központjával), másrészt a kritikus infrastruktúra területén a Kritikus Infrastruktúra Figyelmeztető Információs Hálózat (Critical Infrastructure Warning Information Network – CIWIN) és a Kritikus Infrastruktúravédelmi Európai Referenciahálózat (ERNCIP).

Az Európai Unió maga is számos kezdeményezéssel támogatja az európai kiberbiztonság megvalósítását. Legnagyobb volumenű programja a *Horizon 2020 program [18],* amely az Unió történetének legnagyobb K+F financiális eszköze. Hétéves költségvetése 80 milliárd euró, amely további magánszektorbeli befektetésekre ösztönöz. Ilyen a 2016 nyarán bejelentett *kiberbiztonsági köz-magán társulás* létrehozása, amely 450 millió eurót fektet be az EU K+F tevékenységébe, s várhatóan 2020-ig ezen összeg bő háromszorosa, mintegy 1,8 milliárd euró értékű beruházás valósul meg. [19] A társulás célja az együttműködés elősegítése a kutatási és innovációs folyamat korai szakaszában, és kiberbiztonsági megoldások kidolgozása a különböző ágazatok – elsősorban az energiaipar, az egészségügy, a közlekedés és pénzügyi ágazat – számára. [20]

Végezetül megemlítem, hogy az Európai Unió számos nemzetközi szervezettel aktívan együttműködik a kiberbiztonság területét érintően (is). Kiemelendő az Európai Biztonsági és Együttműködési Szervezettel (OSCE), a Gazdasági Együttműködési és Fejlesztési Szervezettel (OECD) és az ENSZ szakosított intézményével, a Nemzetközi Telekommunikációs Unióval (ITU) kialakított együttműködés. Az együttműködés lényegi pontjainak ismertetése túlmutat jelen tanulmány keretein, azt külön kívánom bemutatni.

[10] 2012-ben felállították a Bizottság és a Tanács Főtitkársága, a Parlament és a Régiók Bizottsága közös CERT-jét is (CERT-EU).

[11] 2016-ban Az Európai Bankföderáció és az Europol Európai Kiberbűnözési Központja (E3C) is csatlakozott a rendezvényhez, mert ezúttal a kiemelt témák között szerepelt a bankolás biztonsága és a mobil eszközök kártevőinek problémaköre is. [17]

A NIS IRÁNYELV

Az Európai Unió évek óta azon dolgozik, hogy Európa kiberbiztonságát megerősítse és képes legyen garantálni. Az Uniót a lépések megtételére olyan események késztették, mint például az Észtországot 2007-ben ért igen átfogó kibertámadás, az ukrán elektromos hálózat megbénítása 2015-ben vagy a kórházi rendszerek állandó megfertőzése különböző (zsaroló)vírusokkal. 2015-ben például globálisan 38%-kal több kiberbiztonságot érintő incidenst jelentettek, mint a megelőző esztendőben, és becslések szerint csak az Unióban évente 260-340 milliárd eurós kár keletkezik ilyen eseményekből. [21]

A jogalkotási folyamat az Unióra jellemző komótos tempóban haladt az utóbbi években, de 2016-ra már kézzelfogható eredményeket sikerült felmutatnia.[12] Ezek a szabályozások hiánypótlóak, mert ezidáig nem létezett olyan uniós szintű egységes szabályrendszer, amely valamennyi tagállamra vonatkozóan kötelező előírásokat tartalmazott volna. Ehelyett a tagállamok a saját érdekeik mentén maguk szabályozták ezt a támadásoknak egyre inkább kitett speciális területet, amely az európai információs piac felaprózódásához és az állampolgárok kiszolgáltatottá tételéhez vezetett. Márpedig manapság nem csak a szolgáltatások nem ismernek országhatárokat, de a bekövetkezett információbiztonsági események is kihat(hat)nak az Unió egészére, ezért a közös uniós fellépés ezen a területen igen indokolt.

Az így kialakuló egységes európai szabályozás egyik pillére a *2016*. július 6-án az Európai Parlament által jóváhagyott (és augusztus 8-án hatályba lépett) *Irányelv a hálózati és információs rendszerek biztonságáról* (Directive concerning measures for a high common level of security of network and information systems across the Union – a továbbiakban: NIS irányelv). [16] Ez az első olyan, uniós szintű kiberbiztonsági szabályozás, amely képes lehet megakadályozni az európai infrastruktúra elleni kibertámadásokat. Az irányelv fő célja a nemzeti szabályok közös nevezőre hozása úgy, hogy kötelező biztonsági minimumokat ír elő valamennyi tagállam számára, s ehhez közös intézményi rendszert és szabályozást bevezetését írja elő.

Az irányelv *alanyi hatálya* kettős: az alapvető szolgáltatást nyújtók köre (azaz a kritikus infrastruktúra) és a digitális szolgáltatás nyújtó köre, vagyis akik ellen intézett támadás a legközvetlenebbül képes kihatni a lakosságra. Az első csoportba tartozók körét a tagállamok olyan kritériumok alapján határozzák meg, hogy a nyújtott szolgáltatás társadalmi vagy gazdasági szempontból alapvetőnek minősíthető-e, a szolgáltatás nyújtása hálózati és információs rendszerektől függ-e és egy esetleges incidens képes-e zavart okozni a szolgáltatás nyújtásában (5. cikk (2) bek.). Ezek alapján ide sorolhatók például az ivóvízellátó cégek, az energiavállalatok, a közlekedési vállalatok, az egészségügyi szolgáltatók, a banki szolgáltatást nyújtók vagy a digitális infrastruktúrák. Természetesen, ha egy kiberbiztonsági incidens egy ilyen vállalatot érint, de a támadás például csak a kommunikációs részlegére hat ki és az alapvető szolgáltatás nyújtását nem befolyásolja, akkor ez nem esik az irányelv hatálya alá. Ugyanakkor egy biztonsági esemény hatásának vizsgálatánál mindig alapvető

[12] A NIS irányelv esetében például már 2013-ban megszületett az első javaslat (2013/0027 (COD). A távközléssel és az információs társadalommal foglalkozó munkacsoport (WP TELE) előkészítő munkáját követően az Európai Unió Tanácsa 2013. július 6-án irányadó vitát folytatott le az irányelvtervezetről. A TTE Tanács előbb 2013. december 5-i ülésén, majd 2014. június 6-i ülésén vitatta meg az addigi eredményekről szóló jelentéseket. 2014 végén és 2015. április 30-án háromoldalú egyeztetésre került sor a Tanáccsal és a Parlamenttel, de még ekkor is lényegi különbségek voltak a két fő szerv álláspontja között. Végül 2015. június 29-re sikerült megállapodniuk az alapelvekről, amelyek már bekerültek a az irányelvtervezetbe. 2015. december 18-án pedig a COREPER közbenjárásával rögzítették az informális megállapodás főbb pontjait. [22] [23] [24].

szempontok, hogy a szolgáltatás kimaradása hány embert érint, mennyi ideig tart és földrajzi értelemben mennyire kiterjedt.

Az alanyi kör másik csoportjába azok a digitális szolgáltatók tartoznak, amelyek fontos, de nem nélkülözhetetlen szolgáltatásokat nyújtanak. Ilyenek például a kereső- és felhőszolgáltatók vagy az online piacterek. A szolgáltatásnyújtók köre nem korlátozódik az Unió területére, a lényeg, hogy a szolgáltatás nyújtására az EU területén kerüljön sor. Így olyan nagy világcégekre is kiterjed az irányelv hatálya, mint például a Google, az Amazon vagy az eBay. Ugyanakkor érdemes megemlíteni, hogy bár az irányelv korábbi tervezetében szerepelt, a végleges szövegből mégis kikerült a közösségi szolgáltatást nyújtók köre, tehát például a Facebook-ra nem vonatkoznak az irányelvben lefektetett szabályok.

Az irányelv mindkét alanyi kör számára vonatkozóan előír két kötelezettséget: egyrészt olyan hálózat- és rendszerbiztonságot kell garantálniuk, amely a rájuk leselkedő kockázatokkal arányos mértékű, másrészt pedig az illetékes hatóságok felé incidens-bejelentési kötelezettségük is van. Az alapvető szolgáltatást nyújtók esetében ezen felül további biztonsági garancia, hogy a tagállami hatóságok ellenőrizhetik, hogy a szolgáltatásnyújtók milyen biztonsági lépések megtételét tervezik és ezeket ténylegesen is valósítják-e.

A tagállamoknak valamennyi, az irányelvben szereplő kötelezettségnek 2018 májusáig eleget kell tenniük. Összegezve az irányelvben előírt legfontosabb előírásokat, azok a következők:

- Minden tagállamnak meg kell alkotnia a saját hálózat-és információbiztonsági stratégiáját.
- Minden tagállamban fel kell állítani egy, a számítógép-biztonsági eseményekre szakszerűen válaszolni képes gyorsreagálású kibervédelmi szakértői csapatot, ún. CSIRT-et (Computer Security Incident Response Team).[13] (Magyarország e kötelezettségnek már korábban eleget tett.)[14]
- A nemzeti CSIRT-ekből fel kell állítani egy uniós CSIRT-hálózatot, amelynek kötelezően valamennyi tagja lesz valamennyi CSIRT.
- Uniós szinten is létre kell hozni egy olyan Együttműködési Csoportot (Contact Group), amely a nemzeti hatóságok és CSIRT-ekből felépülő CSIRT-hálózat közötti stratégiai együttműködést támogatja és segíti. Ezzel az irányelv az első olyan közösségi szabályozás, amely kötelező együttműködést ír elő a (nemzeti) intézmények számára.[15] Ennek azonban előfeltétele a tagállamok közötti bizalom kiépülése, amelynek idő kell.
- Az irányelv átültetésére és végrehajtására ki kell jelölniük egy nemzeti hatóságot.
- Szektoronként pontosítani kell azon kritériumokat, amely alapján egy vállalat az irányelv hatálya alá tartozik, majd a szolgáltatói kört nevesíteni kell. Ezt a

[13] Elterjedt a CERT kifejezés használata is (Computer Emergency Response Team). A kettő mára szinonimává vált; az EU-ban inkább a CSIRT, Magyarországon inkább a CERT kifejezést használják. Az eltérés oka abban keresendő, hogy a CERT kifejezés mára speciális szellemi tulajdonjogi védelem alá esik.

[14] Bár az irányelv alapján tagállamonként csak egy CSIRT felállítása kötelező, de lehetőség van arra is, hogy akár valamennyi szektorban létrehozzanak ilyen szakértői csoportokat. Magyarországon már jelenleg is több ilyen reagáló csoport működik. A kormányzati rendszerek védelmében a GovCERT, a Honvédelmi Minisztériumnál a MilCERT jött létre, de önkéntes alapon a kormányzati szektoron kívül működő HunCERT az internetszolgáltatók, a NIIF CSIRT pedig az oktatási - kutatási - közgyűjteményi intézmények eseménykezelését végzi.

[15] Ezt megelőzően önkéntes és erősen bizalmi alapon zajlott az együttműködés az illetékes tagállami szervek között.

tagállamoknak 2018 novemberéig kell megtenniük. (A kritikus ágazatokban működő mikro- és kisvállalatokra ezen előírások nem vonatkoznak.)

A szabályozás részleteinek kidolgozására és az irányelv által nevesített feladatok végrehajtására az Európai Bizottság 2016 májusában felállított egy szakértői csoportot valamennyi tagállam részvételével (Magyarországot a Nemzeti Kibervédelmi Intézet képviseli).

Az irányelv 25. cikke értelmében a rendelkezéseket valamennyi tagállamnak át kell ültetnie a nemzeti jogába. Az átültetési határidő 2018. május 9-e. Az elfogadott és kihirdetett főbb törvényi, rendeleti és közigazgatási rendelkezések szövegét pedig valamennyi tagállam köteles a Bizottsággal közölni.

Az irányelv rendelkezik a szabályozás ellenőrzésének menetéről is. A 23. cikk értelmében a Bizottság feladata, hogy értékelje a tagállamok alapvető szolgáltatásokat nyújtó szereplők azonosítására vonatkozó kötelezettségének teljesítését. Ezt 2019. május 9-ig jelentés formájában kell megtennie, amely elfogadásáról a Parlament és a Tanács dönt.

A GDPR

Az újonnan kialakuló egységes európai szabályozás második pillére az Unió általános *adatvédelmi rendelete* (General Data Protection Regulation, a továbbiakban: GDPR).[16] A korábbi adatvédelmi irányelvet[17] még 1995-ben fogadták el az Unióban, éppen a digitális kor hajnalán, ezért az abban foglalt szabályokat az elmúlt húsz év alatt meghaladta az idő, és azok hol elégtelennek bizonyultak az újszerű problémák megoldásához, hol túl tág mozgásteret adtak a tagállamoknak. A legnagyobb probléma mégis az volt, hogy az irányelv nem tudta elérni azon célját, hogy a tagállami szabályozásokat közös nevezőre hozza, így *mára 28 különféle adatvédelmi szabályozás jött létre az Unión belül.* Ez azzal járt, hogy a felhasználók egészen más védelemben részesülnek az egyik tagállamban, mint adatfeldolgozás helyén, mint egy másik országban. Többek között ezt a helyzetet hivatott orvosolni az új szabályozás, amelyet egy hosszas, mintegy négy éves előkészítő munka előzött meg. A Bizottság már 2012-ben útjára indította a reformkezdeményezést, amely az EU főszervei között létrejött kompromisszumot követően nyerte el végleges formáját. A rendelet legnagyobb jelentősége ezért abban rejlik, hogy az Unió *igen nagy lépést tehet a digitális egységes piac kialakulása felé.*

Az új szabályozás két elemből épül fel: az egyik a már említett GDPR, a másik pedig az új adatvédelmi irányelv, amely a rendőri és bűnüldöző szervek adatkezelésére vonatkozóan tartalmaz előírásokat. A továbbiakban csak röviden ismertetem a GDPR legfontosabb szabályait.

Az Európai Parlament 2016. május 4-án fogadta el a rendeletet, amely a kihirdetést követő 20. napon lép hatályba, ténylegesen azonban csak *2018. május 25-től kezdve kell alkalmazni*. A tagállamoknak és a vállalatoknak tehát két évük van a felkészülésre, amely bár első ránézésre hosszú időnek tűnhet, valójában azonban még a legfelkészültebbeknek is sok tennivalójuk van hátra.

---

[16] *Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről*

[17] 95/46/EC irányelv

A rendelet *tárgyi hatálya* minden olyan adatra kiterjed, amely természetes személyt azonosít, vagy amely által természetes személy azonosítható. Ennek értelmében egyes online adatkategóriák is személyes adatnak minősülhetnek, így például a cookie ID-k, az IP-címek[18] vagy az online azonosítók. A különleges adatokra továbbra is szigorúbb szabályok vonatkoznak (kezelésükre csak az érintett kifejezett hozzájárulásával van lehetőség), és ezen adatok köre is tovább bővült *a genetikai és biometrikus* adatokkal.

A rendelet – jogforrási mivoltából fakadóan – közvetlenül alkalmazandó és valamennyi tagállamra vonatkozóan állapít meg kötelezettségeket, amely már önmagában jelzi a szabályozás fontosságát. A rendelet *személyi hatálya* azon vállalatokra is kiterjed, amelyek bár az Unión kívül működnek, tevékenységük azonban érinti az uniós polgárok személyes adatait. Ugyanakkor könnyít a szabályozás a tekintetben, hogy azon vállalatoknak, amelyek több tagállamban rendelkeznek leányvállalattal, már csak egy, a központi ügyintézés helye szerinti hatóság felé kell eljárniuk.[19] További jelentős változás, hogy a rendelet már nem csak az adatkezelőkre, hanem az ő megbízásukból eljáró adatfeldolgozókra is előír kötelezettségeket.

A GDPR tehát vonatkozik olyan, Unión kívüli vállalatokra is, amelyek Európán kívül végeznek adatkezelést. Esetükben elsősorban az adatok továbbítása lehet problémás. A rendelet alapján harmadik országba csak akkor továbbítható adat, ha az adatok megfelelő szintű védelme a célországban is biztosított. Ennek igazolására három lehetőség kínálkozik:

- A Bizottság ezt egy ún. megfelelőségi határozatban deklarálja.[20] [27]
- Egyes vállalatok kialakult adatkezelési gyakorlata is igazolhatja az adatok megfelelő szintű védelmét. A gyakorlatot a cégek a Bizottsággal kötendő modellszerződésekkel tudják szentesíteni, amelyek lényegében általános szerződési feltételek vállalását jelentik.[21] [28]
- Végül megoldás lehet a kötelező érvényű vállalati szabályok (BCR) bevezetése is. [29] Ez a cégcsoporton belüli adattovábbítást teszi lehetővé különböző államok között.

A rendelet értelmében súlyos szankciókkal sújthatók az előírásokat megszegő vállalatok. A felügyeleti hatóságok által kiszabható pénzbüntetés mértéke attól függ, hogy a rendelet mely rendelkezését sértette meg a szolgáltató. Ez legalább a vállalat előző évi *globális árbevételének 2%-a*, de legsúlyosabb esetben a bírság elérheti a 4%-ot is.[22] Emellett a vállalatnak igen szigorú átláthatósági követelményeknek is meg kell felelniük és a tájékoztatási kötelezettséggel kapcsolatos eljárások is jelentősen szigorodnak. Részletesen szabályozták továbbá, hogy adatkezelési incidens esetén a cégeknek hogyan kell eljárniuk a felügyeleti hatóságok és az érintettek felé. A hatóságokat[23] 72 órán belül értesíteni kell, az érintetteket azonban csak akkor, ha az incidens minden valószínűség szerint magas kockázattal jár rájuk nézve.

---

[18] Az IP-címek személyes adat jellegével kapcsolatos jelenlegi bizonytalanságokat olyan és ahhoz hasonló eseti döntések szüntethetik meg, mint például az Európai Unió Bíróságának döntése a Breyer v. Németország ügyben. [25]

[19] A Bizottság becslése szerint ezzel évente 2,3 milliárd eurót lehet megtakarítani. [26]

[20] Ilyen jelenleg 11 nem uniós terület esetében létezik és ilyen volt a Safe Harbor egyezmény is az Egyesült Államokkal (amelyet hatályon kívül helyezését követően a Privacy Shield váltott fel 2016 júliusában).

[21] Ezen megoldás hátránya, hogy a cégek számára nem biztosít mozgásteret és sok leányvállalattal rendelkező cégek esetében az adminisztratív teher nagyon megnövekedhet.

[22] A kiszabható pénzbírság mértéke tehát jóval magasabb, mint a Magyarországon maximálisan kiszabható 20 millió forint.

[23] Magyarországon a kijelölt hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóságát (NAIH).

Végül megemlítem, hogy a rendelet az *érintettek jogait* jelentős mértékben kiszélesítette. Az új szabályozás változatlanul biztosítja az érintettek számára a tájékoztatáshoz és a helyesbítéshez való jogot (azzal, hogy ezeket csak ésszerű határok között érvényesíthetik, amely az adatkezelőket védő klauzula), ugyanakkor a jogosultságok listája jelentősen kibővült. Az egyik legfontosabb a felejtéshez való jog, amely az érintett személyes adat törlése iránti kérelmét jelenti – bár ez nem abszolút jog, mert más jogalappal az adatkezelő tovább kezelheti az adatokat. Emellett az érintettnek joga van tiltakozni egyes adatkezelések ellen. Bár ez önmagában szintén nem abszolút jog, de a direkt marketing célú adatkezelések elleni tiltakozást viszont már abszolút jogként rögzítették. Az érintetteknek joga van adatai hordozására is, tehát kérésére az egyik szolgáltató köteles átadni a személyes adatait a másik szolgáltatónak. Ezen jog gyakorlati működése azonban igen kérdéses.

A rendelet az adatvédelmi szabályok érvényre juttatását is forradalmasítani kívánja, mégpedig oly módon, hogy az „egyablakos ügyintézés” megvalósítására felállítja az *Európai Adatvédelmi Tanács*ot (European Data Protection Board, EDPB). A Tanács a kijelölt tagállami hatóságok egy-egy képviselőjéből fog állni, és működésében szavazati jog nélkül részt vesz majd az Európai Bizottság képviselője is. Feladata alapvetően véleményalkotás lesz egyedi ügyek vonatkozásában.

A NIS IRÁNYELV ÉS A GDPR RENDELET KÖZÖTTI LEGFŐBB KÜLÖNBSÉGEK

Bár első ránézésre a két jogforrás nagyon hasonlónak tűnhet, ugyanis mind a kettő biztonsági előírásokat ír elő a tagállamok számára és incidens-bejelentési kötelezettséget rögzít számukra, azonban a két jogi norma más irányból közelíti meg az információbiztonság témakörét. A különbségek az alábbiakban ragadhatók meg [30]:

- A GDPR rendelet középpontjában a felhasználó mint egyén áll, mert a szabályozás célja a személyes adatok és a magánszféra védelme. Ezzel szemben a NIS irányelvben foglaltak a szolgáltatókat célozzák meg és a hálózatvédelemre helyeződik a hangsúly.
- Míg a GDPR valamennyi olyan vállalatra vonatkozik, amely az unió polgárainak személyes adatait kezeli, addig a NIS irányelv csak a legfontosabb szolgáltatókra vonatkozóan ír elő kötelezettségeket.
- Az incidens-bejelentési kötelezettség terén különbség, hogy a GDPR esetében olyan biztonsági eseményeket kell bejelenteni, amelyeknél személyes adat sérül(het), a NIS esetében pedig azokat, amelyeknél az adott szolgáltatás kerül veszélybe.

Az értesítési kötelezettség tekintetében különbség, hogy személyes adat sérelme esetében az adott cégnek közvetlenül az érintett felhasználót kell értesítenie, míg a NIS hatálya alá tartozó szolgáltatásnyújtóknak a felügyelő hatóság felé kell bejelentést tenniük, de csak a jelentős hatásúnak minősülő hálózati incidensek esetében

KÖVETKEZTETÉSEK

Az Európai Unió az elmúlt években igen jelentős lépéseket tett az európai digitális piac megteremtése felé. A megalkotott szabályok hiánypótlóak, mert korábban nem léteztek minden tagállamra vonatkozó, kötelező és egységes szabályok a kiberbiztonság területén. Az Unió intézkedései a kiberbiztonság megteremtése érdekében egyre határozottabb formát öltenek, az Európai Digitális Menetrendben megfogalmazott lépések sorra valósulnak meg és a Kiberbiztonsági Stratégia alapján elkezdett felépülni az uniós kibervédelem intézmény- és szabályrendszere. Az a jövő kérdése, hogy ezek a szabályok képesek-e elérni a céljukat és az uniós kibertér megfelelően védetté válhat-e. Szintén nyitott kérdés az olyan új technológiák, mint a Dolgok Internete (Internet of Things – IoT) és az okos eszközök hálózata, amelyek

által kezelt adatok mennyisége és minősége is jelentősen változhat a jövőben, és ez újabb biztonsági kockázatot rejt magában.

FELHASZNÁLT IRODALOM

[1] Global internet map http://www.internetsociety.org/map/global-internet-report/?gclid=CjwKEAiA79zDBRCgyf2FgeiY-CESJABzr0BMDdAMYfp2IUkRws20s3cTN5sV-SKnzy6Mr5aju1ATVRoCRu3w_wcB#global-internet-penetration 2016. 12. 05.

[2] http://www.internetworldstats.com/stats.htm 2016. 12. 05.

[3] A Bizottság közleménye a Tanács és az Európai Parlament részére – A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben. http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52004DC0702, 2016. 12. 05.

[4] EPCIP - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF, 2016. 12. 05.

[5] A kritikus infrastruktúrák védelmének kapcsolatos előrelépési lehetőségeket – Tanács 2008/117/EC irányelve (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, 2016. 12. 05.

[6] Az Európai Biztonsági Stratégia https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf, 2016. 12. 05.

[7] Az EU globális kül- és biztonságpolitika stratégiája – 2016 https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf, 2016. 12. 05.

[8] MOLNÁR, ANNA: Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája. Nemzet és biztonság, 2016/2. szám 75-85. oldal

[9] Bizottsági munkacsoport jelentése – 2013.08.28., https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf, 2016. 12. 05.

[10] eEurope Action Plan http://ec.europa.eu/idabc/en/document/70/5849.html, 2016. 12. 05.

[11] i2010 – European Information Society for growth and employment http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF, 2016. 12. 05.

[12] Európai Digitális Menetrend - http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R(01), 2016. 12. 05.

[13] Az Európai Parlament határozata – „Kritikus információs infrastruktúra védelme: a globális kiberbiztonság megteremtése felé” http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1479216690655&uri=CELEX:52012IP0237, 2016. 12. 05.

[14] Az Európai Unió kiberbiztonsági stratégiája http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu, 2016. 12. 05.

[15] GDPR – általános adatvédelmi rendelet http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, 2016. 12. 05.

[16] NIS – hálózat-és információbiztonsági irányelv https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, 2016. 12. 05.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, 2017. 01. 16.

[17] Európai Kiberbiztonsági Hónap http://www.cert-hungary.hu/kiberhonap, 2016. 12. 05.

[18] Horizon 2020 https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020, 2016. 12. 05.

[19] Kiberbiztonság: 1,8 milliárd eurót „mozdítana meg" az Európai Bizottság. 2016. július 5. http://kamaraonline.hu/cikk/kiberbiztonsag-18-milliard-eurot-mozditana-meg-az-europai-bizottsag, 2016. 12. 05.

[20] Nagy pofont kapnak a kiberbűnözők. 2016. július 5. http://www.napi.hu/nemzetkozi_gazdasag/nagy_pofont_kapnak_a_kiberbunozok.617292.html, 2016. 12. 05.

[21] SÁGI, Gyöngyi: Közelebb jutottunk a kiberbiztonság egységes uniós szabályozásához. 2016. január 18. http://bitport.hu/ujabb-akadalyt-vett-sikerrel-az-unios-kiberbiztonsagi-torveny-tervezete, 2017. 01. 16.

[22] A kiberbiztonság javítása az Európai Unióban http://www.consilium.europa.eu/hu/policies/cyber-security/, 2016. 11. 07.

[23] Hálózat- és információbiztonság: áttörés a Tanács és a Parlament közötti tárgyalásokban. http://www.consilium.europa.eu/hu/press/press-releases/2015/06/29-network-information-security, 2016. 11. 07.

[24] EU steps up cyber security: member states approve agreement. http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement, 2016. 11. 07.

[25] Európai Unió Bírósága: Breyer v. Németország ügy. http://curia.europa.eu/juris/liste.jsf?td=ALL&language=hu&jur=C,T,F&num=C-582/14 2017. 01. 16.

[26] GÁLFFY, Csaba: Itt az EU új adatvédelmi keretrendszere. 2015. december 16. http://www.hwsw.hu/hirek/54917/eu-adatvedelem-szabalyozas-keretrendszer.html 2017. 01. 16.

[27] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm 2017. 01. 17.

[28] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm 2017. 01. 17.

[29] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm 2017. 01. 17.

[30] BOLCSÓ, Dániel: Európa készül a kiberháborúra. 2016. augusztus 8. http://index.hu/tech/2016/08/08/europa_kiberbiztonsag_halozatvedelem_nis_iranyelv/ 2016.11.07.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

INTEGRÁLT FELÜGYELETI RENDSZER

INTEGRATED MONITORING SYSTEM

PUSKÁS Béla

(ORCID: 0000-0001-6211-7579)

pb@pbnet.hu

Absztrakt

A kritikus informatikai infrastruktúrák egy összetett hálózatot alkotnak napjainkban. Emiatt is egyre fontosabbá vált alaposan megismerni és dokumentálni a rendszerelemeket, azok hatásait, kapcsolatrendszerét. Fel kell ismerni, hogy minden egyes fizikai és logikai elem hatással van egymásra, amelynek feltérképezése fontos a rendszerüzemeltetés szempontjából. Ennek egyik legfontosabb része az adatok összegyűjtése és azok rendszerezése.

Kulcsszavak: *Hálózati struktúra, Kritikus Infrastruktúra, Kritikus Információs Infrastruktúra, Szolgáltatásmenedzsment, Konfigurációmenedzsment*

Abstract

The Critical Information Infrastructures has become a complex network. Consequently, the items of the system, their mutual effects and links and the map of the network have to be known properly. We have to realize that everything is linked with each other and the physical and logical networks have mutual effects on each other as well. It is obvious, that the problem of mapping the complexity is very important. One of the most important part of the cognition is the obtainment and sorting of information.

Keywords: *Structure of networks, Critical Infrastructures, Critical Information Infrastructures, Service Management, Configuration Management*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.09.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.01.)

BEVEZETÉS

Neumann János 1945-ben közzétette a nevéhez fűződő Neumann-elv leírását a „First Draft of a Report on the EDVAC" művében. [1] A mai napig ezen elvek alapján épülnek fel a számítógépek, és ezen eszközök a központi részei az informatikai rendszereknek. Az elv segítségével kapcsolat épült ki az ember által betáplált adat és az elektronikus gép közt. A bevitt vagy mentett adatokon a gépben tárolt program meghatározott műveletet hajt végre, melynek eredményeképpen a kimeneten újabb adat jelenik meg, amit akár újból lementhetünk. Ez már nem csak egy célhardver, hanem egy univerzális felhasználhatóságot elősegítő szerkezeté vált. Kezdetben önálló és egyszerű felépítésű szerkezet volt, mára azonban világméretű hálózat épült ki a gépekből, amelynek a koordinálása szinte lehetetlen. Neumann már 1948-ban a Hixon Symposiumon tartott előadásában feltette a kérdést, amely a mai napig komoly kihívást okoz az informatikai rendszereket tervezését és üzemeltetetését végző személyek számára.

AZ INTEGRÁLT FELÜGYELETI RENDSZER

„Lehet-e megbízhatatlan szerkezeti elemekből megbízhatóan működő automatákat építeni?" [2, 50. o.]

A Hixon Symposiumon tartott előadások leginkább a számítógépek megbízhatóságával foglalkoztak, de ma már az összetettebb rendszerekkel kapcsolatban még inkább felmerülő kérdésé vált. A számítógépeket felépítő elektronikai alkatrészek nem örök életűek és bár statisztikai adatok rendelkezésünkre állnak, de azt, hogy mikor melyik alkatrész fog meghibásodni nem tudhatjuk. A hibamentes működést elősegíthetjük az ideális közeli környezet kialakításával, a rendszer *„hibatűrő"* kialakításával, a folyamatok szabályzásával, stb. Azt szokták vizsgálni, hogy egy rendszerelem meghibásodása milyen hatással van a rendszer egészének működésére. Azonban ez egy kezdetleges számítógép esetében sem volt egyszerű nemhogy egy adatközpont, vagy összekapcsolt adatközpontok esetében. Egy váratlan vagy nem kívánt esemény hatásának csökkentése az ugyanolyan feladatot végző rendszerelemek párhuzamos üzemeltetésével, különböző technológiák, gyártók bevonásával, de független energia-szolgáltatókkal, telekommunikációs cégekkel történő szerződéssel is elősegíthető. Természetesen a költségek és az adminisztrációs többletfeladatok miatt mérlegelni kell mikor éri meg ez. Hibás működésből adódó becsült veszteség és a befektetett költségnek összhangban kell lenni. A rendszerünknek robusztusnak és alkalmazkodónak kell lennie, csillapítva ezáltal a nem kívánt hatásokat. Ez azt jelenti, hogy a hibákat részben elnyeli vagy késlelteti azok kimenet hatását. Diverznek tekinthető a rendszerünk, ha a rendszerelemeket, bemeneti forrásokat, technológiákat párhuzamosan alkalmazzuk.

A természetben megfigyelhető jelenségeket, mint az öngyógyítást több dolog miatt is nehéz megvalósítani egy ember által épített és kézben tartott rendszernél. Egyrészt olyan mértékű túlbiztosításra és kapcsolati rendszerre lenne szükség, amely már túlzott mértékben megdrágítaná a rendszerünket, másrészt pedig folyamatos kontroll alatt akarjuk tartani a rendszerünket (legalábbis ma még ez a cél) és nem engedhetjük saját életet élni, ill. ma még nincs is rá módunk. Véleményem szerint ma egyre inkább fontosabb Neumann megállapítása, amely azt mondja:

„… valamely szerkezet működési biztonságát nemcsak technikai eszközökkel, hanem lényegében véve szervezési eszközökkel is növelni lehet." [1]

[1] Idézet: Neumann János: A számológép és az agy. [2]

A szervezési és irányítási eszközöket segíti, ha a vállalatnál létrehozunk egy konfigurációkezelő rendszert. Az angol elnevezése többet mond, mint a magyar fordítás, így a továbbiakban az eredeti angol elnevezést CMS (Configuration Management System) használom. Az ITIL3[2] megfogalmazás szerint a CMS egy szoftver, amely képes kezelni az informatikai szolgáltatásokat biztosító összetevők és a köztük lévő kapcsolatok konfigurációját. Magába foglalja továbbá az incidenskezelést, problémamenedzsment, tudásmenedzsment, változáskövetést, erőforrás-kezelést és dokumentumkezelést, valamint ezek kapcsolatrendszerének kezelését. Az alapadatok szintén tartalmazzák a rendszerrel kapcsolatba kerülő személyek, helyszínek, erőforrások, üzleti folyamatok és a környezet leírását. Azonban a CMS nem egyenlő a CMDB[3]-vel.

A CMDB naprakészségéért a konfigurációmenedzser a felelős, aki a konfigurációmenedzsmenten keresztül, azok irányításával hajtja végre a feladatot. Egy jó CMDB-ét azonban az IT rendszert üzemeltető valamennyi személy, szolgáltatásmenedzsment használja. Két dolog miatt is fontos ez. Egyrészt ha mindenki ezt használja, akkor nem fognak kialakulni szigeteket alkotó önálló adatbázisok, nyilvántartások, amelyek átfedéseket, eltérések tartalmazhatnak az üzemeltető egységek közt. A másik fontos szempont, hogy az adatbázist mindenkinek magának kell éreznie, mert csak így biztosítható, hogy a személyzet folyamatosan karbantartsa az adatbázist, aminek ez a naprakészség legkritikusabb pontja. Amennyiben elhanyagolják a folyamatos adatkarbantartást az adatbázis rövid időn belül használhatatlanná válik. Minden szereplőnek úgy kell érezni, hogy az adatbázis az ő érdekeit szolgálja, ezért érdemesnek, sőt kifejezetten hasznosnak érzik azt karbantartani. Olyan megjelenítő felületeket kell alkalmazni, amelyek az egyes szinteknek megfelelő, a számára leglogikusabb és hasznosabb információkat közöl. Ösztönzőleg hathat, ha a felső vezetők is kapnak összefoglaló információkat, így ezek elmaradása, a téves adatok kérdéseket szülhetnek. Ahogyan a CMS nem egyelő a CMDB-vel, úgy a CMS sem egyenlő a feltérképező szoftverek által biztosított adatokkal. Az csak egy kisegítő eszköz, amely leginkább az auditálásra szolgál. Hasonlóan nem keverhető össze a hálózatfelügyeleti és rendszerfelügyeleti eszközök, szoftverek által szolgáltatott adatok nyilvántartása, tárolása. Ezek az alrendszerek a CMS rendszer részét kell, hogy képezzék, de nem válthatják ki egymást. Fontosnak tartom, hogy a CMDB magját azok az adatok alkossák, amelyek a jóváhagyási mechanizmus után kerülnek be. Ebből következik, hogy a rendszer részét kell képezze egy munkafolyamat leírás, amelyet a szolgáltatást biztosító személyek mindegyikének be kell tartani. A rendszerbe kerülő elemek adatait az egész életútjuk alatt nyilván kell tartani. A változásoknál a régi adatokat nem szabad törölni, azokat archiválni kell a későbbi kereshetőség érdekében.

Nagyon érdekes kérdés és problémakör, hogy egy rendszerelem (ITIL-ben konfigurációs elem[4]) mennyi tulajdonságát kell rögzíteni. Természetesen ennek meghatározása a rendszer kialakításakor kell, hogy megtörténjen. A mélységében és szélességében is vizsgálható a kérdés. Mélység alatt értem, hogy mennyire kell részleteiben vizsgálni egy eszközt. Például kell-e, tud-e hosszútávon információt adni egy Routerben lévő kondenzátor, tekercs típusa, gyártmánya, stb. Kell-e nekünk az őrzésvédelmi rendszereket alkotó kameráit gyártó cég tulajdonosi szerkezetét vizsgálni?

[2] ITIL (IT Infrastructure Library): Az IT-szolgáltatásmenedzsment számára jól bevált gyakorlatot leíró útmutatók gyűjteménye. Az ITIL tulajdonosa az OGC, és olyan kiadványok sorozata, amely minőségi IT-szolgáltatások nyújtására ad útmutatást, valamint a támogatásukhoz szükséges folyamatokra, és létesítményekre. További információért ld. http://www.itil.co.uk/. [5]

[3] CMDB: Konfiguráció Management Adatbázis

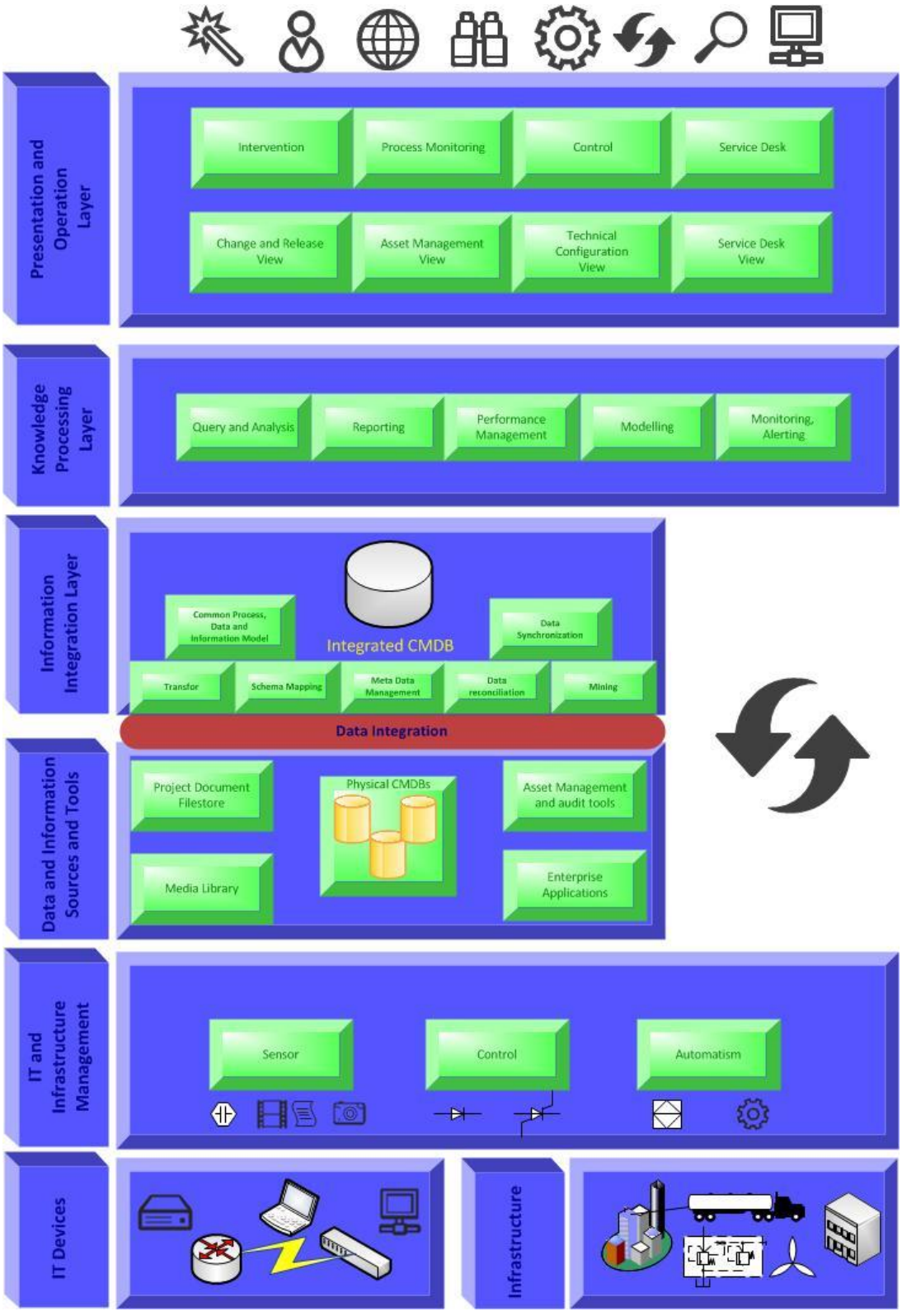
[4] Bármelyik komponens, amelyiket felügyelni kell valamilyen IT-szolgáltatás nyújtása érdekében.

Ezer ilyen kérdést tehetünk fel, amelyek elsőre talán meghökkentő és talán nevetséges is, de egy kiemelten védett infrastruktúrák esetében már lehetnek érdekes részei is. Természetesen mindig kérdés, hol alkalmazzuk a CMS rendszerünket. Egy vegyipari cégnél elképzelhető, hogy sok olyan paraméter érdekes, amely egy katonai, nemzetbiztonsági cégnél nem, és fordítva is igaz. Ezeket az adatokat a kockázatelemzésnél is fel kell használni. Érdekes azonban, hogy pont a kockázatelemzésből derülhet ki, hogy milyen adatokat kell nyilvántartanunk még. A szélesség alatt pedig azt értem, hogy milyen messze nyúl el a nyilvántartás keze. Amennyiben meghatározzuk, hogy a cégen belül egy bizonyos szegmensig tartok mindent nyilván, akkor azon belül minden egyes elemet el kell érnünk az adatszolgáltatás szintjén. Hasonlóan, hogy ha a kapcsolódó cégek adataira is szükség van, akkor az összes beszállító cégnél meg kell követelni az adatszolgáltatást. Tehát biztosítani kell az egyenszilárdságot, annak érdekében, hogy használható elemzéseket tudjunk elkészíteni.

Minél nagyobb és „kritikusabb”[5] egy informatikai infrastruktúra annál bonyolultabb, összetettebb felépítésű és annál nehezebb az üzemeltetés számára egy CMS segítsége nélkül átlátni az egész működését. A rendszerelemek bonyolult kapcsolatai eredményezhetnek olyan nem várt esemény bekövetkezését, amely negatív irányba mozdíthatja el a rendszer működését.

Kiegészítve az ITIL ajánlását az **1. ábra** segítségével mutatom be a CMS kialakítását.

[5] Kritikusabb alatt azt értem, hogy az üzemszerű és elvárt működéstől való eltérés veszélyeztethet más rendszerek, emberek, közösségek életminőségét negatív irányba.



1. ábra CMS felépítése (a szerző szerkesztése a [6] alapján)

Az ábrán látható mitől több a CMDB-nél egy CMS felépítése.

A legalsó szinten helyezkednek el az IT és a hozzátartozó (épület elektronikus berendezései, klíma, UPS, beléptető és riasztó rendszer, tűzérzékelő és oltórendszer, zártláncú videó hálózat, stb.) infrastruktúra elemek.

Ez a szint minden esetben megvalósul, még ha hiányosan is, mert különben nem is létezne informatikai rendszer.

A következő szinten az érzékelők helyezkednek el. Ezek általában rendszerenként a gyártó által szállított szoftverrel van ellátva. Itt találhatóak meg a rendszereket - általában a gyártó által szállított - vezérlő eszközök, szoftverek. Léteznek integrált rendszerek is, ilyenek például azok a biztonsági rendszerek, amelyek egy egységet képeznek a beépített beléptető, riasztó, zártláncú videó és tűz jelző rendszerek által. Ezek kimenete sokszor az IT rendszer bemenete is lehet, amikor például a tűz, vízbetörés esetén utasítják az IT infrastruktúrát a rendszer mentésére, leállítására. Ezen a szinten már információs infrastruktúráról beszélünk, mert az infrastrukturális elemeket komplexen kezeljük.

A következő szinten jelenek meg a rendszerenként különálló CMDB-k, vagy a dokumentum könyvtárak. A szenzorokból érkező jeleket átalakítást követően az adatbázisban tároljuk. Itt nagy a felelőssége az adatbázis tervezőnek, mert nem adatokra, hanem információkra van szükségünk. Ezt azonban sokszor a nagyon sok adatból nem lehet kihámozni, a nagyon kevés adat pedig téves információkat adhat.

Az integrációs szinten jelenik meg az egységes CMDB. Ez lehet valóban egy önálló adatbázis, de hasznosabb, ha virtuális értelemben jelenik meg csak egy adatbázisban. Ahhoz, hogy a különböző adatbázis adatait egységként kezeljük szükséges például az adatok meta adatait központilag kezelni, elvégezni a szükséges átalakításokat, a közös pontokat megtalálni és nyilvántartani. Természetesen a szinkronizáció ütemezése és végrehajtása az egyik legkomolyabb feladat ezen a szinten.

Amennyiben rendelkezésünkre áll a tömeges adat, akkor a tudásbázis szinten kezelhetjük azokat. Itt nem csak az aktuális adatokat, de az archiváltokat is hasznosítani lehet, illetve kell. Itt valósulnak meg a különböző elemzések, lekérdezések, a modellalkotások, amelyek segítségével algoritmusokat hozhatunk létre. Az adatok halmaza, azok kapcsolódása, időbeni változása olyan összefüggéseket mutathat, amelyet külön-külön nem vehetnénk észre. A rendszer riasztási eseményeit összetetten lehet kezelni, amely hatékonyabb beavatkozáshoz vezethet.

A legfelső rész gyakorlatilag a rendszerfelügyeleti szint, a jelzéseket, elemzéseket megtekinthetjük, utasításokat adhat ki az üzemeltető személyzet. Ez a szint biztosítja a felső vezetés részére is az információ megjelenítést. A tudásbázis által biztosított algoritmusok és az adatbázis adatai segítségével automatizmusok által javaslatokat tehet a felügyeleti rendszer a beavatkozásra, vagy akár automatikusan végre is hajthatja azokat.

Abban az esetben, ha külső információáramlás is szükséges, akkor ellenőrzött formában becsatlakozhat különböző szinteken is az együttműködő szervezet. A maximális biztonságot is szem előtt tartva a kapcsolat egyirányú kell, hogy legyen, és a kimenő adat az ellenőrzést követően adatdióda segítségével továbbítható.

A CMS kiépítettségét tekintve egy cég különböző fejlettségi szinten lehet. Legtöbb esetben sajnos a harmadik és a negyedik szinten vannak a cégek. A kiépítést a moduláris felépítés miatt lehetőség van szakaszosan végrehajtani. Az egyik legkritikusabb rész egy már működő cég esetében az adatbázisok integrációja, a közös CMDB létrehozása. A CMDB-t tekintve is több fejlettségi mutató lehet, amelyek a következők:

- Az információk a rendszerről többnyire a közvetlen üzemeltető állomány fejében létezik. Legtöbbször a tudás hatalom elv alapján nem osztják meg az információt mással, így vélik biztosítottnak a munkahely megmaradását, a nélkülözhetetlenséget;
- Valaki leírja saját Word, Excel dokumentumba, jobb esetben valamilyen adatbázisba a saját számítógépén. Egy bonyolultabb rendszernél már nem valósítható meg, mert az hamar a rendszer összeomlásához vezetne;

- Az előbb létrehozott nyilvántartásokat a közös mappákban tárolják. Ebben az esetben, ha az üzemeltető személlyel történik valami, van esély a leírás megtalálására;
- Ezen a szinten már a közös mappában tárolást valamilyen szabály írja elő, így a mapparendszer is előre kidolgozott, átlátható. Így valóban kezelhető az információ abban az esetben is, amennyiben kiesik a rendszert alkotó személy, személyek;
- Egy magasabb fejlettség, amikor már adatbázisban tárolják az adatokat. Így az adatok gyorsan kezelhetők, azokkal könnyebb feladatokat végrehajtani;
- A következő szint, amikkor az összes információ egy fizikai vagy virtuális adatbázisban tarolunk, amely természetesen szabályozott módon történik;
- A legfejlettebb, amikor a cég normál működése során már nem is lehet végigvinni egy folyamatot a CMDB használata nélkül;

Véleményem szerint egy kritikus információs infrastruktúrát üzemeltető cégnél szükséges a legmagasabb szintet elérni. Ezek a rendszerek már annyira bonyolultak, hogy másképpen nem kézben tartható a biztonságos üzemeltetés. A másik fontos szempont, hogy a kezelő személyektől nem függhet közvetlenül az infrastruktúra működése. A személyzet cserélődése nem okozhat fennakadást. Az információ minden esetben rendelkezésre kell, hogy álljon az új szakembereknek is a lehető legrövidebb időn belül. Persze nagyon nehezen helyettesíthető az a karbantartó munkás, aki az iskola elvégzését követően már a cégnél dolgozik és készül nyugdíjba menni, de egyszer mindenki elmegy a cégtől. Amennyiben a cég rendelkezik a legfelső szinttel logikus felépítéssel, „szervezési" eszközökkel viszonylag könnyen megvalósítható a CSM rendszer passzív állapota[6]. A szintek egyes funkciói nem minden esetben valósulnak meg egy időben. A legfontosabb a közös adatbázis, amin a tudásbázis elemek folyamatosan bővíthetők. A közös kezelőfelületbe folyamatosan integrálhatók a gyártók által szállított kezelőfelületek. Persze itt is van egy nagy kérdés. A gyártók rendelkezésre bocsájtanak-e minden információt, biztosítják-e a megfelelő csatolófelületet az információáramláshoz. Üzemeltetés szempontjából nagy előnyt jelenthet egy homogén rendszer kialakítása, azonos gyártók kiválasztása. Ez azonban ellentmondásban van azzal, hogy a magas rendelkezésre állás különböző technológiák, gyártók alkalmazását követeli meg.

Eddig még nem eset szó az egyik legfontosabb rendszerelemről, az emberről, amelyről jelenleg a CMS rendszerek nagyon kevés információt tárolnak. Ráadásul ezeket az adatokat teljesen más módszerrel kell felvinni a CMDB-be, mint a rendserek adatait.

Mik is lehetnek ezek az adatok? Fontos kérdés a személyzet, felhasználók képzettsége, tapasztalata és egy sor jellemzője, amely befolyásolja a rendszer működését. Ilyen például a viselkedés, melynek rögzítésére már ma is rengeteg eszköz áll a rendelkezésünkre, de léteznek olyanok is, amelyek a személy együttműködése nélkül is összegyűjthető, ilyen a viselkedés alapú profilkészítés. Persze ezek sok erkölcsi és jogi kérdést is felvetnek, de létezhet olyan hely, ahol ezzel együtt kell élni. A hétköznapokban is megfigyelnek ilyen eszközökkel minket, amikor az Internetet használjuk, majd ezeket az adatokat kereskedelmi céllal fel is használják. Lépten-nyomon otthagyjuk a digitális nyomunkat mindenhol, ahol az informatikai eszközök által kezelt rendszereket használjuk.

[6] Passzív alatt azt értem, hogy a rendszer nem képes automatikusan beavatkozni a működésébe. A kezelőszemélyzet egy rendszert használ, jogosultsági szintnek megfelelő lekérdezéseket tudnak végrehajtani és utasításokkal vezérlik a rendszert.

Ilyenkor nem csak az internet (e-mail, közösségi média, weblapok, internetes csevegő- és telefonszolgáltatások, stb.), de a mobiltelefon, a GPS eszköz, bankkártya, banki szolgáltatás használat, térfigyelők felvételei és még számos tevékenységünk digitális lenyomata ott marad valahol. A banki adatbázisból kiderülhet, hol vásárolunk, mikor és mennyiért, kinek milyen rendszerességgel utalunk pénzt, vagy ki utal nekünk, ezáltal megtudható, kikkel vagyunk kapcsolatban. A mobiltelefonunk aktív használat nélkül is folyamatosan árulkodik a hollétünkről, hová milyen gyakorisággal megyünk és ott mennyi időt töltünk. Érdekes adat az Internet használatakor, hol mennyit időztünk, milyen billentyűzet vagy egér aktivitásunk van, honnan jöttünk és merre tartunk. Talán mégis a legveszélyesebbek a felhőben tárolt adatok. Sajnos sok cég az ügyfelek adatait tárolja üzletileg egyes esetekben talán valóban a leghatékonyabb egy harmadik fel által biztosított szolgáltatásként a virtuális IT környezetben. De ezeket az adatbázisokat összekötve egy cég biztonsági rendszerével, mozgásnaplónkkal és kapcsolati hálónkkal még értékesebb információt kapunk. Főleg, ha nem csak az aktuális adatokat figyeljük, hanem tendenciákat és összefüggéseket keresünk.

Mint mindent ezt is lehet jó és rossz dologra felhasználni, de egy biztos, hogy ezek a technológiák léteznek és használják már őket. A kérdés, hogy mikor kapcsoljuk ezeket mind össze, illetve mikor leszünk képesek kezelni az óriási mennyiségű adatot. Véleményem szerint nem a biztonsági terület lesz, az ahol esőként hasznosítják az elméletben elért eredményeket. Az üzleti élet gazdasági szereplői a potenciális vásárlók felkutatásánál és a reklámok célba juttatására hatékony módszer lehet, így rengeteg pénzt fordítanak rá, és az emberekkel is elfogadtatják a kellemetlen oldalát is. [3] Az emberek viselkedésének az elemzéséhez jól jöhet a környezeti hatások adatbázisba mentése. Ugyanis az embereknek az a normális viselkedése, hogy követni akarják a társadalmi normákat, a csoportok viselkedését, és a legtöbben feljebb és feljebb akarnak kerülni, vagy meg akarnak felelni a cégüknek, főnöküknek. Ezekből a viselkedési formáktól a környezeti változás fogja őket eltéríteni. A rendszerünk viselkedésének megjóslásánál az emberi tényezők mellett, amelyek sokszor kiszámíthatatlanok, a gyártók megadnak az alkatrészek, eszközök tekintetében olyan adatokat, amely a meghibásodási valószínűséget mutatják. Ezeket az adatokat is bevihetjük az adatbázisunkba, így a gráfelméletben alkalmazott algoritmusok segítségével olyan elemzéseket végezhetünk, amik a rendszer nagyobb megbízhatóságát segítik elő.

Természetesen az adatok gyűjtésével és elemzésével a gazdasági élet szereplői mellett már ma is foglalkoznak a rendvédelmi szervek és titkosszolgálatok. Sajnos a kapcsolódások bonyolultsága és az adatok számossága nem segíti elő a robbanásszerű fejlődést, de talán a hálózatkutatásban elért eredmények segíthetnek ezen. Egy ilyen a nemrég megjelent publikálás is, amely Babai László matematikus nevéhez kötődik, aki jelenleg a Chicagói Egyetem oktatója. Ő egy új eljárást mutatott be, ahol egy algoritmus segítségével gyorsabban megállapítható, hogy két gráf azonos-e. Ez segítséget nyújthat az informatikai rendszerek felügyeleténél, persze akkor, ha megfelelő számú információ áll a rendelkezésünkre. [4] Hasznos lehet például, ha a mintákat, az előzményeket összehasonlíthatjuk az aktuális helyzettel. A módszer tűzfalak esetében már ma is egy létező gyakorlati alkalmazás, de az összetett rendszerek esetében még nem.

A fejlődést szintén nagyban felgyorsítja Barabási Albert-László kutatásai, aki a hálózatelméleti kutatásai során informatikai rendszerek felépítéséből, vagy éppen a telefontársaságok által átadott névtelen adatbázisokból alkot olyan megállapításokat, amelyek a hálózatok egészére vagy legalábbis tipikus hálózati felépítésre igaz.

A CMS használatához, mint az időjárás előrejelzés esetében is sok adatra van szükség, és minél későbbi bekövetkezendő eseményt akarunk előre jelezni, a megbízhatósága annál bizonytalanabb lesz. Egy nem várt eseménynél a reagáláshoz az üzemeltető személyzetnek a lehető legtöbb időre van szüksége, hogy biztosítsa az üzletmenet folytonosságot az informatikai rendszerek segítségével.

Sajnos azonban ma a legtöbb védelmi és a riasztást kiváltó eszköz már csak az esemény bekövetkezésekor jelez, amikor azonnal reagálni kell. Értékes információ lehet a kezelőszemélyzetnek az is, hogy mi és mikor várható a rendszerünkben, ha például leáll egy rendszer eleme, vírussal fertőződik meg, kiesik egy összeköttetés. Ezeket sok adat elemzésével a CMS tudja biztosítani.

Neumann megállapítása, amikor a szervezési eszközöket említi mindenképpen igaz a kritikus információs infrastruktúra esetében is. Azt, hogy a szűk reagálási időt hogy hogyan használjuk ki, az előre megtervezett intézkedési stratégiákkal lehet a leghatékonyabbá tenni, és egy komplex rendszerre kidolgozott biztonsági, üzemeltetési utasítással, rendszabállyal lehet a bekövetkezés előtt megnövelni a várható időkeretünket. A CMS pedig elősegíti az átláthatóságot és egyes esetekben az automatizmussal csökkenti a reagálási idő is. Úgy működik, mint a Neumann elv a tárolt adatokon az előre megírt (vagy a folyamatában kidolgozott) program elvégez műveleteket. A cél a stabil állapot fenntartása.

KÖVETKEZTETÉSEK

Egy rendszer nem csak az eszközöktől válik biztonságossá. A jól megtervezett rendszer tartalmazza a szükséges eszközöket és a rendszer üzemeltetéséhez és használatához szükséges rendszabályokat. Már a rendszer fejlesztése során a tervezési fázisban gondoskodni kell a megfelelő szabályozottságról. Azonban nagyon fontos, hogy nem a jogszabályok és ajánlások betű szerinti betartása a fontos, ennél több kell, a szellemiséget kell átvenni és alkalmazni.

Hasonlóan, ahogyan ma mára tűzfalak is „tanulnak” a szokásainkból, az elmúlt időszak eseményeit elemzik, így a CMS rendszereken keresztül a kritikus információs infrastruktúráknál is egyre inkább alkalmazni kell ezt a módszert. Az eseményekhez hozzárendelve annak bekövetkezésének idejét az idő múlásával a felgyülemlett adatokból egyre megbízhatóbb és több jóslást adhat a rendszerünk az esetleges nem várt események bekövetkezésére.

A Neumann János állítása miszerint valamely szerkezet működési biztonságát nemcsak technikai eszközökkel, hanem lényegében véve szervezési eszközökkel is növelni lehet ebben az esetben is igazolható. Egy rendszernek minél kisebb az entrópiája[7], az annál rendezettebb, tehát a 0 entrópiájú rendszerhez kell közelítenünk ahhoz, hogy minél inkább kézben tarthassuk a rendszerünk irányítását. Ehhez azonban ismernünk kell a rendszerünk elemeit, kapcsolódási pontjait és természetesen ezek egy gondosan megtervezett folyamatosan kontrolált fejlesztésen, majd üzemeltetésen kell átesniük.

FELHASZNÁLT IRODALOM

[1] NEUMANN, J. V.: First Draft of a Report on the EDVAC, Pennsylvania: University of Pennsylvania, 1945.

[2] NEUMANN J.: A számológép és az agy, Budapest: Gondolat Könyvkiadó, 1964.

[3] ALBERT-LÁSZLÓ, B: Kiszámítható-e az emberi viselkedés dinamikája? www.ceeol.com Megtekintés ideje: 2015.11.26

[7] *„Az entrópia azt mutatja meg, hogy mennyire rendezett egy rendszer belső viselkedése. Minél nagyobb a rendszer entrópiája, annál rendezetlenebb. Az entrópia tehát a rend mértéke. Azért fontos, mert szorosan összefügg a jósolhatósággal.”* [3]

[4] CHO, A.: Sciencemag.org http://news.sciencemag.org/math/2015/11/mathematician-claims-breakthrough-complexity-theory Megtekintés ideje:2015.11.18

[5] itSMF Hungary: ITIL® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5, Budapest: itSMF Hungary, 2008.

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

THE IMPACT OF INFORMATION AND COMMUNICATION TECHNOLOGIES ON PRISON INSTITUTIONS

AZ INFORMÁCIÓS ÉS KOMMUNIKÁCIÓS TECHNOLÓGIÁK HATÁSA A BÖRTÖN INTÉZMÉNYEKRE

TSEND-AYUSH Ganbadrakh

(ORCID: 0000-0001-6182-4984)

ganbadrakht54@gmail.com

Absztrakt

Faced with increasing prison populations, limited capacity, and rising prison construction costs, prison administrators have intensified their search for new innovative and creative technologies and solutions .[1] The part of that entity is the Information and Communication Technologies (ICT). New technological innovations have been developed to monitor and to improve the performance of the prison institutions, but we know little about how and why ICT are adopted, and the consequences. The aim of the paper is to provide an examination of a wide range of ICT that have applications in the areas of prison institutions. We provide a description of recent ICT solutions, and then emphasize the impact of new ICT on operation of prison institutions. We specifically discuss three key social groups in prisons – (1) prison administration, (2) prison staff, (3) prisoners and the impact of the use of new ICT on them respectively. They are the fundamental and important nods and conduits through which the main information and financial resources are circulating in the prison network. Finally, we would outline any other developing ICT that can be used in the future. Ide kell beírni az esetleges egyéb információkat is a cikkel kapcsolatban. (Pl. Ha valamilyen pályázat támogatásával készült.)

Keywords: *ICT, prison system, prison institutions, prison administration, prison staff*

Abstract

Az egyre növekvő börtönpopuláció, a korlátozott kapacitások, és a növekvő börtönépítési költségek, a büntetés-végrehajtásban dolgozók fokozottan keresik az új, innovatív és esetenként kreatív technológiákat és megoldásokat. [1] Ezen megoldások közé tartozik az Információs és Kommunikációs Technológiák (IKT) keresése is. Különböző technológiai újítások kerültek kifejlesztésre annak érdekében, hogy a börtön intézmények javítsák a teljesítményüket. Ennek ellenére keveset tudunk arról, hogyan és milyen módon választják ki a különböző IKT-kat. Jelen írás célja, hogy a börtön intézményekben használatos különböző IKT alkalmazásokkal kapcsolatos döntéseket vizsgálja. Leírja az IKT megoldásokat, majd hangsúlyozza az új IKT-k hatását a börtön intézmények működésére. Konkrétan vizsgálja az új IKT-k hatását három kulcsfontosságú csoportok esetében, úgymint (1) a büntetés-végrehajtási személyzet, (2) a börtönök személyzete, valamint (3) maguk a fogvatartottak. Ezek a csoportok képezik azokat az alapvető csomópontokat és kapcsolatokat, amelyeken keresztül a főbb információs és pénzügyi források megtalálhatók a börtönökben. Végül az írás felvázolja az IKT-k lehetséges felhasználását a jövőben.

Kulcsszavak: *IKT, börtönrendszer, börtön intézmények, a büntetés-végrehajtás, büntetés-végrehajtási személyzet*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.13.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.16.

INTRODUCTION

We are living in the era of immense influence of the Information and Communication Technologies (ICT) on society. The ICT is generally regarded as the super high way through which information is transmitted and shared by people all over the world. [2] The ICT is shaping our daily activities whether at home or on other places. It completely changed the way the government services are conducted. We can provide numerous examples of the wider application of the ICT in the spheres such as economy, trade, finance and education. In a society and economy networked with complex info communications systems we take care of almost all of our daily businesses in the net, we might fall into our own trap of advanced state. The government, economy structure, traffic network, power supply system etc. of a well networked and developed country can become paralyzed or can be limited in their operations. [3]

Public organizations' management and leadership are actively encouraging the mechanisms to support the promotion of the newly established ICT. For example, it seems to be that the Internet and mobile phone applications could enhance the effectiveness and efficiency of public service providers like hospitals, schools and administrative offices.

But there is one specific public field of activity where the process of the ICT penetration made a slow start at the beginning. It is the prison system[1]. At the first half of the twentieth century prison institutions lagged far behind business and other government institutions in adopting new technology. The deprivation of access to ICT seems to be as a new obstacle for all core social groups making up the prison institution as whole entity. Prison administration's main role is to lead and organize the daily activities of the organization. The role of prison staff is to support and organize the daily activities of the organization according to the rules and procedures which are applied to the particular organization. Prisoners are the essential group of people which on all functions and operations of prison institutions are focused on.

Some experts stated that the reason of prison organizations' use of the ICT particularly slow is related to the specific characteristics of its activities. It is fair to state, based on the evidence and analyses developed by key researchers in the field, the following propositions: *the technology can greatly improve the safety and effectiveness of the prison institutions in any country*. A clear and overriding concern of those in the prison institutions is the safety of prison staff and prisoners themselves. The best way to do this is to reduce the possibility of dangerous and critical situations in prisons. In short, ICT can make prisons safer for both prison staff and prisoners. New and innovative technologies could enhance the effectiveness of prison institutions. [4] For example, computers will offer nearly unlimited possibilities for collecting information and sharing it with other governmental organizations which is very important for the functioning of any institution.

THE USE OF ICT IN PRISON ADMINISTRATION

Information as well as the legal, administrative and financial areas is crucial to prison system as a whole. Knowing what is happening gives prison administrators as leaders of particular prison institution the power not only to react to problems urgently, but also to prevent them. In recent decades, ICT has undergone significant changes. Prison administrators can now

[1] Here, we are using the term **prison system**. There is different application of the term among the national prison communities. It depends on the legal background, tradition and culture of each nation-state. For instance, in Hungary the main organization dealing with imprisonment of inmates called Hungarian Prison Service (Büntetés-végrehajtási Szervezet).

keep in touch by *e-mail* and can share information on web pages on *the Internet* with relevant organizations so that to optimize the available resources.[5] To put it more clear, ICT give more accurate and quick access to information and internal units of the prison. The timely, accurate and relevant information sharing with both head-on and subordinate organizations is the indispensable characteristic of modern prison administration. The following ICT and devices are commonly used in prison institutions around the world.

Videoconferencing is another way to share thoughts and ideas in the prison administration. Meetings that once required expensive travel can now be attended from the one's office or from a local teleconference site. In addition, satellite TV and video technology have enhanced distance communication for prison administrators. [5]

Mapping tools (electronic bracelets) is another ICT solution. It can help to prison administration by tracking disciplinary incidents, visitation patterns and medical information; managing gangs and escape threats; and identifying personal information about prisoners' daily activities. [5] In the form of data collection, storage, and processing systems, ICT allows prisoner administration to cooperate with local governments, decreasing their dependence on head-on organization. There are various kinds of information management systems (software) and solutions available and applicable for the specific operation and performance of different prison institutions (pre-trial detention centers, prisons, high security prisons). [6] It means that the overall process of decision making and agenda setting (which are the main functions of prison administrations) would become more agile and productive. Therefore secured intranet and internet networks, computers and software programs play critical role in managing daily activities of prison administration.

THE USE OF ICT FOR PRISON STAFF

The increasing use of ICT is an important aspect in addressing the needs of the prison officers. New technologies have also proved helpful in reducing costs and improving the effective operation of facilities.

Modernization of security systems and improved protection for staff are key issues facing prisons. Real power in a prison resides in information. To manage prisons effectively, operators need to control information at all levels. This means knowing what is happening at all times, despite the difficulties associated with a prison environment in which, by definition, information is frequently withheld or concealed. [7]

The wider implementation of ICTs in prisons helped to increase the level of security for the prison officers and prisoners. Because of unique situation, prison staff is constantly facing the dangerous conditions which could put their wellbeing and life in jeopardy. The prison system brings various technological solutions to tackle the persistent issues of security and safety. The physical security measures for prison staff include X-ray machines, wands and portals for detecting metal; systems for detecting explosives; and biometric entry systems for visitors, to ensure that prisoners do not escape by posing as visitors. [5]

In healthcare service, many prisons' medical staff utilizes *telemedicine*. Telemedicine allows physicians to consult with medical personnel from distance through videoconferencing, using devices such as medical video cameras. It can improve health care in prison establishments by reducing costs of health care for prisoners, and making the work of prison medical staff more efficient. Taking a prisoner with health illness to a specialist outside the prison poses a danger to prison staff and the community by giving the prisoner an opportunity to escape.

Fairly new in the prison system is the *Global Positioning System* (GPS). GPS is now used for monitoring prisons both inside and outside of the prisons. The GPS tracking unit worn by a prisoner (who can go out of prison facilities) allows computers to find locations at any time

to the precise point. *Surveillance* technology allows prison staff to view several areas of a prison at the same time. Prison officers can also wear personal alarm and location units that allow a computer to track their locations and respond to distress signals by sending the closest officers to the site of the emergency. [5]

Prison staff is also relying on new ICT to help track inmates and former inmates. *Speaker ID* technology can be used to keep track of who calls inmates in prisons and to monitor criminal activity such as escape plans, gang activity, and smuggling of contraband.
In near future, to increase the efficiency of prisoners' monitoring, a smart card, a plastic card embedded with a computer chip, could be used to store all types of information about the prisoner, from medical care to food eaten. ICT has also made it possible for prison officers to remotely open prison cell doors either individually or in unison and to remotely control the flushing of toilets. [5]

Additionally, prisons have been actively using *Closed Circuit Television* (CCTV) technology to make it possible for locations in prison to be remotely viewed. Given that prisons are violent places and a wide range of negative behavior occurs in this environment, it is possible that the prevention of prison disorder is a purpose of CCTV. [8] This behavior is usually engaged in by prisoners and results in physical negative impact (prisoner-on-prisoner assault, prisoner-on-officer assault, sexual aggression, and murder), psychological negative impact (verbal abuse and threats), or economic risks (theft, extortion, and robbery). [8] Other purposes of CCTV surveillance in prisons include the detection of crime and disorder, improving the internal control or acting as a general monitoring tool (Figure 1). [8]

Figure 1 CCTV devices used in US correctional facilities [9]

Radio communications: [7]

Prison managers and staff use professional mobile radio (PMR) systems to meet their secure communications needs. PMR solutions offer useful additional functionalities such as group management and priority management. In addition, the deployment of smart terminals allows radio communications infrastructure to be used for transmitting alarm information.

Prison staff equipped with PMR terminals have access to the following functionalities:

- radio communications,
- hidden alarm button for alarm and emergency backup calls (gradually replacing wall-mounted alarm buttons),
- tamper detector,
- lone worker protection (terminals are worn in the vertical position, and an alarm is generated if they are tilted to the horizontal, i.e. in the event of a member of prison staff falling ill or being attacked),
- integrated GPS,
- patrol management (optional).

Transmission of voice, data and alarms to PMR terminals allows staff to rapidly and effectively locate, characterize and verify emergency situations. Appropriate resources can then be dispatched to manage the incident. [7]

Besides this advantages, ICT application in prison have the following impact on daily activities of prison staff such as less movements, diminish routine tasks, and versatile communication between prison staff and prisoners.

ICT in concert with hardware and software tools as computers, programs form network that is complex and making it possible the processes associated with information such as storage, manipulation, managements, display, interchange, and transmission of data.

E-learning would be used for further qualification of prison staff. By using e-learning systems for their own purposes prison officers become aware of the advantages using ICT in education. [10] E-learning for staff provides innovative tools for necessary continuous qualification and at the same time raises the insight in the benefits of e-learning. [10]

The prisons are also starting to use videoconferencing for interrogations and visitation. Criminal justice officials and prosecutors can now save on travel and avoid standing in line by scheduling videoconferences with prisoners and potential wrongdoers. [5]

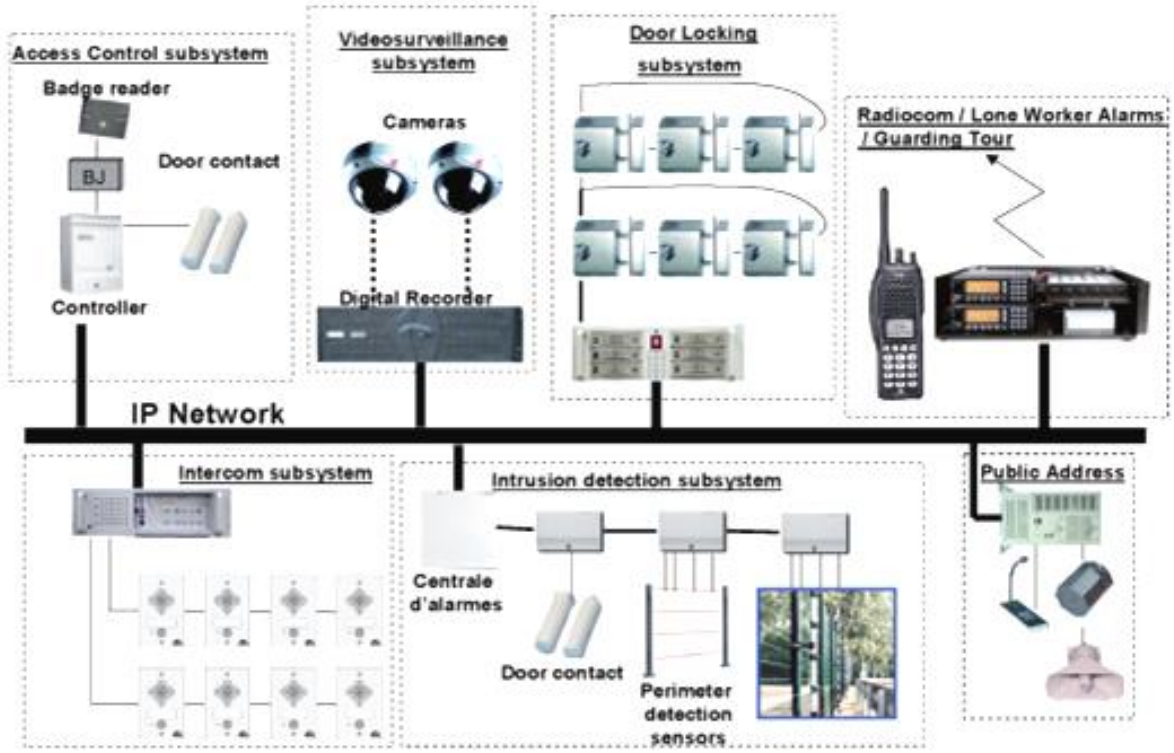


Figure 2 The current safety and security system (French private company and security solution provider) [7]

The system ties together seven subsystems via a secure IP network controlled via the SATHI hyper vision system:

- access control,
- door locking,
- intrusion detection (with information from perimeter detection system alarms, door contacts, wall-mounted alarm buttons, hidden alarms, lone worker alarms, etc.),
- video surveillance (digital system incorporating image analysis capability),
- intercom,
- radio communications,
- public address. [7]

THE USE OF ICT FOR PRISONERS

Society and the prisoners benefit from the continued use of ICT in prison institution. It influence could be seen beyond the prison institutions. The monitoring equipment as electronic bracelets add to tax revenues, reduce welfare costs, and relieve the need to build additional prisons. [10] They also allow a prisoner to retain family and community ties (Figure 3). [10]

Figure 3 Monitoring ankle bracelet [11]

The main area of prison institution there ICT made a vivid footprint is educational programs for inmates. By participating in the programs, the inmates would access to *digital literacy* (*E-learning*). The programs could support prisoners' rehabilitative potential and increases the chances of having more family contacts. [12] ICT programs will increase and equip the inmate's knowledge and opportunities in empowering them. [12]

Human beings need connection with one another. For people imprisoned in prison institution, it can be very important. Regular interactions with family, friends, and supporters can help to alleviate the pain of imprisonment. All of above-mentioned processes could definitely increase the chances of success. To sustain such activities further prison establishments have been seeking new ways. For example, *video visitation*, like *Skype*, allows prisoners to hold video calls with their family members and friends from a personal computer. [11] Video visits provide the opportunity not only to see, but to hear their voices. [11] It has rather emotional effect.

Prison sentences always constitute a deprivation of freedom. But beyond security aspects the aim of the organization is to foster reintegration of prisoners into society after release. According to international conventions and recommendations the prisoners have the same right to education as other citizens. Education helps to develop the personality and character of the individuals. Education plays an important role in the process of reintegration.

All prison systems apply prison education all around the world. It is evidence that rehabilitation is effective in reducing the criminal behavior in at least some of the offenders. Imprisonment is not a panacea for all criminals but an important and in many cases necessary tool for crime prevention. The evidence from the meta-analyses suggests that effective correctional treatment programs appear to follow some basic principles. The effectiveness of any prison treatment and education depend on the level and quality of them. The prison atmosphere, level of free-will and cooperation basically determines the success. Prisons are part of any societies and prisoners are human beings who committed crimes and therefore they have to been punished. But the kind of punishment we use against them is vital. [13]

Considering the growing importance of ICT in society, prisoners should have the chance to use ICT for education and training purposes (E-learning).

E-learning can give prisoners – online or offline – access to learning material from general schools, vocational training schools or colleges. [10] In addition, central examination facilities, which can be reached via secure internet channels, should be used by inmates to obtain degrees which are widely acknowledged by employers. [10]

E-learning for inmates provides a huge opportunity to enhance prison education by broadening qualification opportunities, improving the quality of education and training, motivating (especially young) inmates. E-learning gives inmates the chance to not only to learn subjects of general or vocational education but also provides the opportunity to build up digital literacy. [8] In today's society where digital skills becomes necessary at the workplace as well as in daily life the chance for reintegration of prisoners can be strongly increased. [10]

Some experts emphasize the public has to be informed that the introduction of ICT in prison education is not a "leisure tools" for inmates but a necessary measure to provide an up-to-date qualification which improves social reintegration chances, job opportunities and finally reduces costs in a substantial way by reducing the risk and costs of re-offending. [10]

Mobile phone jammers:

Smuggling of items into prison – in particular mobile telephones – is a major security headache for prison operators. Mobile phones have become a vital tool for escape attempts involving contact with accomplices outside the prison walls. As phones become increasingly smaller and contain fewer metal components, they become harder to detect using conventional metal-detection technology. Carefully targeted jamming of mobile phone frequencies has emerged as the most effective means of combating this kind of threat. [7]

CHALLENGES

Introducing the ICT in multiple prison institutions raises significant logistical and operational challenges. [12] The establishment of reliable and relevant ICT in prisons must be followed by setting up the network of sophisticated hardware and software systems and highly trained specialists.

It also raises the threshold for the prisoners who could and could not afford it specifically when they are participating in educational programs (E-learning). It means the increasing the gap between the "haves" and "have not's". Some prisoners eager to be involved but have a lack of financial and educational (qualifications) skills and capacities to pursue the educational training.

The widespread use of the ICT in prison institutions could bring forward the issue of "digital divide" which are very actual in society. People lacking digital competence are at the risk of social exclusion. [10] It is related not only to prison staff but also to the prisoners.

ICT can lead to gross violations of individual privacy. When the prison staff uses the ICT for tracking and surveillance functions they could have more leverage to change the behavior of the prisoners. It makes the status and rights of the inmates considerably weak and low.

Is it usual for the prison staff to track and control nearly all activities of the prisoners 24/7? Does it mean that the prisoner can lose their individual privacy even when they use toilet of bathroom? Isn't it infringe the universal basic human rights which also applicable to the prisoners? We don't have any clear answers to the questions.

We could see the dominance of two opposite views in society. In one hand, group of people are more optimistic to the future development and application of ICT in prison system. They state that the technological progress could change the overall established paradigm of prison institutions in the positive way. It could not only support and maintain the prison administration and prison institutions' operation quality and availability but also could improve intellectual and mental capacities of the prisoners. On the other hand, group of people firmly oppose the widespread application of ICT in prison institutions. They have overall negative and skeptical attitudes about how the ICT used in prisons. They argue that ICT make the daily routine activities of prisoners more vulnerable and against the basic human rights. At the same time it makes the work of prison staff more routine and inhumane. The outcome would be that the current link between prison staff and prisoner, prison staff and prison staff, prison staff and prison administration, prison administration and prisoner could

be lowered. Otherwise, people to people and human to human relations might become loose and at the end long established prison system would destroyed. To say in other word, there would be a huge loss to community connections which is vital to future of the prisoners after the release.

However, the structure of the prison system creates many barriers to meaningful contact. Imprisoned people often serve their sentences far from home in places unreachable by public transport. [12] Personal visits can place a substantial burden on the visitor, who may have to miss work, pay for childcare, and cover the costs of travel for their loved ones. [12] All these conditions seem to be showing that the use of ICT in prisons more rational and reasonable.

In addition to it, the overall security of ICT in prison institutions is very important. Sometimes prisoners and prison staff are attempting to access or to dismantle the established ICT systems related to security, monitoring, surveillance and event E-learning facilities. In order to prevent and deny such activities in the future the authorities and competent ICT professionals need to develop the rules, regulations, procedures, and all-inclusive hardware/software programs in concert with sophisticated information systems.

CONCLUSION

Despite the growth of the ICT, there are still obstacles to overcome. Prison staff can be resistant to drastic changes. They feel more satisfied with current status quo and are more willing to follow the current rules and procedures. When the reform to be placed the opposing groups become more resistant and intense.

Another reason for hesitancy to adopt new technology is the cost. [5] The setting up of new technologies demand the huge amount of investment. It could in turn bring more burdens to the state budget which is always a “hot issue” for discussion and consideration. [5] Or to say other way, in order to put forward innovative and new technologies additional reliable and significant financial resources must be guaranteed.

Ethical concerns about the rights of prisoners might be another obstacle to implementing new technology. We need to build up the coherent legal mechanisms which could assure that the basic human rights of prisoners and invaluable privacy will be protected. The assurance must come from both the highest and the lowest level of prison establishments.

However, there is no question that new systems and devices are playing an increasingly constructive part in the work of prison institutions. The reason is that it is a modern trend which is shaping the whole aspects of human life. The prison institution itself is a part of it. Thus it must be a part of the modern trend alike.

The use of technology in prison environments has undoubtedly changed the way that prison administration, prison officers undertake their duties. It improved the performance and operation of prison administration and prison staff duties and responsibilities. It brought the situation when the prisoners have the chances of self-realization, contribute to the development of society, and have more ways to come in contact with families, friends and supporters.

The question is that how this new prison environment when ICT influence on all area of prison institution could be more sustainable in coming years and not become more critical and dangerous.

The ICT development is dynamic process. The potential for the application of new technological products and devices is immense. The following is the list of potential ICT which could be applicable in near term:

- A computerized system that predicts potential trouble spots within prisons, allowing managers to assign extra staff or take other actions to prevent violence and other problems. Dubbed *COTAS* (Correctional Operational Trend Analysis System), the system uses information about prisoners — such as age, gang

membership, escape attempts, violent incidents, and medical and psychological conditions — to predict potential trouble spots. [12]

- *Prison Cloud* (Belgium Prison Service) - active participation of inmates to the prison internal and external information system (Intranet and Internet); organizing and supervising the daily activities of inmates into the unified information system. For example, Belgium prison authorities introduced a new web-based, multi-agency, multi-lingual integrated detention management system. It include prison life (prison banking and shopping), communication (internal message system and video-calling), education and training (E-learning, library and job searching before release), legal(access to judicial files) and leisure (movie rental and cable TV service) activities of all inmates in particular prison institution. [15]
- *E-learning* (further progress). There are a lot of opportunities to enhance the level of E-learning in prison institutions - In the future their might be learning applications on mobile devices like notebooks or personal digital assistants (PDA) to provide inmates with appropriate learning material in an effective way. Prisons need pedagogical and technical advice and finally have to decide which educational setting (pedagogical approach, learning content, technology and organizational environment) has to be introduced. From a technical point of view all means for running a secure educational technology in prison can be provided. In addition prisons have to care about organizational means to support secure operation of the system.
- *The security information system in prison institutions* – The proper training of prison staff and prisoners (dealing with technology). The special educational and training programs for them.
- *Controlled access to web content for prisoners* (Internet) - access to web content should be based on three criteria: controls which protect the system from misuse; the quality, extent and nature of the content; and the accessibility of ICT within the prison environment. [16]

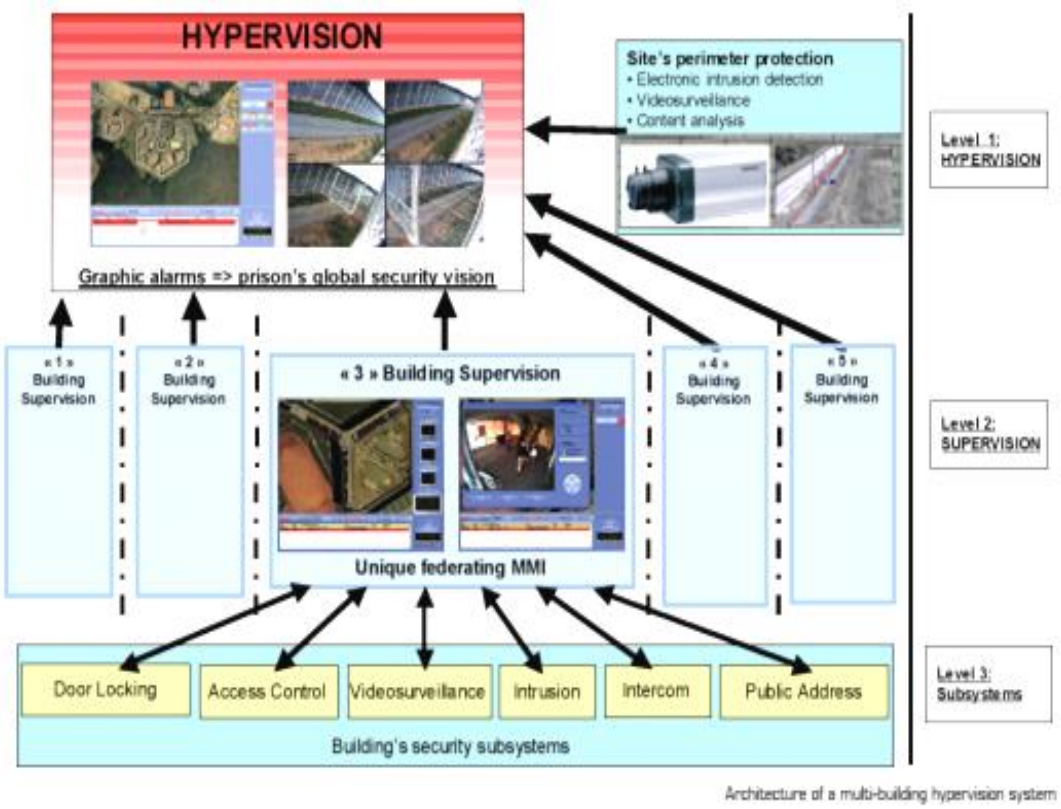


Figure 4 The future model of ICT impact on prison activity- The Fleury Mérogis project (French private company and security solution provider) [7]

The Fleury Mérogis project at a glance [7]:

- 46,000 field sensors (2,000 access points, 500 cameras, 3,300 intercoms), giving a total of 138,000 potential alarm conditions;
- Over 100 operator stations distributed among five supervision sub-servers and one central hyper vision server;
- 4,000 inmates, 1,000 prison officers, total area: 25 hectares.

REFERENCES

[1] U.S. Congress, Office of Technology Assessment: *Criminal Justice, New Technologies, and the Constitution*, OTA-CIT-366 (Washington, DC: U.S. Government Printing Office) p.31. (1998) URL.: https://www.princeton.edu/~ota/disk2/1988/8809/8809.pdf (Viewed 4 Dec 2016)

[2] TENIBIAJE, D. J.: Literacy, Information and Communication Technology as Tools for Empowerment of Inmates, EUROPEAN JOURNAL OF EDUCATIONAL RESEARCH Vol. 1, No. 2 (ISSN 2165-8714), pp.117-126.. (2012) URL.: http://www.eu-jer.com/EU-JER_1_2_117_Joseph.pdf (Viewed 3 Dec 2016)

[3] HAIG Zs., Connections between cyber warfare and information operations, AARMS, Vol. 8, No. 2, pp.329–337, (2009) URL.: http://www.zmne.hu/aarms/docs/Volume8/Issue2/pdf/13haig.pdf (Viewed Viewed 4 Dec 2016)

[4] HART, S. V.: Making Prisons Safer through Technology, By, Corrections Today, Vol. 65, No. 2, (2003) URL.: https://www.ncjrs.gov/pdffiles1/nij/04_03.pdf (Viewed 2 Dec 2016)

[5] SCHMALLEGER, F., SMYKLA O. J.: Corrections in the 21st century, Glencoe/McGraw-Hill, (ISBN: 0-02-802567-9) pp.186-18. (2000)

[6] Hungarian Prison Service Yearbook (ISSN: 1587-2319) 2014, (Büntetés-végrehajtási Szervezet, Évkönyv 2014)

[7] www.thalesgroup.com/seciruty-services (Viewed 4Dec 2016)

[8] ALLARD T., WORTLEY R., and STEWART A.: The Purposes of CCTV in Prison. URL.: https://www98.griffith.edu.au/dspace/bitstream/10072/13693/1/33137_1.pdf (Viewed 2 Dec 2016)

[9] STOLLER E. NANCY, STRUPP H.: Technology and Dehumanization in U.S. Prisons (Presentation), Public Health through the Bars. (2002) URL.: https://cjtc.ucsc.edu/PowerPoints/Technology-prison-apha.pdf (Viewed 2 Dec 2016)

[10] LOCKITT G. W.: Technology in prisons, Report by, Winston Churchill Travelling Fellowship, (2011) URL.: https://www.wcmt.org.uk/sites/default/files/migrated-reports/797_1.pdf (Viewed 4 Dec 2016)

[11] JUNGEN, A.: GPS Ankle Bracelet Monitoring of Low-Risk Offenders Costs More than Anticipated, La Crosse Tribune, Wis. (2016) URL.: http://www.govtech.com/public-safety/GPS-Ankle-Bracelet-Monitoring-of-Low-Risk- Offenders-Costs-More-than-Anticipated.html (Viewed 3 Dec 2016)

[12] DIGARD L., DI Z. M., YARONI A., and RINALDI J.: A New Role for Technology? Implementing Video Visitation in Prison. New York, NY: Vera Institute of Justice. (2016) URL.: https://www.vera.org/publications/video-visitation-in-prison (Viewed 3 Dec 2016)

[13] RUZSONYI, P.: Prison and crime prevention – crime prevention through prisoners' preparation for successful reintegration, 4th International scientific and professional conference 'police college research days in Zagreb', Zagreb, Croatia, 23-24 April 2015 pp.221-241(ISBN 978-953-161-291-6): URL.: https://www.mup.hr/UserDocsImages/PA/vps/idvps2015/Zbornik_sa%C5%BEetaka_Konferencije.pdf (Viewed 4 Dec 2016)

[14] BULMAN P.: Using Technology to Make Prisons and Jails Safer, p.4. URL.: https://www.ncjrs.gov/pdffiles1/nij/225764.pdf (Viewed 2 Dec 2016).

[15] MEURISSE H.: The use of modern technologies and the impact on prison life, Director General EPI, Belgium. URL.: https://www.coe.int/t/DGHL/.../PRISONS/...20.../Hans%20MEURISSE%20presentation.pdf (Viewed 4 Dec 2016)

[16] KIMMETT E.: Through the gateway: How Computers Can Transform Rehabilitation, Nina Champion, p.6. (2013) URL.: https://www.prisonreformtrust.org.uk/portals/0/documents/through%20the%20gateway.pdf (Viewed 3 Dec 2016)

HADMÉRNÖK

XII. Évfolyam 1 szám – 2017. március

CISCO HÁLÓZATI AKADÉMIAI KÉPZÉS-NETACAD PROGRAM

CISCO NETWORKING ACADEMY TRAINING-NETACAD PROGRAM

JOBBÁGY Szabolcs

(ORCID: 0000-0002-2104-4665)

jobbagy.szabolcs@uni-nke.hu

Absztrakt

Jelen publikációban egy cikksorozat egyik elemeként egy átfogó képet szeretnék adni a CISCO Hálózati Akadémia – NetAcad rendszerről, valamint az ennek keretében biztosított CISCO Hálózati Akadémiai Képzésről – NetAcad Programról általánosságban.

Kulcsszavak: *CISCO Hálózati Akadémiai, NetAcad rendszer, CISCO Hálózati Akadémiai Képzés, NetAcad Program, CISCO Akadémia, CISCO minősítések*

Abstract

In my publication as one of a series of articles I would like to give an overall picture about The CISCO Networking Academy – NetAcad System and also about in this context provided CISCO Networking Academy Training – NetAcad Program as a general overview.

Keywords: *CISCO Networking Academy, NetAcad System, CISCO Networking Academy Training, NetAcad Program, CISCO Academy, CISCO certifications*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.04.

BEVEZETÉS

Mint az mindenki számára egyértelmű és nyilvánvaló, az információs társadalom mindenapjait éljük, globális, korszerű infokommunikációs hálózatok erőforrásait, szolgáltatásait vesszük igénybe, a negyedik generációs hadviselés, a kiberhadviselés küszöbén állunk, melynek nélkülözhetetlen alkotóeleme egy olyan szakember, képzett tiszt vagy tiszthelyettes, aki rendelkezik a szükséges korszerű, digitális, hálózatos ismeretekkel is.

A digitális, infokommunikációs korszak hatásai tehát a védelmi szférát sem hagyják érintetlenül. Ennek eredményeképpen például a Magyar Honvédség infokommunikációs hálózata is egy folyamatos és állandó megújuláson, változáson megy keresztül, melynek részét képezi többek között például a hálózati infrastruktúráját kiszolgáló hardver platform folyamatos cseréje és megújítása is, természetesen új szolgáltatások igénybevételének lehetőségével párhuzamosan. Ennek az átalakulásnak a következtében egyre nagyobb számban kerülnek implementálásra többek között CISCO eszközök (VoIP és IP telefónia végberendezések, hálózati aktív eszközök, video - telekonferencia berendezések, IP kamerák, műholdas összeköttetések megvalósítását biztosító eszközök, stb.) a különböző vezetés - irányítási rendszerek hatékony támogatására hivatott infokommunikációs hálózatokba, rendszerekbe, komplexumokba, stacioner és tábori helyszínekre, a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatába. Ezek hatékony és célorientált működtetéséhez viszont elengedhetetlenül szükséges e technológiáknak- és technikáknak az elvárt szinten történő ismerete és azok gyakorlati alkalmazásának képessége készség szinten.

Ez volt többek között az egyik meghatározó momentum, amit a CISCO System Incorporated nemzetközi IT nagyvállalat is megragadott a Hálózati Akadémiai Képzés - NetAcad Program útjára bocsátásának idején, ugyanis nagyon gyorsan belátta, és rájött arra, hogy piaci részesedését, profitját, vásárlói körének kiszélesítését úgy tudja a lehető legeredményesebben maximalizálni, ha az általa kifejlesztett technológiákat, eszközöket és szolgáltatásokat versenytársaihoz képest minél nagyobb arányban tudja értékesíteni, eljuttatni a potenciális ügyfelekhez. Ehhez viszont az szükséges, hogy annak felhasználói, igénybevevői, a vásárlók ismerjék a benne rejlő lehetőségeket, legyenek képesek azt saját infokommunikációs hálózataikba implementálni, konfigurálni, menedzselni, hiba elhárítani, ne féljenek használni, bizalmat szavazzanak neki, stb. E tudat minél széles körben történő elültetése legkiválóbb táptalajának pedig ennek a globális oktatási, tanulási, karrierépítési, munkaerő piaci virtuális online közösségnek a kialakítása, a CISCO Hálózati Akadémia Képzés - NetAcad Program megálmodása és bevezetése bizonyult e - learning formában, mely a részvevők számát figyelembe véve nagyon sikeresnek bizonyul napjainkban is, és vélhetően ez a tendencia fog érvényesülni a közeljövőben is. Ennek keretében ugyanis lehetősége van a részvevőknek elméleti ismereteket elsajátítani, és gyakorlati készségeket szerezni az adott technológiák- és technikák vonatkozásában oly módon, hogy mindeközben a munkaerőpiacon is jelentős mértékben felértékelődik értékük, és egy globális szinten elismert iparági minősítést kapnak az adott képzési szintnek megfelelően. Megítélésem szerint ennek lehet részese a Magyar Honvédség, az a szakmai állomány, az a fiatal, felsőoktatásban tanulmányaikat folytató leendő híradó vagy informatikus tiszt vagy tiszthelyettes is, akit erre a képzésre a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Üzemeltető Intézet (NKE HHK KÜI) Híradó Tanszék gondozásban működtetett CISCO Akadémia képzéseire, kurzusaira beiskoláznak.

Mindezeken túlmenően elmondhatjuk azt, hogy a technológiai- és technikai megújulással karöltve, eleget téve többek között a különböző szövetségesi tagságunkból adódó kötelezettségeknek és elvárásoknak, a Magyar Honvédség szervezetén belül is folyamatosan jelennek meg például azok a szervezeti elemek, melyek ilyen ismeretekkel is rendelkező szakemberek beosztásba helyezését igénylik. Ennek egyik eklatáns példája lehet például a

Nemzeti Telepíthető Híradó- és Informatikai Század (DCM - E[1]), ahol alapvető igény mutatkozhat ilyen képzettséggel rendelkező szakemberekre. Mi sem bizonyítja ezt jobban, minthogy például a század szervezeti felépítésben megtalálható híradó és informatikai szakaszon belül kialakításra kerültek többek között LAN és WAN[2], VoIP és VTC[3] rajok, de ezt igazolja a feladatrendszere is. Másik kiemelkedő példaként hozhatnám fel a Katonai Nemzetbiztonsági Szolgálatot (KNBSZ[4]), melynek releváns szervezeti elemei a kiberhadviseléshez kapcsolódó feladatok és tevékenységek érdekében igénylik többek között az ilyen jellegű ismeretekkel is felvértezett szakembereket. Ehhez kapcsolódóan többek között az oktatás fontosságára világított rá a kiberbiztonságot illetően Dr. Kassai Károly ezredes a „Kommunikáció 2016" Nemzetközi Tudományos - Szakmai Konferencia keretében elhangzott előadásában alapul véve a 1139/2013 (III. 21.) Kormányhatározatot Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Ennek értelmében „*A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.*" [1] Viszont véleményem szerint jelenleg az ilyen jellegű beosztások, szervezeti elemek, alegységek feltöltése a megfelelően képzett szakembergárda hiányában nehézségekbe ütközhet. Meglátásom szerint olyan tisztek és tiszthelyettesek képzésére van tehát szükség, akik hasonló ismeretekkel rendelkeznek, mint más szövetséges tagországok tisztjei és tiszthelyettesei annak érdekében, hogy ne csak az egyes tagországok infokommunikációs hálózatai legyenek képesek egymással együttműködni, hanem maga az azt kiszolgáló szakmai, személyi állomány is. Nagyon sok külföldi példát hozhatnánk fel egyrészt más nemzetek haderejének alapvető képzési bázisát adó katonai felsőoktatási intézmények vonatkozásában (pl. Franciaország Saint - Cyr), másrészt különböző szintű szakmai tanfolyami képzési lehetőségek (USA híradó hadnagyi és századosi tanfolyamok) tekintetében, melyek mindegyikének szerves részét képezi már évek óta a CISCO, a hálózati ismeretek valamilyen formában történő oktatása az érintett szakemberek részére.

Érvként sorakoztathatnám fel a képzés szükségessége és pozitív hozadékainak sorában azt az alapvető tényt is, hogy az online, e - learning oktatási anyagnak nagyon sok más idegen nyelvre történő lokalizálása mellett, az angol nyelvű oktatási hátterének köszönhetően a képzésben részvevők a szakmai ismeretek elsajátítása mellett elsajátíthatják az angol nyelvű szakterminológiát is, mindamellett, hogy a nyelv általános ismeretének fejlesztése és folyamatosan történő szinten tartására is egy alapvető lehetőségként kínálkozik. A gyakorlati ismeretek alkalmazása során nagyon sok esetben akár honi, akár idegen nemzet területén végrehajtott gyakorlatok, képzések, felkészítések, szélsőséges esetben éles helyzetek, hadműveletek végrehajtása során más nemzetek katonáival történő együttműködés érdekében az angol nyelv, a szaknyelv ismerete alapvető kritériumként fogalmazódik meg.

Az érvek és tények sorozatát azzal szeretném zárni, hogy nem egy alkalommal tett látogatást a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karán más külföldi ország katonai felsőoktatási intézményének delegációja keresve az együttműködés lehetőségét hallgatóik egyetemünkön történő beiskolázására valamilyen kiajánlott képzést illetően. Előzetes visszajelzések alapján e kiajánlott képzések között is kiemelkedő figyelem

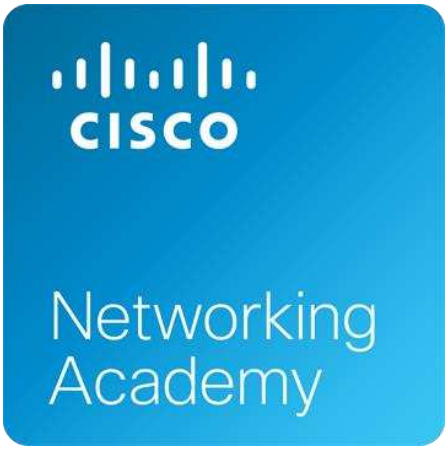
[1] Deployable CIS Module - E (NATO CIS Group (NCISG) 3. NATO Signal Battalion (NSB) Deployable CIS Module)
[2] Wide Area Network
[3] Video Teleconferencing
[4] Katonai Nemzetbiztonsági Szolgálat

és lehetséges igény merülne fel a hálózati informatikai képzés iránt, a CISCO Hálózati Akadémiai Képzést - NetAcad Programot illetően. Ennek legutóbbi sikeres megmutatkozását bizonyítja egy algír delegáció 2015 - ben egyetemünkön tett látogatása, ahol, mint oktató és előadó képviselve a Híradó Tanszéket, lehetőségem nyílott a hálózati akadémiai képzés tanszékünk által biztosított formában történő bemutatására, népszerűsítésére, kiajánlására.

CISCO HÁLÓZATI AKADÉMIA KÉPZÉS-NETACAD PROGRAM

A CISCO Hálózati Akadémia vagy másik nevén a NetAcad[5] rendszere egy globálisan elérhető, IT szakképzettséget adó, szakértelmet biztosító, képességeket fejlesztő, és egyben az e szakterületen karrierépítésre és elhelyezkedésre lehetőséget biztosító képzési rendszer, online, e - learning oktatási- és tanulási felület (NetSpace[6]), munkaerőpiac, tudásbázis és virtuális közösség is egyben. Egy széleskörű, műszaki tudomány jellegű technológiai program.

A CISCO Hálózati Akadémia - Netacad, mint oktatási-, képzési rendszer 1997-ben került megálmodásra és megvalósításra korunk egyik legjelentősebb IT nagyvállalata, a San Francisco- i székhelyű CISCO Systems Incorporated nemzetközi nagyvállalat által. Találóan a város nevéből ered elnevezése, továbbá logójában is magában hordozza a központjának otthont adó hely egyik nevezetességének, a Golden Gate hídnak a sziluettjét, mint az a lentebbi ábrán is látható.



1. ábra A CISCO Hálózati Akadémia logója [2]

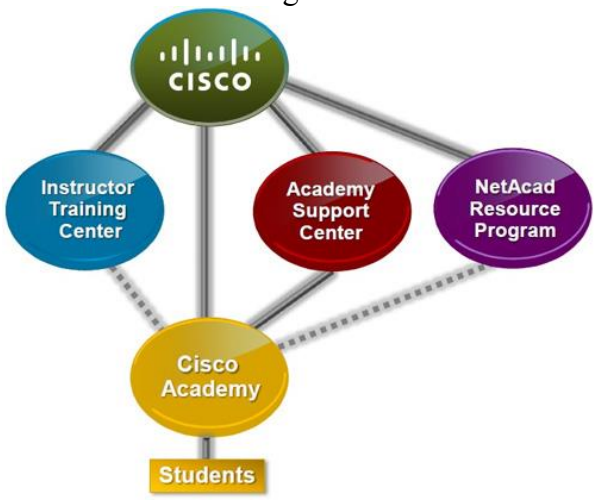
Magyarországon 1999 - ben került sor bevezetésére, és azóta is töretlen lendülettel képzi az IT szakterület szakembereit, legyen szó akár középiskolás tanulmányaikat folytató, az „y" sőt már az „α" generációt képviselő diákokról, felsőfokú képzésben részvevő hallgatókról, vagy minden olyan, a szakterület iránt elhivatottan érdeklődő egyénről, akik korszerű ismeretekkel felvértezve, az információs társadalom polgáraiként, a mindennapi megélhetésük biztosításának reményében, a legjobb szakemberek közé szeretnének tartozni, a lehető legmagasabb szintű iparági minősítések megszerzése által. Globális jellegét misem bizonyítja jobban, minthogy több mint százhetven ország, nem kevesebb, mint kilencezer oktatási

[5] CISCO Networking Academy

[6] A CISCO Hálózati Akadémia - NetAcad rendszer online, e - learning oktatási portálja, kezelőfelülete, mely mind az oktatók, mind a tanulók részére hozzáférést biztosít a tancsoportokhoz, tananyagokhoz, segédanyagokhoz, alkalmazásokhoz, az akadémiai rendszerrel kapcsolatos újdonságokhoz, hírekhez, összességében ehhez a globális közösséghez minden lehetőségével és erőforrásával.

intézményében vagy valamilyen szervezet, vállalat által biztosított képzés, oktatás keretében érhető el az így létrejövő Hálózati Akadémiák rendszere által biztosított különböző szintű és tartalmú kurzusok széles tárháza. Napjainkban közel hat millió ember alkotja akár oktatóként, akár hallgatóként, akár támogatóként ennek a globális közösségnek a humán erőforrás részét, mely egyben kimeríthetetlen szellemi kapacitását, tőkéjét is megtestesíti. Ennek az IT képességfejlesztő és karrierépítő programnak a segítségével a CISCO arra törekszik, hogy egyetlen oktatási platformon belül biztosítson minden szükséges erőforrást, ismeretet, tudásanyagot a hallgatóknak, annak érdekében, hogy egy magasan kvalifikált, jól fizetett, a munkaerőpiacon keresett, és magasan pozícionált értékkel bíró munkavállalóként legyenek képesek megjelenni és jelen lenni. Megmutatja nekik, hogy mit kell tenniük, milyen ismereteket kell elsajátítaniuk annak érdekében, hogy azt a munkát, amit szeretnek, a lehető legjobban tudják ellátni. Ezen okból kifolyólag a képzés érinti többek között a tejesség igénye nélkül napjaink legkorszerűbb, aktuális hálózati, biztonsági, a felhő alapú számítástechnikához kapcsolódó technológiákat- és technikákat, megoldásokat és eljárásokat, amelyek készség szintű elsajátítása érdekében, megragadva az információs társadalom egyik legnagyobb vívmányának az online, e - learning oktatásnak a lehetőségét, laborgyakorlatokkal, szimulációs és emulációs programok alkalmazásával készíti fel a hallgatókat az elméleti ismereteik gyakorlati keretek közé történő átültetésére. Ennek érdekében az akadémia képviselői folyamatosan együttműködnek az oktatókkal, munkáltatókkal, a szakterület élenjáró nagyvállalataival annak érdekében, hogy azonosítani tudják mindazokat a globális trendeket, igényeket és kihívásokat, amelyek mentén az akadémiai rendszer továbbfejlesztése, a hallgatók és természetesen az oktatók naprakész ismeretekkel történő felvértezése támogatott és biztosított.

A CISCO Hálózati Akadémia - NetAcad rendszerének szervezeti felépítése egy többszintű, hierarchikus tagozódást mutat. A továbbiakban a hazai viszonyokat, és az NKE HHK KÜI Híradó tanszék gondozásában működtetett CISCO Akadémiát (CA) érintő kérdéseket megfeleltetve ennek a szerkezeti modellnek fogom ismertetni az akadémiai rendszer saját elemeit és azok szerepét az alábbi ábrának megfelelően.



2. ábra A CISCO Hálózati Akadémia - NetAcad rendszerének strukturális felépítése [3]

A legmagasabb szinten maga a *CISCO Systems Incorporated IT nagyvállalat* áll, mint ennek a nemzetközi képzési, oktatási programnak a jogtulajdonosa. Szülőatyjaként legfelsőbb szintű felelőse a képzés gondozásának, mindenirányú biztosításának, támogatásának, továbbfejlesztésének, működtetésének.

A hierarchiában eggyel lentebb található szinten három különböző alkotóelemről kell, hogy beszéljünk, melyek az alábbiak [3]:

- Oktatóképző Központok (ITC[7]);
- Akadémiai Támogatóközpontok (ASC[8]);
- NetAcad Erőforrás Program (NRP[9]).

Az *Oktatóképző Központok (ITC)* felelősek akár a már működő, akár az újonnan megalapított CISCO Akadémiák oktatóinak a képzéséért különböző kurzusok, oktatások végrehajtása formájában. Természetesen az itt dolgozó oktatóknak magas követelményeknek, szigorú feltételeknek kell megfelelniük, és különböző szintű minősítéseket kell megszerezniük. Az az oktatási intézmény, vállalat vagy szervezet, aki részese akar lenni a CISCO Hálózati Akadémia - NetAcad rendszerének, annak tagjává kell, hogy váljon, és egy CISCO Akadémiát (CA) kell, hogy működtessen. Az akadémia különböző funkciókat betöltő személyekből épül fel úgy, mint akadémiai kapcsolattartó (Academy Contact), valamint az oktatók (Instructor). Minden egyes oktatónak, aki bármelyik szintű képzés kurzusait és a hozzá kapcsolódó tananyagokat oktatni szeretné, el kell végeznie az ahhoz kapcsolódó oktatóképző tanfolyamot. Ezt követően szerez jogosultságot arra, hogy elérje az e - learning webes portált, a NetSpace - t, tancsoportot hozzon létre, elindítson egy adott kurzust a hallgatóknak, hozzáférjen az online tananyagokhoz és minden oktatást támogató erőforráshoz, vizsgákat indíthasson, valamint a sikeres záróvizsgák letételét tanúsító igazolásokat központilag lekérje, és a végzett hallgatók részére azokat rendelkezésre bocsássa. A Híradó Tanszék által működtetett CA esetében ezt a szerepet a Hálózati Tudás Terjesztéséért Programiroda Alapítványa (HTTP) tölti be egy részletesen szabályozott, a CA oktatóinak szakmai továbbképzéséről szóló szolgáltatói megállapodás keretében. Magyarországon jelen pillanatban két másik intézmény, szervezet rendelkezik ehhez a szerepkörhöz dedikált jogok gyakorlásával, mégpedig a Győri Műszaki Szakképzési Centrum Jedlik Ányos Gépipari és Informatikai Szakgimnáziuma, Szakközépiskolája és Kollégiuma, valamint a Pannon Egyetem. Az imént említett szerződés rögzíti mind az ASC, mind pedig a CA jogait és kötelességeit az oktatók továbbképzésének vonatkozásában. Ez a képzési szolgáltatásra vonatkozó megállapodás kiegészítő részét képezi a CISCO Akadémia CISCO Hálózati Akadémiai - NetAcad tagságának, működésének és támogatásának biztosítását szolgáló támogatói megállapodásnak az ASC valamint a CA között.

Az *Akadémiai Támogatóközpontok (ASC)* hivatottak arra, hogy különböző szintű szolgáltatások, támogatások biztosításával hatékonyan hozzájáruljanak a CISCO Akadémiák működéséhez, az ott folyó képzések sikeréhez. Valamennyi működő vagy létrejövő CISCO Akadémiának kötelező csatlakoznia, tartoznia valamelyik Akadémiai Támogatóközponthoz. [4] A Híradó Tanszék gondozásában működő CA vonatkozásában az ASC szerepét ugyan úgy, mint a korábban ismertetett Oktatóképző Központ funkcióját szintén a Hálózati Tudás Terjesztéséért Programiroda Alapítvány tölti be. Természetesen nem Ő az egyetlen ASC hazánkban, viszont 2011 - ben a CISCO Hálózati Akadémiai Képzés - NetAcad Program jelentős és alapvető megreformálását követően, melyet Academy Evolution folyamatnak neveztek, Ő volt az első szervezet, aki ebben a szerepkörben, mint egykori Regionális Akadémia megjelent. Az Academy Evolution folyamatot megelőző időszak CISCO Hálózati Akadémia - NetAcad rendszerének felépítésére terjedelmi korlátok miatt nem kívánok kitérni. Mellette 2013 - ban sikeresen pályázott és nyerte el e funkció betöltésének lehetőségét a Pannon Egyetem. [4] A támogatásnak az alapja egy támogatói megállapodás, mely

[7] Instructor Training Center
[8] Academy Support Center
[9] NetAcad Resource Program

vonatkozik mind a CISCO Hálózati Akadémiai - NetAcad tagságra, mind az annak keretében folyó képzésre, mind pedig az ahhoz kapcsolódó szolgáltatásra. Továbbá a szerződés mind a két fél, a CA és az ASC részére is megfogalmaz jogokat és kötelezettségeket az akadémiai programban történő magas színvonalú és eredményes részvétel érdekében.

Ezen a szinten található utolsó alapvető strukturális elem a *NetAcad Erőforrás Program (NRP)*. Ezt alapvetően olyan szervezetek, támogatók, külső szereplők, partnerek, kapcsolattartók alkotják világszerte, akik különböző eszközökkel, megoldásokkal, eljárásokkal megpróbálnak hozzájárulni a CISCO Hálózati Akadémiai Képzéshez - NetAcad Programhoz azáltal, hogy plusz értékekkel, új szolgáltatásokkal bővítik azt annak érdekében, hogy az minél sikeresebb legyen, valamint az oktatás minősége minél magasabb szintet érjen el. [3] Ennek az erőforrásprogramnak a részét képezi többek között a teljesség igénye nélkül a tananyagfejlesztésre vonatkozó törekvések megvalósítása is, melynek kiemelkedő képviselője és jelenleg, mint egyetlen NRP szereplője a CISCO Hálózati Akadémiai Képzés - NetAcad Program magyarországi piacának az Observans Képzési Szolgáltató Kft[10]. [5]

A hierarchikus szerkezeti modell következő, alsóbb szintjén maguk a *CISCO Akadémiák* (CA) foglalnak helyet, akik a CISCO Hálózati Akadémiai Képzés - NetAcad Program legalapvetőbb alkotóelemeinek, mozgatórugóinak, a hallgatók tényleges oktatásáért, képzéséért, vizsgára, versenyekre történő felkészítéséért felelősek többek között. Világszerte ezek az akadémiák számtalan képzés, kurzus teljesítését teszik lehetővé hallgatóik részére, melyek szinte az IT világ teljes hálózati szegmensét lefedik. A CISCO Hálózati Akadémiai Képzés - NetAcad Programban elérhető képzési szinteket, képzéseket, kurzusokat és a megszerezhető minősítések, képesítések hierarchikus egymásra épülését szemlélteti a teljesség igénye nélkül a következő két ábra.

[10] Fő profilja a felnőttképzés, tartalomszolgáltatás, tartalomfejlesztés az infokommunikáció vívmányainak alkalmazásával, törekedve a kommunikációs folyamatok hatékonyságának növelésére.

3. ábra A CISCO Career Certifications [6] [7]

4. ábra A CISCO Career Certifications Hierarchy [8] [9]

Mint azt a fentebbi két ábrából is jól láthatjuk, a teljesség igénye nélkül, alapvetően öt különböző képzési szintet különböztethetünk meg. Ezek mindegyike más és más területeket érintő, eltérő mélységű ismeretekkel vértezi fel a hallgatókat, és ezen okból kifolyólag természetesen más és más szintű minősítéseket, képesítéseket is biztosít számukra, ami pedig alapvetően determinálja az azokkal betölthető állásokat, munkaköröket, pozíciókat, kompetencia szinteket. Ez az öt képzési szint a következő:

- IT Essentials PC Hardware and Software;
- Entry level;
- Associate level;
- Professional level;
- Expert level.

Nem esett még szó a CISCO Hálózati Akadémia - NetAcad rendszer egyik legfontosabb alkotóeleméről, magáról a *hallgatóról*, aki vagy azért mert karrierépítésbe szeretne kezdeni az IT területen,vagy azért mert a szakképzés rendszerében ebben a formában kell eleget tennie tanulmányi kötelezettségeinek, vagy azért mert pusztán érdeklődik ezen IT szegmens iránt, és szeretné bővíteni ismereteit, de csatlakozott a képzéshez, programhoz, kurzusokat teljesít, és eredményes iparági minősítő vizsgákat tesz a különböző minősítések, képesítések megszerzése érdekében. Bárki részese lehet ennek az e - learning oktatási, képzési, IT ismereteket adó, IT készségeket fejlesztő, IT szakképzettséget biztosító, IT szakértelmet nyújtó, az IT területen karrierépítésre lehetőséget teremtő programnak, globális online közösségnek, tudásbázisnak, munkaerőpiacnak, ennek a széleskörű, műszaki tudomány jellegű technológiai programnak egy CA közreműködésével, a NetSpace felület által. Ez utóbbi, mint azt már korábban említettem volt, nem más, mint a CISCO Hálózati Akadémia - NetAcad rendszer online, e - learning oktatási, képzési portálja, kezelőfelülete, mely többek között mind az oktatók, mind a tanulók részére hozzáférést biztosít a kurzusokhoz,

képzésekhez, tancsoportokhoz, tananyagokhoz, segédanyagokhoz, alkalmazásokhoz, az akadémiai rendszerrel kapcsolatos újdonságokhoz, hírekhez, összességében ehhez a globális közösséghez minden lehetőségével és erőforrásával. A NetSpace felület a www.netacad.com linken keresztül érhető el akár az oktatók, akár a hallgatók részére, természetesen a bejelentkezést követően más és más felületekhez való hozzáférést biztosítva. Ez az új felület ugyancsak a már korábban említett Academy Evolution folyamatnak az eredményeképpen jött létre, és váltotta le a korábbi hasonló funkciókkal, szolgáltatásokkal és lehetőségekkel rendelkező Academy Connection felületet. A NetSpace valójában egy tanulási környezet, mely tartalmazza magát az e - learning tananyagot interaktív médiatartalmakkal, beágyazott feladatokkal, parancs szimulátorral, szimulációs Packet Tracer feladatokkal, fizikai és távoli elérésű laborgyakorlatokkal, tesztfeladatokkal, a különböző kurzusokon belül a tanulók elektronikus leckekönyvét, egy adott kurzus teljesítéséhez szükséges próba és éles elméleti és gyakorlati záróvizsga feladatokat, a különböző iparági minősítő vizsgákra történő felkészülést segítő próbavizsgákat. Mindezek részét képzik az úgynevezett e - doing folyamatnak, melynek legfontosabb célja a hatékony tanulás ösztönzése, a megszerzett tudás megtartásának elősegítése, a tananyag megértésének megkönnyítése, összességében élvezhetővé és élményekkel telivé tenni ezt az e - learning környezetet. A képzés, program keretében a hallgatónak a NetSpace felületen keresztül van lehetősége akár oktató által irányított, akár önállóan teljesíthető kurzusokon való részvételre és vizsgázásra is. A hallgatók teljesítménymutatói több szinten és formában kerülnek mérésre. Ennek keretében, mint azt a későbbiekben, az egyes kurzusok, minősítések és képesítések részletesebb ismertetésénél látni fogjuk, minden egyes kurzusfejezet végén szükséges egy online fejezetzáró vizsga, teszt kitöltése, és annak elvárt szinten történő teljesítése. Majd ezt követően a kurzus zárásaként, meghatározott alkalommal egy online elméleti és egy laborban végrehajtott gyakorlati záróvizsga teljesítése szükséges annak érdekében, hogy a kurzus elvégzését tanúsító igazolás a hallgató részére kiállítható legyen. Ezt követően van lehetősége egy akkreditált, külön erre a célra kijelölt vizsgahelyszínen ipari minősítő vizsgát tenni, és minősítést, képesítést szerezni, melynek költsége jelentős mértékben csökkenthető az egyes képzési szintek kurzusai mérföldköveinek számító online elméleti záróvizsgák első alkalommal bizonyos szinten történő teljesítése esetén. A korábban említett fejezet és kurzuszáró vizsgák, melyek valamelyik CA közreműködésével tehetőek le az adott kurzus keretében, ingyenesek mindamellett, hogy egy - egy kurzuson történő részvétel a választott CA függvényében egy bizonyos költséggel jár. Természetesen mivel a Híradó Tanszék által működtetett CA keretében a hallgatók tantárgyiasított keretek között vesznek részt a CISCO Hálózati Akadémiai Képzésben - Netacad Programban, ezért ez számukra teljes egészében költségmentes, kivéve az iparági minősítő vizsgák letételét. Mivel a CISCO Hálózati Akadémia Képzés - NetAcad Program non - profit elven működik, ezért az ebből befolyó bevételeket a CA a korábban ismertetett ASC - vel kötött megállapodás értelmében az oktatásba, képzésbe és azok járulékos tevékenységeibe kell, hogy visszaforgassa.

KÖVETKEZTETÉSEK

A XXI. század új típusú társadalmi berendezkedésében, az információs társadalomban való tudatos, „digitális állampolgári”, valamint szakemberi lét elképzelhetetlen korszerű ismeretekkel, kompetenciákkal és megfelelő gyakorlati készségekkel, tapasztalattal való rendelkezés nélkül. Mindennapjainkban a különféle elektronikus és nyomtatott médiafelületek felhasználásával az állami szféra szereplői a digitális állam, a digitális írástudás megteremetése mellett kampányolnak, melyek megvalósítása érdekében a különböző szabályozói háttér megteremtése mellett változatosabbnál változatosabb eszközöket és lehetőségeket kínálnak. Ezek sorában megemlíthetjük többek között a teljesség igénye nélkül a digitális jóléti programokat, a szélessávú Internet hozzáférés lehetőségének szinte mindenki

számára történő biztosítását, vagy olyan speciálisan erre a célra kifejlesztett korszerű megoldásokat, mint a Mobidik konténer. Ez utóbbi például egy olyan oktatástechnikai fejlesztés, mely egy mobil, a legmodernebb számítástechnikai eszközökkel felszerelt tanterem formájában, Magyarország digitális oktatási stratégiájának bevezetését támogatja a köznevelésben.

Mint azt a fenti okfejtésből is láthatjuk, e modern és korszerű ismeretek és készségek megszerzésének egyik alapvető, kiemelkedő és legmegfelelőbb módja az oktatás és képzés, mely történhet akár szervezett, akár egyéni keretek között is. Erre kínál egy kiváló alternatívát a CISCO Hálózati Akadémiai Képzés – NetAcad Program is, és az annak keretében különböző szinteken elérhető képzések, kurzusok, melyek alapvetően az IT világ hálózati informatikával kapcsolatos szegmensében segítenek elmélyülni. Az oktatásban, képzésben való részvétel mellett, annak érdekében, hogy a megszerzett ismereteink és gyakorlati készségeink hitelt érdemlően igazolásra, bizonyításra kerüljenek, valamint a munkaerő piacon értékkel bíró munkavállalóként jelenjünk meg, az egyes képzések, kurzusok sikeres elvégzését követően iparági minősítő vizsgák sikeres abszolválása által globálisan is elismert iparági minősítések, képesítések birtokába juthatunk.

Mivel egyrészt az információs társadalom hatásai a védelmi szféra szereplőit sem hagyják érintetlenül, másrészt mivel ebben az új korban, a negyedik generációs hadviselés korszakában a megjelenő új típusú kihívások, fenyegetések és egyben lehetőségek is egy modern digitális hadszíntéren jelennek meg, ezért a haderő érintett szakmai személyi állományának is ezekkel a korszerű ismeretekkel és gyakorlati készségekkel rendelkeznie kell. [10; 11] A Magyar Honvédség különböző szervezeteinek, egységeinek és alegységeinek híradó és informatikai szakbeosztású állománya a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Üzemeltető Intézet Híradó Tanszéke által működtetett CISCO Akadémia képzései, kurzusai által részesévé válhat, bekapcsolódhat a CISCO Hálózati Akadémiai Képzésbe – NetAcad Programba. Ennek köszönhetően azon túlmenően, hogy a szervezet számára a követelmények teljesítése, a kihívásokra adandó megfelelő reagálás, és hatékony válaszok kialakítása érdekében nélkülözhetetlen és hasznos kompetenciákkal vértezi fel az egyént, a civil szféra IT szegmensének munkaerőpiacán is értékkel bíró, versenyképes szereplővé teszi Őt, mely egy esetleges a szervezetből történő kiválás esetén megkönnyíti a civil szakmai társadalomba történő integrációját, tudásának átültetését. [12]

FELHASZNÁLT IRODALOM

[1] 1139/2013. (III.21.) Kormány határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (letöltve: 2017.02.12.)

[2] http://netacad.hu/hu/ciscohalozatiakademia (letöltve: 2017.02.12.)

[3] http://www.netacad.hu/akademiai_rendszer (letöltve: 2017.02.12.)

[4] http://www.netacad.hu/ciscohalozatiakademia_hu (letöltve: 2017.02.12.)

[5] http://www.observans.hu/ (letöltve: 2017.02.12.)

[6] https://learningnetwork.cisco.com/community/certifications (letöltve: 2017.02.12.)

[7] https://www.netacad.com/careers/certifications/ (letöltve: 2017.02.12.)

[8] http://www.tomsitpro.com/articles/online-cisco-certification-resources,5-75.html letöltve: 2017.02.12.)

[9] http://cisco.jedlik.eu/index.php?page=4 (letöltve: 2017.02.12.)

[10] FARKAS T.: Signal Officer Training at the National University of Public Service (Budapest, Hungary) In: ŠOSTRONEK M., BEREŠIK R., BABJAK M., SPILÁ D. (szerk.) New Trends in Signal Processing 2014: Proceedings of the International Conference : 15-17 October 2014, Tatranské Zruby, Slovakia. Konferencia helye, ideje: Tatranské Zruby, Szlovákia, 2014.10.15-2014.10.17. Liptovski Mikulas: Armed Forces Academy of General Milan Rastislav Štefánik, 2014. pp. 37-43.

[11] FARKAS T.:CIS officer training at the National University of Public Service: capabilities and requirements In: Hruby M. (szerk.) Distance Learning, Simulation and Communication (DLSC) Conference. Konferencia helye, ideje: Brno, Csehország, 2015.05.19-2015.05.21. Brno: University of Defence Faculty of Military Technology, 2015. pp. 84-90.

[12] FARKAS T., JOBBÁGY SZ.: Cisco Networking Academy for signal officer training; a "Kommunikáció 2011" nemzetközi szakmai tudományos konferencia előadása; 2011. november 15

HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

A DÖNTÉSKÉPESSÉG PROBLÉMÁJA A VÉDELMI SZFÉRÁBAN

DECIDABLENESS IN THE DEFENCE SPHERE

KUN István

(ORCID: 0000-0003-1117-2433)

kunistvan47@gmail.com

Absztrakt

A védelmi szféra munkájában gyakran előforduló probléma, hogy intézkedni kell egy nemkívánatos esemény elhárítására, miközben az esemény bekövetkezéséről nincs biztos tudomásunk. Ilyen helyzet áll elő, ha például egy informatikai vagy fizikai támadás gyanúja merül fel. Az érintett szervezet hatékony működése szükségessé teszi az egyszerű és világos döntési kritériumok alkalmazását. Amikor testületi döntést kell hozni, a javaslat elfogadásához az „igen" szavazatoknak egy előzetes megállapodás szerinti aránya szükséges. Kérdés, hogy mekkora legyen ez az arány. A jelen tanulmány tárgya a testületi döntések adekvát konszenzushatárának megállapítását segítő, a szubjektivitást kiküszöbölő matematikai-informatikai elv bemutatása és igazolása.

Kulcsszavak: *védelmi igazgatás, kockázatkezelés, bizottsági szavazás, konszenzushatár*

Abstract

A frequently appearing problem in the work of the defence sphere is that some action must be taken in order to avoid an undesirable event while we have no secure information on the occurrence of the event. Such situation may emerge if for example the suspicion of an informatical or physical attack is encountered. Efficient operation of the organization concerned makes it necessary to apply simple and clear decision criteria. When a board decision must be made, a previously agreed ratio of „yes" votes is needed to adopt the resolution. The question is, how much this ratio should be. The topic of the present study is presentation and justification of a mathematical-informatical principle helping to state the adequate consensus threshold and eliminating subjectivity in board decisions.

Keywords: *defence administration, risk handling, committee voting, consensus threshold*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.25.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.24.

BEVEZETÉS

Amikor valamilyen kockázati rendszer nemkívánatos főeseményének valós veszélyként történő deklarálásáról – ami egyben a komoly ráfordításokat igénylő megelőző vagy védekező tevékenység beindítását is maga után vonja – kell testületi döntést hozni, akkor az elfogadáshoz az „igen" szavazatok egy előzetes megállapodás szerinti arányának elérése a feltétel. [1] Így felmerül a szavazási eredmény minősítésének a problémája, tehát az indítvány elfogadásához szükséges minimális szavazatarány, vagyis a konszenzushatár meghatározása.

A TESTÜLETI SZAVAZÁS PARADOXONAI

A testületi szavazás a hatalom megosztásának, demokrácia valamilyen szintű gyakorlásának legrégebbi eszköze, ezért legmegfelelőbb lebonyolítási formájának megtalálása már évezredek óta (gondoljunk csak az ókori athéni cserépszavazásra) filozófiai és matematikai kutatások tárgya. Az első tudományos igényű szavazáselméletet a tudós katalán szerzetes, Ramon Llull dolgozta ki [1], aki saját korának megfelelő megfogalmazásban lényegében megelőlegezte Borda és Condorcet fél évezreddel későbbi, alább ismertetendő gondolatait.

A szavazás elve központi témává a XVIII. század második felében, a rendi társadalomból a deklarált egyenlőség, és az ezzel együtt járó széles körű szavazati jog felé mozgó Franciaországban vált.

Hamar kiderült azonban, hogy nem egyszerű megfelelő szavazási elvet kidolgozni. Alapvető problémát jelent ugyanis, hogy egy legalább három alternatíva közötti választás esetében esetleg egyáltalán nem születik egyértelmű eredmény, vagy olyan eredmény születik, amelyet a többség ellenez.

A legdemokratikusabbnak a relatív többségi szavazás látszik, hiszen elvileg bárki indulhat azonos feltételek mellett, és egyszerű, egyértelmű szabály határozza meg a győztest: az nyer, aki a legtöbb szavazatot kapja. Mégis lehetséges, hogy a végeredmény nem a szavazók akaratát tükrözi. Ennek konkrét, komoly politikai következményekkel járó példája volt az 1912. évi amerikai elnökválasztás. A republikánus párt a szavazatok abszolút száma alapján fölényesen nyert volna, de végül a demokrata Thomas Woodrow Wilson 42 %-os országos szavazataránnyal is győzni tudott. A republikánus szavazatok ugyanis megoszlottak William Howard Taft és Theodore Roosevelt között, és ez a megosztottság az USA kétszintű választási rendszerében döntően befolyásolta az elnökválasztó elektori testület összetételét.

Bár az előbbi példát természetesen nem látták előre a XVIII. században, hasonló jellegű esetek előfordultak a Francia Akadémia tisztségeinek választásain. Ezekből okulva, a kor tudósai megoldást kerestek a többségi szavazás problémáinak kiküszöbölésére.

Az első, matematikailag megalapozott szavazási módszert Jean-Charles de Borda francia katonatiszt, matematikus és fizikus publikálta 1770-ben [2]. Borda ötlete az, hogy minden jelölt a helyezésének megfelelő pontszámot kap a választóktól, vagyis a választók teljes preferenciarendszerére kiterjed a szavazás. A módszer nagyon hasonló ahhoz, amit ma a pontozásos sportágakban alkalmaznak. Hátránya is nagyon hasonló. A Borda-paradoxon abban áll, hogy hiába nyeri el az egyik jelölt a legtöbb első helyezést a szavazóknál, mégse nyerheti meg a szavazást, ha a szavazótestület egy része durván lepontozza őt, mert akkor a pontösszesítésben alulmarad. Tehát könnyen manipulálható a végeredmény.

[1] Valójában azt is meg kell adni, hogy a teljes szavazótestület létszáma, vagy pedig a konkrét szavazásban részt vevő testületi tagok száma az arány viszonyítási alapja. Az itt felhasznált Moore-Shannon modellnek az első értelmezés felel meg.

Ennek a problémának a megoldására dolgozta ki Nicolas de Condorcet márki, matematikus és filozófus (további tudományterületeit nem említve), a Francia Akadémia tagja 1785-ben saját módszerét [3], de ez is paradoxonra vezethet. Condorcet a többségi elv helyett a páronkénti összehasonlítások alapján dönti el a választást.

A Condorcet-paradoxont egyszerű példán szemléltetjük. Tegyük fel, hogy egy adott célra A, B, C politikusok közül akarjuk a legjobbat kiválasztani. Három szempontból tudunk összehasonlítást tenni: szakszerűségi, morális, népszerűségi szempontból. Mindhárom szempontot egy-egy külön szakértői testület vizsgálja. Szakszerűségi szempontból A > B > C, morális szempontból B > C > A, népszerűségi szempontból C > A > B a sorrend.

Az első paradoxon abban áll, hogy ha egymástól teljesen függetlenül vizsgáljuk a három szempontot, akkor hiába van egyértelmű sorrend mindhárom szempont alapján, a végeredmény mégis holtverseny, tehát döntésképtelenség lesz.

A második paradoxonnal akkor találkozunk, ha fel akarjuk oldani a döntésképtelenséget oly módon, hogy többfordulós döntési folyamatot választunk, ahol mindegyik fordulóban az egyik döntési szempont alapján kizárjuk a mezőnyből az utolsó helyezettet. Ha a leggyengébb szakszerűségű jelöltet zárjuk ki először, akkor a C jelölt marad ki. Ezután legyen a moralitás a következő szempont. Ekkor A esik ki, és a B jelölt marad állva győztesként. Ha viszont a népszerűség az első szempont, akkor először a B jelölt esik ki. Legyen a szakszerűség a második szempont, ekkor a C jelölt esik ki, és marad győztesként az A jelölt. Vagyis hiába egyenrangúak elvileg a döntési szempontok, érvényesítésük sorrendje döntően befolyásolja a végeredményt.

Egy választási rendszer akkor felel meg a Condorcet-kritériumnak, ha mindig nyertesként hozza ki azt a jelöltet, aki külön-külön mindegyik másik jelöltet legyőzné. A fenti első példa mutatja, hogy nem mindegyik választási rendszerben található ilyen univerzális nyertes, tehát a Condorcet-kritérium nem feltétlenül biztosítja a döntésképességet.

Ismét más elv alapján történik a közvetett többszintű szavazás, amelyre példa az USA elnökválasztása. Ez az elv ugyancsak vezethet paradoxonhoz: a 2016. évi választáson olyan jelölt nyert, aki közvetlen szavazás esetén vesztett volna.

A felsorolt és további ismert választási rendszerek alapelveinek és hátrányainak bemutatása megtalálható a [4] cikkben.

A többségi elvű szavazási módszerek burkoltan arra a feltételezésre épülnek, hogy az a döntési alternatíva a leginkább megalapozott, amelyet a legtöbben tartanak annak. A tapasztalatok azonban ennek ellentmondanak. Felmerül a kérdés, mikor és milyen szavazatarány esetében indokolt a kisebbségi véleményt elfogadni.

A KONSZENZUSHATÁR PROBLÉMÁJA

Lehetséges-e, hogy a számbeli kisebbségben levőknek van igazuk a többséggel szemben?

Természetesen lehetséges. Gondoljunk csak Kasszandra trójai királylánynak az Iliászból ismert történetére: jóslatai kivétel nélkül beigazolódtak, mégis mindig kisebbségben maradt véleményével.

És ez rendszeresen előfordulhat a védelmi szférában, amikor információmorzsák alapján kell dönteni. Csak példaként:

- Adott előjelek alapján várható-e egy természeti vagy műszaki katasztrófa?
- Adott hírszerzési információk alapján várható-e egy bizonyos fajta informatikai vagy fizikai támadás?

A konszenzushatár megállapítása a gyakorlatban általában önkényes. Vagy valamilyen korábbi testületi döntésen, azaz precedensen, vagy politikai alkun nyugszik. Függ a döntés tárgyát képező kockázati esemény jellegétől, de nem függ annak logikai struktúrájától.

A logikai kockázatelemzés a *testületi döntés* illetve a döntés-előkészítési *tanácsadás* konszenzushatárának meghatározására is alkalmas. Az, hogy a döntés kisebbségi támogatással

is meghozható, összhangban van a védelmi igazgatás gondolkodásmódjával. A továbbiakban foglalkozunk majd ennek strukturális okaival.

MEGBÍZHATÓSÁGI MODELLEKEN ALAPULÓ SZAVAZÁSI RENDSZEREK

A fentebb tárgyalt tradicionális szavazási eljárások problémáit gyakran a konszenzushatár megállapításával lehet hatékonyan kezelni. Ez utóbbihoz viszont a logikai áramkörök megbízhatóbb működését segítő modellekkel juthatunk el.

A továbbiakban sorra vesszük ezen modellek legfontosabb típusait.

A Neumann-modell

Neumann János 1945-ben közzétette saját, EDVAC-nak [2] nevezett (1949-ben ténylegesen megvalósult) számítógép-koncepcióját [5]. Ebben már foglalkozott a megbízhatóság problémájával, amelyre 1952-ben megoldási javaslata is megszületett [6].

Felismerte, hogy a logikai áramkörök komponenseinek, ezen belül főleg az akkoriban általánosan használt elektroncsöveknek a jeltorzulásban megnyilvánuló megbízhatatlansága a gyártási és üzemeltetési problémák miatt elkerülhetetlen, és ennek hatására a teljes logikai áramkörök is megbízhatatlanok. A megbízhatatlanságon azt értette, hogy az áramkör kimeneti értékei a tervezett, az esetek nagy részében helyesen teljesített funkció szempontjából időnként irrelevánsak.

Neumann értelmezésében a megbízhatóság javítása olyan konstrukciós módosításokat jelent, amelyek megfelelően nagy biztonsággal lehetővé teszik a téves kimeneti értékek kiszűrését és korrekcióját. Ez a problémakör tehát közvetlenül nem érinti a megbízhatóság-elmélet olyan tipikus területeit, mint a hirtelen üzemképtelenné válás és az elöregedés okozta degradáció. Az áramkör elemeinek megbízhatósági szintjét Neumann időben állandónak feltételezte.

Neumann célul tűzte ki a saját komponenseinél megbízhatóbb, hibatűrő logikai áramkör tervezését. Komponensként gyakran NAND kapukat alkalmazott, mert így a NAND kapuk ismert tulajdonságát felhasználva egyetlen fajta komponenssel bármilyen logikai áramkört meg lehet valósítani.

A megfelelő mértékű hibajavítást redundancia alkalmazásával sikerült ténylegesen elérni . A konstrukció kétféle redundanciát tartalmaz, mert az eredeti komponenseket és a komponenseket összekötő kommunikációs vonalakat egyaránt megtöbbszörözi párhuzamosan beépített azonos kivitelezésű példányokkal. Amikor a végrehajtandó algoritmus előírja egy művelet elvégzését, azt az eredetileg az adott művelethez rendelt komponensnek a többszörözés után előállt összes példányán el kell végezni, mindegyik részeredményt a komponensek közti megtöbbszörözött kommunikációs vonalak mindegyikén továbbítani kell, majd az esetlegesen (a hibák miatt) eltérő eredmények között többségi alapon kell dönteni. Vagyis a rendszer kimenő jelei a komponensek kimenetein lebonyolított szavazások eredményeinek aggregálásával állnak elő.

Ez a struktúra az emberi agy működésének egyszerűsített modellje, amire Neumann több esetben konkrétan utal, például a komponenseket időnként neuron néven említi. Az emberi agyban nagyságrendileg 10^{11} neuron van, mindegyikük több ezer másik neuronnal áll közvetlen összeköttetésben. Egy ilyen bonyolult struktúra elektronikus megvalósítása

[2] EDVAC: Electronic Discrete Variable Automatic Computer (Elektronikus diszkrét változós automata számítógép)

Neumann korában a távoli jövő problémájának tűnt. Még ma sincs közvetlen napirenden, de belátható időn belül elképzelhető.

Neumann eredeti eredményei inkább elméleti jelentőségűek. Egyrészt a komponenseknek 1/6-nál kisebb hibaaránnyal kell működniük. Másrészt a komponensekénél lényegesen kisebb áramköri hibaarány eléréséhez igen nagy redundancia szükséges, az illusztratív példákban a redundancia több tízezerszeres. Meg kell jegyeznünk, hogy a mikroelektronika mai fejlettségi szintjén ilyen mértékű redundancia már nem tűnik technikailag megvalósíthatatlannak, de az idézett publikációk születésekor, az 50-es évek első felében mindenképpen az volt. Neumann maga is hangsúlyozza, hogy az általa javasolt eljárás a gyakorlatban nem használható, bár hozzáteszi, hogy a mikroelektronika valamilyen jövőbeni technológiájával ez a megítélés is változhat.

Neumann modelljének azonban komoly inspiratív hatása volt, konstrukciós ötleteit számos szerző átvette és továbbfejlesztette [7].

A Moore-Shannon modell

Moore és Shannon [8] felismerték, hogy Neumann a redundancia alkalmazásával helyes irányban indult el, és ennek hatékonyabb módját keresték. Az általuk vizsgált rendszer jóval egyszerűbb, mint Neumanné: a logikai áramkör komponensei kizárólag relék, a kommunikációs vonalakat pedig megbízhatónak feltételezik. Ők sem a közvetlen megvalósíthatóságra törekednek, hanem bizonyos konstrukciós lehetőségek bemutatására.

Moore és Shannon cikke rámutat, hogy az ő konstrukciójukban a Neumann-modellével azonos mértékű megbízhatóság-növekedéshez elég 100-szoros redundancia, és nincs szükség a komponensek minimális elvárt megbízhatósági szintjére.

Moore és Shannon célkitűzése az, hogy bemutassa: egy $0 < u < 1$ megbízhatóságú kapcsolókból álló, egyetlen bemenettel és egyetlen kimenettel rendelkező, egy logikai struktúrát leképező kapcsolórendszer megbízhatóságát (az adott esetben zárt, vagyis áteresztő, illetve nyitott, vagyis nem áteresztő állapotának világos elkülönítését jellemző, a [9] cikkben hindrancia-függvénynek [3] elnevezett) $H(u)$ függvény hogyan függ a komponensek u értékű megbízhatóságától. Ezt pontosabban úgy értelmezi a modell, hogy az egyedi kapcsolók egymástól függetlenül egy közös u paraméterű Bernoulli-eloszlás szerint működnek, vagyis u valószínűséggel zárt, $1–u$ valószínűséggel nyitott állapotban vannak, és keresendő a teljes logikai hálózat zárt illetve nyitott állapotának $H(u)$ illetve $1–H(u)$ valószínűsége. A cikk bebizonyítja, hogy a tisztán konjunktív (vagyis soros) illetve a tisztán diszjunktív (azaz párhuzamos) kapcsolás esetét leszámítva létezik olyan $0 < u_0 < 1$ egyedi megbízhatósági szint, hogy

$$Q(u) < H(u) < u, \text{ ha } u < u_0 \tag{1}$$

$$Q(u) > H(u) > u, \text{ ha } u > u_0 \tag{2}$$

ahol $Q(u)$ annak valószínűsége, hogy a logikai áramkör kapcsolói u arányban zártak. u_0 elnevezése *quorum*, $Q(u)$ elnevezése *quorumfüggvény*. [4]

Ha az áramkör kapcsolóit egy szavazótestület tagjainak tekintjük, ahol az egyéni „igen” szavazatot a kapcsoló zárt állapota jelenti, akkor $Q(u)$ az egyszerű u arányú igenlő szavazás

[3] Az elnevezés eredete: a *hindrance* szó jelentése angolul gát(lás), akadály(ozás).

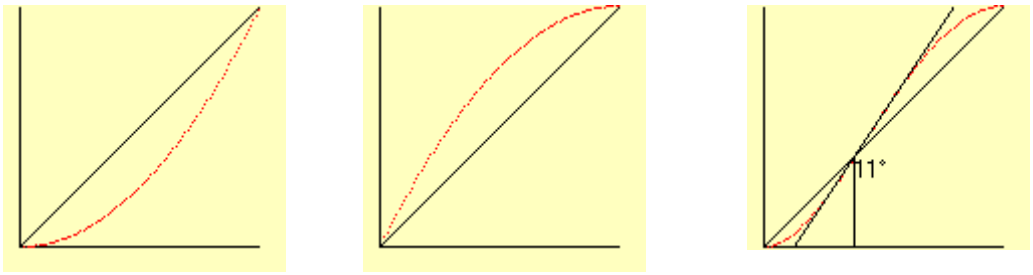
[4] Az angolszász joggyakorlatban a *quorum* szó valamely testületi döntés érvényességéhez minimálisan szükséges szavazási létszámot jelenti.

(vagyis amikor a szavazótestület tagjai u arányban szavaznak igennel) valószínűsége. $Q(u)$ Bernoulli-eloszlású változók átlaga. Bernoulli-eloszlású változók összege binomiális eloszlású változó ugyanazzal az u valószínűségi paraméterrel, az átlag pedig ennek a testületi létszámmal osztott értéke. Nyilvánvalóan $H(u)$ és $Q(u)$ is folytonos függvénye u-nak, ezért

$$Q(u_0) = H(u_0) = u_0 \tag{3}$$

Az (1), (2) és (3) összefüggések azt mutatják, hogy ha azonos számú, azonos megbízhatóságú kapcsolókból álló, de különböző struktúrájú logikai áramkörök hindrancia-függvényei $u = 0$ és $u = 1$ között átmetszik a 45^0-os egyenest, akkor ezek a metszéspontok egybeesnek, ugyanahhoz az $u = u_0$ quorumhoz tartoznak.

A szemléletesség kedvéért az 1. ábrán grafikusan is bemutatjuk a hindrancia-függvényt. A $H(u)$ függvény görbéjének és a 45^0-os egyenesnek u_0 abszcissza-értékű metszéspontja mellett látható a két alakzat által bezárt szög értéke. Ennek jelentőségére később visszatérünk.



1. ábra Konjunktív, diszjunktív és vegyes típusú hindrancia függvény alakja [10]

Az 1. ábra harmadik függvénygörbéjén jól látható, hogy a vegyes típusú hindrancia-függvény alacsony u értékeknél konjunktív, magas u értékeknél diszjunktív jellegű. Ez általános törvényszerűség, amint azt [8] formálisan is igazolja.

[8] továbbá azt is bebizonyítja, hogy az ottani szóhasználat szerint az áramkör „kompozíciója” (vagyis az egyedi kapcsolók helyettesítése az eredeti logikai áramkör teljes kapcsolórendszerével) növeli a megbízhatóságot, ami formálisan azt jelenti, hogy

$$u > H(u) > H(H(u)) > H(H(H(u))) \text{ s.i.t., ha } u < u_0 \tag{4 [8]}$$

$$u < H(u) < H(H(u)) < H(H(H(u))) \text{ s.i.t., ha } u > u_0 \tag{5 [8]}$$

Tehát a kompozíció n-szer iterált alkalmazása n növelésével u_0 előtt csökkenti, u_0 után növeli az iterált kompozíció hindrancia-értékét. Ezáltal szűkíti az áramkör zárt és nyitott állapota közötti bizonytalan zónát u_0 közvetlen környezetében, pontosabban erősíti a kontrasztot a kétféle állapot között.

A kompozíciónak ez az előnyös tulajdonsága azonban a gyakorlatban kevéssé aknázható ki, mert az áramköri elemek (az adott esetben relék) száma n exponenciális függvényeként nő.

A Sah-Stiglitz modell

Joseph Stiglitz Nobel-díjas közgazdász szerzőtársával elsőként veti fel azt a hasonlóságot, amely a Moore-Shannon megbízhatósági modell és a testületi szavazások között van [11]. A Sah-Stiglitz modellben a szavazótestület projektek elfogadhatóságáról dönt. Egy ilyen testület struktúrája hagyományosan vagy poliarchikus (párhuzamos), vagy hierarchikus. Mint a cikk rámutat, egyik sem működik megfelelően. A poliarchia könnyen válhat döntésképtelenné, a hierarchiában pedig gyakran történik befolyásolás, hiszen a testületbeli alárendeltség általában

az intézménynél elfoglalt pozíciót képezi le, ami kizárja a szavazatok függetlenségét. Ugyanakkor a kétféle struktúra vegyítése a testületen belül, vagyis hierarchiák poliarchiája vagy poliarchiák hierarchiája már mentes ezektől a problémáktól.

A Ioannides-modell

A [12] cikkben ismertetett eljárás a testület szavazási hierarchiájára alkalmazza a Moore-Shannon modellt. Itt a kompozíció a testületi struktúra többszintű replikációját jelenti, ami a cikk megállapítása szerint a gyakorlatban pénzügyi és szervezési okokból egyaránt képtelenség. A Moore-Shannon modell használata így a konkrét problémához jobban alkalmazkodó, ugyanakkor egyszerűbb szavazási hierarchia kialakításában nyújthat segítséget. Erre példaként a keresztkompozíciót javasolja, ami az eredeti testületi struktúrával történő szisztematikus struktúrabővítésnek a Sah-Stiglitz modellben vázolt, a hierarchia és a poliarchia együttes alkalmazásával végrehajtott módját jelenti. Ez bizonyítottan növeli a helyes döntés esélyét, de nem jár együtt a rendszer önmagával való kompozíciójának esetében fellépő exponenciális mértékű struktúrabővüléssel.

A KONSZENZUSHATÁR MEGÁLLAPÍTÁSA

Egy bizonytalan tényezőktől függően aktiválódó kockázati esemény bekövetkezési esélyét minősíteni kell [13], ami rendszerint testületi szavazás útján történik [9]. Amikor egy szavazási eljárásra alkalmazzuk a Moore-Shannon modellt, az u_0 értéket, mint döntési küszöböt használhatjuk. Kétféle módon járhatunk el.

Az egyik irány, amelyet [12] ismertet, a testület szavazási hierarchiájára alkalmazza a modellt. Itt a kompozíció a testületi struktúra többszintű replikációját jelenti, ami a cikk megállapítása szerint a gyakorlatban pénzügyi és szervezési okokból egyaránt képtelenség. A Moore-Shannon modell használata így a konkrét problémához jobban alkalmazkodó, ugyanakkor egyszerűbb szavazási hierarchia kialakításában nyújthat segítséget.

A másik irányt [9] és [10] tárgyalják, amelyek az eldöntendő probléma logikájára, vagyis a vizsgált kockázati rendszer hibafájára alkalmazzák az áramköri modellt. A publikációk utalnak arra, hogy u_0 a hibafa egyik alapvető strukturális jellemzője, és ilyenformán az elfogadási küszöbérték alapja lehet. Ennek azonban csak az elvi lehetőségét vetik fel, de nem bizonyítják. A következőkben ezzel a problémával foglalkozunk.

Minden közigazgatási eljárási szituációra jellemző, hogy van egy pont, amikor az ügyintéző saját szubjektív véleményére van utalva. Ez azt jelenti, hogy bizonyos esetekben az ügyintézőnek saját hatáskörében álló eszközeit és képességeit óhatatlanul lényegileg egyenlő intenzitással, egyenlő gyakorisággal és egymástól függetlenül kell használnia. Ez a logikai konfliktuselmélet terminológiája szerint *kolluktációs* helyzetet [5] teremt (l. [10], 2.3.1. pont.)

Most a hibafa prímeseményei játsszák az áramkör egyedi kapcsolóinak szerepét, így tehát a prímeseményekről feltételezzük, hogy független, azonos u paraméterű Bernoulli-eloszlások szerint vannak aktív állapotban. Kérdés, hogy a döntéshozó testület mikor tekintse a nemkívánatos főesemény aktuális vagy várható állapotát aktívnak esetleg akkor is, ha a főesemény állapotát aktívnak tekintő döntéshozók számszerű kisebbségben vannak.

A főesemény állapotát két alapvető, önmagában is összetett tényező határozza meg: egyrészt a prímesemények egyedi állapotainak összessége, másrészt a hibafa logikai

[5] A *kolluktáció* szó vitát, széthúzást jelent. Használatát az indokolja, hogy az egymástól függetlenül realizálódó kockázati tényezők konkrét állapotai kívülről áttekinthetetlen, kaotikusnak tűnő módon határozzák meg a teljes rendszer állapotát.

struktúrája. A szavazás során a döntéshozók a rendelkezésükre álló információ alapján döntenek. [9] rámutat arra, hogy a hibafa általában igen bonyolult logikai kapcsolatrendszert jelent, amely csak a szakértők számára érthető és áttekinthető, az egyes döntéshozók számára azonban nem. Ezért természetes, hogy a döntéshozók a főesemény aktiválódásának esélyét közvetlenül a prímeseményekről, vagyis a lehető legegyszerűbb, tovább már nem bontható rizikófaktorok aktiválódási aránya alapján ítéljék meg. (Kézenfekvő, hogy ha a rizikófaktorok nagy része aktív, akkor „nagy a veszély", ha pedig csak kis része aktív, akkor „kicsi a veszély".) A döntéshozók számára így elég lenne u értékének ismerete.

Legyen M a prímesemények száma, N a döntéshozók száma. Legyen u_i az i. döntéshozó szerinti prímesemény-aktiválódási arány. u_i értéke a 0, 1/M, 2/M, 3/M, …(M-1)/M, 1 számok valamelyike lehet, vagyis a döntéshozók M+1 alternatíva közül választhatnak. Reális esetben $M > 2$, így előáll a legalább 3 alternatíva közüli választás esete. Látható, hogy itt kétféle probléma is előállhat. Egyrészt a korábban tárgyalt szavazási paradoxonok valamelyike, másrészt a többségi vélemény téves volta. Megmutatjuk, hogy a Moore-Shannon modellen alapuló testületi szavazás mindkét problémát képes adekvát módon kezelni.

Feltételezhető, hogy a döntéshozók rendelkeznek megfelelő kompetenciával, ami az adott esetben úgy nyilvánul meg, hogy u értékét a döntéshozó testület a tagok által vélelmezett prímesemény-aktiválódási arányok átlagaként képes egy „elég jó" $\hat{u}$ becsléssel közelíteni, vagyis

$$\frac{u_1 + u_2 + ... + u_N}{N} = \hat{u} \approx u \tag{6}$$

Most következik az eljárás legkritikusabb lépése, vagyis $\hat{u}$ minősítése abban a tekintetben, hogy a döntéshozó testület a főesemény aktiválódását tekinti-e reális forgatókönyvnek. A minősítés alapja a $H(u) / \hat{u}$ hányados, ami a hindrancia-függvény definíciója és (6) alapján azt fejezi ki, hogy egy, a testület által vélelmezett főesemény-aktiválódásra mennyi valóságos főesemény-aktiválódás esik. Itt u tényleges értékét nem ismerjük, ezért $H(u) / \hat{u}$ értékét sem, de a $H(u)$ függvény folytonossága miatt

$$H(\hat{u}) \approx H(u) \tag{7}$$

következésképpen

$$\frac{H(u)}{\hat{u}} \approx \frac{H(\hat{u})}{\hat{u}} \tag{8}$$

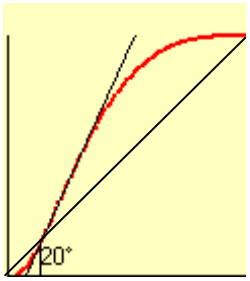
Ha a $H(\hat{u}) / \hat{u}$ arány 1-nél nagyobb, akkor a döntéshozó testületben azoknak a véleménye megalapozottabb, akik a főesemény aktiválódására szavaztak. Hasonló módon, ha az előbbi arány 1-nél kisebb, akkor viszont azoknak a véleménye megalapozottabb, akik a főesemény passzivitására szavaztak. A $H(u)$ függvény korábban ismertetett tulajdonságai miatt a $H(\hat{u}) / \hat{u}$ arány akkor nagyobb 1-nél, ha $\hat{u} > u_0$, és akkor kisebb 1-nél, ha $\hat{u} < u_0$. Tehát a szavazási eredmény minősítésében u_0 valóban adekvát küszöbértékként használható. (u_0 értéke a hibafa ismeretében meghatározható [14]).

Ezen a ponton nyer értelmet a függvényábrákon látható, korábban már említett metszésszög-érték a 45^0-os egyenes és a hindrancia-függvénygörbe között. Ha a szögérték lényegesen nagyobb 0-nál, akkor u_0-tól kezdve egy darabig a főesemény tényleges aktiválódási aránya sokkal gyorsabban növekszik, mint az aktiválódást vélelmező szavazatok u aránya. Ez ismét u_0 mint döntési küszöbérték választása mellett szól.

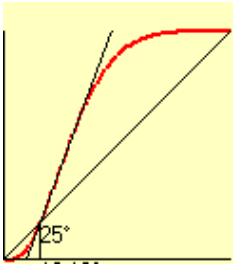
Az $u_0 < 0{,}5$ esetben az u_0 és 0,5 közé eső $\hat{u}$ szavazási értékeknél kisebbségben vannak az „igen” szavazatok, mégis testületi döntésként az „igen”-t kell elfogadni, mert szakmailag ez a helyes.

CIVIL ÉS VÉDELMI KOCKÁZATKEZELÉSI SZEMLÉLET

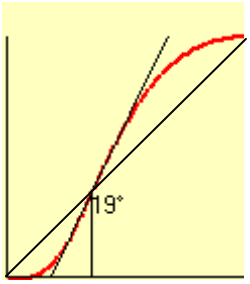
A [14] publikációban három jellegzetes példát mutattunk be védelmi igazgatási problémákra, a hibafákat „szaknyilatkozat” formátumban prezentáltuk. Ezeknek a fent tárgyalt elemzése a „Talajszennyezés” esetben kb. 1/8, az „ISO sikertelen bevezetése” problémánál kb. 1/6, a „Sikeres merénylet” problémánál kb. 1/3 konszenzushatárt mutat ki. Vagyis jól látszik az a tendencia, hogy a védelmi hibafák konszenzushatára jóval 50 % alatt van.



2. ábra „Talajszennyezés” esemény hindrancia-függvénye és konszenzushatára (a szerző szerkesztése [14] alapján)



3. ábra „ISO 9001:2000 sikertelelen bevezetése” esemény hindrancia-függvénye és konszenzushatára (a szerző szerkesztése [14] alapján)



4. ábra „Sikeres merénylet” esemény hindrancia-függvénye és konszenzushatára (a szerző szerkesztése [14] alapján)

Itt mutatkozik meg a civil és védelmi szféra eltérő kockázatkezelési szemlélete. Mindkét szféra a költségtakarékosság és a biztonság közötti ésszerű kompromisszum kialakítására törekszik a kockázatkezelésben.

A civil szféra szemléletében a főesemény aktiválódása a rizikófaktorok „szerencsétlen egybeesésének” a következménye, vagyis a megközelítés alapvetően konjunktív jellegű, a megelőzéshez elég a rizikófaktorok együttes aktiválódását kizárni.

Ezzel szemben a védelmi szféra szemléletében a főesemény aktiválódásában döntő szerepe van a rizikófaktorok egyenkénti aktiválódásának, vagyis a megközelítés alapvetően diszjunktív jellegű, a megelőzéshez a rizikófaktorok aktiválódását külön-külön kell kizárni.

Az a szituáció, hogy a rizikófaktorok mindegyike aktív, sokkal ritkábban következik be, mint az, hogy legalább egyikük aktív. Ennek megfelelően a civil szemlélet költségtakarékosabb, hiszen sokkal kevesebb kockázati szituációt kíván kizárni.

Ugyanakkor éppen emiatt a civil szféra esetében alacsonyabb a biztonsági szint, ami viszont ellentmond a védelmi szféra szemléletének, amelyben a biztonság fontosabb a költségtakarékosságnál, így a védelmi szféra a rizikófaktorokat egyenként kívánja kizárni, ami természetesen sokkal „drágább”.

A szemléleti különbséget a hindrancia-függvény is mutatja: az idézett védelmi jellegű példákban 0,5-nél sokkal alacsonyabb u_0 értéknél kezdődik a felső diszjunktív jellegű szakasz, ahol tehát a szavazótestület a kockázati esemény aktiválódását vélelmezi.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A jelen dolgozatban a testületi szavazás adekvát konszenzushatárának meghatározásával foglalkoztunk.

Igazoltuk, hogy a konszenzushatár értékét, a quorumot a szavazás tárgyát képező nemkívánatos kockázati esemény logikai struktúráján alapuló hindrancia-függvény segítségével találhatjuk meg.

A quorum értéke lehet 0,5-nél kisebb is, ami azt jelenti, hogy a kockázat megítélésében ilyenkor a kisebbségnek van igaza a többséggel szemben.

Beláttuk, hogy bár a döntési alternatívák száma általában legalább 3, nem áll elő az ilyen típusú szavazási eljárásoknál lehetséges holtversenyes döntésképtelenség.

Rámutattunk arra, hogy a kockázati események hibafája a civil megközelítés szerint konjunktív, míg a védelmi megközelítés szerint diszjunktív jellegű. Ennek alapján magyarázatot adtunk arra, miért gyakori a védelmi szféra testületi döntéseiben az olyan döntési probléma, amelynek alacsony a konszenzushatára.

További kutatás tárgya, hogy az itt tárgyalt döntési modell mennyire van összhangban a statisztikai döntéselmélet modelljeivel. Indokolt megvizsgálni a kockázatelemzésben általánosan használt Bayes-típusú gondolkodásmódot követve is a konszentzushatár interpretálását.

FELHASZNÁLT IRODALOM

[1] LLULL, R: Ars eleccionis. 1299. (Elveszett, de 2001-ben megtalált kézirat.)

[2] BORDA, J.-C. de: Mémoire sur les élections au scrutin. Histoire de l'Académie Royale des Sciences, Paris, 1781. http://asklepios.chez.com/XIX/borda.htm (letöltve: 2017.01.12.)

[3] CONDORCET, M.: Essai sur l’Application de l’Analyse à la Probabilité des Décisions Rendues à la Pluralité des Voix. Paris, 1785. http://gallica.bnf.fr/ark:/12148/bpt6k417181 2016.12.31 (letöltve: 2016.12.27.)

[4] CSEKŐ, I.: Szavazáselmélet és mechanizmustervezés. Magyar Tudomány, 170/2009 No. 5. 538-546 o.

[5] NEUMANN, J. von: First Draft of a Report on the EDVAC. University of Pennsylvania, Philadelphia, 1945. http://www.virtualtravelog.net/wp/wp-content/media/2003-08-TheFirstDraft.pdf (letöltve: 2017.03.21.)

[6] NEUMANN, J. von: Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components. California Institute of Technology, Pasadena, 1952. http://fab.cba.mit.edu/classes/862.16/notes/computation/vonNeumann-1956.pdf (letöltve: 2013.03.17.)

[7] PIPPENGER, N.: Developments int he „Synthesis of Reliable Organisms from Unreliable Components". Proc. of Symposia in Pure Mathematics 50/1990 pp. 311-323. http://www.dna.caltech.edu/courses/cs191/paperscs191/Pippenger.pdf (letöltve: 2017.03.20.)

[8] MOORE, E., SHANNON, C. E.: Reliable Circuits Using Less Reliable Relays. Journal of the Franklin Institute, 262/1956. pp. 191-208. http://www.cctbio.com/wiki/images/3/30/Moore_Shannon_Reliable_Circuits_Using_Less_Reliable_Relays.pdf (letöltve: 2017.01.15.)

[9] BUKOVICS I.: A „jó állam" algoritmikus elmélete. Polgári Szemle, XI. 1-3. (2015). http://www.polgariszemle.hu/?view=v_article&ID=661 (letöltve: 2016.12.17.)

[10] BUKOVICS I.: A természeti és civilizációs katasztrófák paradigmatikus elmélete. MTA doktori értekezés, Budapest, 2007.

[11] SAH, R. K., STIGLITZ, J.: Committees, Hierarchies and Polyarchies," The Economic Journal, 98/1988, pp. 451-470.

[12] IOANNIDES, Y.: Complexity and Organizational Architecture. Discussion Paper 13/2003. Department of Economics, Tufts University, Medford, Massachusetts, 2003. http://www.aueb.gr/crete2004/docs/Ioannides.pdf (letöltve: 2015.02.14.)

[13] BUKOVICS I.: Gondolatok a közigazgatás tudományos megalapozásáról. Pro Publico Bono, 2/2013. 4-27. o. http://uni-nke.hu/uploads/media_items/bukovics-istvan-gondolatok-a-kozigazgatas-tudomanyos-megalapozasarol.original.pdf (letöltve: 2016.12.16.)

[14] BUKOVICS I., FÁY GY., KUN I.: A jó állam és a védelmi szféra. Hadmérnök X. 2. (2015) 208-222. o. http://hadmernok.hu/152_19_bukovicsi_fgy_ki.pdf (letöltve: 2016.12.15.)