HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

XI. Évfolyam 4. szám 2016. december

NKE
BUDAPEST

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

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

Jelen számban megjelent írások szerzői:

Balog Károly – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Csősz László – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Prof. Dr. Halász László – Nemzeti Közszolgálati Egyetem, HHK professzor emeritus
Holicza Péter – Óbudai Egyetem BDI doktorandusz
Horváth Kristóf – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. habil.Kátai-Urbán Lajos Nemzeti Közszolgálati Egyetem, KVI egyetemi docens
Dr. Kovács Zoltán – Nemzetbiztonsági Szakszolgálat
Mógor Tamás – Nemzeti Közszolgálati Egyetem, HDI doktorandusz
Őszi Arnold – Óbudai Egyetem BDI doktorandusz
Pető Richárd – Óbudai Egyetem BDI doktorandusz
Phuoc Dai, Nguyen Huu – Óbudai Egyetem BDI doktorandusz
Ruiz S, Lourdes – Óbudai Egyetem BDI doktorandusz
Sebestyén Zsolt – Országos Atomenergia Hivatal
Somosi Vilmos – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Szabó András – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Szádeczky Tamás – Nemzeti Közszolgálati Egyetem, ÁKK adjunktus
Szendi József – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Szűcs Endre – Óbudai Egyetem, BGK adjunktus
Dr. Tóth András – Nemzeti Közszolgálati Egyetem, HHK adjunktus
Tóth Attila – Óbudai Egyetem BDI doktorandusz
Végvári Zsolt – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Arnold ŐSZI – Lourdes RUIZ S
oszi.arnold@bgk.uni-obuda lourdes.ruiz@ bgk.uni-obuda.hu

BIOMETRIC USES IN OCCUPATIONAL SAFETY AND HEALTH

Abstract

Biometrics is used to recognize the identity of a specific individual using unique physical or behavioral traits such as: fingerprints, facial recognition, iris, gait, DNA, etc. Occupational safety and health (OSH) is a multidisciplinary field that focuses on recognizing, analyzing, preventing and minimizing risks in the workplace in order to provide health and safety to the employees. Biometrics and OSH are different study fields but share a common goal that is to provide enhanced safety. The following document identifies and describes conventional and potential uses of biometrics in the workplace, devices and technology relevant to OSH procedures and practices.

A biometrikus azonosítást egyének felismerésére alkalmazzák, felhasználva az egyéni fizikai és viselkedési jellemzőket, mint például az ujjnyomat, az arc felépítése, az írisz, a járás, a DNS, stb. A munkahelyi biztonság és egészségvédelem (OSH) egy multidiszciplináris terület, amelynek a középpontjában a munkahelyi kockázatok minimalizálására, felismerése, elemzése, megelőzésére áll, annak érdekében, hogy biztosítsa a biztonságot és az egészség megőrzését az alkalmazottak. A biometria és a munkavédelem egymástól különböző tanulmányi területek, de közös bennük, hogy a céljuk a nagyobb biztonság megteremtése. Az alábbi dokumentum beazonosítja és leírja a biometrikus eszközök hagyományos és a további lehetséges felhasználási területeit a munkahelyen, az eszközöket és a technológiákat, amelyek relevánsak a munkavédelmi szempontból kritikus eljárásokhoz és gyakorlatokhoz.

Keywords: *biometrics, occupational, safety, technology, health, uses, devices ~ biometria, munkavédelem, biztonság, technológia, egészség, felhasználás, eszközök*

INTRODUCTION

Biometrics is the science used to measure and analyze specific physical or behavioral traits in humans, in order to recognize the identity of a specific individual. Some of the characteristics used are: fingerprints, face, iris, voice recognition, hand geometry, gait, signature, DNA, odor [1]. Biometric systems are implemented to provide safety in various areas such as forensics, banking, airport control, electronical commerce, government social services and building accessibility. Biometrics technology poses a broad potential in other areas such as occupational safety. Occupational Safety and Health (OSH) is a multidisciplinary field that focuses in the recognition, analysis and prevention of hazards in the workplace. Its main goal is to protect workers by offering a healthy and safe work environment [2]. The purpose of this document is to identify conventional and prospective uses of biometrics in the workplace relevant to OSH practices.

Biometric systems focus on the concept that physical or behavioral characteristics in humans can be distinctive, for this reason it eases the identification of a specific person. These systems offer a high level of security compared with passwords or identification cards because they are based in the identification of a person using their inherited attributes that are unique. Biometric systems are based on pattern recognition which consists of two parts: enrollment and recognition. In the enrollment step, biometric traits are obtained from the individual, only distinctive features of the data collected are stored in the database. In the recognition part, biometric data is collected from the individual and compared with the data stored at the enrollment step in order to recognize and authenticate the person identity [1]. Biometric technologies offer an accurate verification where just an authorized person gets access to the information or place that is secured. Moreover, accountability is an advantage that can successfully identify a particular action or event to a person. It also prevents duplication, sharing of information and fraud, which provides a safer organizational environment.

OSH management systems concentrate in recognizing, addressing and preventing risks inside an industry aiming the welfare, health and safety of the employees. Moreover, the implementation of OSH practices contributes to the reduction and elimination of accidents, incidents, work related injuries and diseases. These systems involve the participation of the whole company and resources, including policies, processes, procedures, workforce and leadership at all levels of the organization [3].

Biometrics and OSH systems emphasizes in providing safety in different fields. Biometrics can be a powerful tool to be implemented in the workplace by providing access and correctly authenticate personnel identity. Biometric technology is becoming very popular among companies. Devices such as biometric time clocks and biometric physical access control readers had revenues of $225 million and $190 million in 2013 and it is expected to increase to $350 million and $ 300 million respectively in 2018 [4]. For this reason, it is important to distinguish the different occupational hazards and risks in an industry and therefore utilize biometric devices to protect workers and minimize accidents.

HAZARDS AND RISKS IN THE WORKPLACE

Hazards are present in every work environment. An occupational hazard is anything that has the potential to hurt or harm a worker. A risk is the likelihood or chance that the hazard will harm an employee [5]. Hazards are classified into two groups: safety hazards, cause accidents that can injure a worker and; health hazards, cause an occupational disease or illness, these hazards can be biological, physical, chemical, ergonomic, and organizational.

Safety hazards include conditions such as spill in the floors, blocked aisle, improper handling of cords in the floors, work from heights using ladders or in roofs, unguarded machinery, moving parts, electrical and confined spaces

Health hazards are subdivided into:

- Biological hazards involve the exposure to infected animals, people or plants by blood, bacteria, viruses and insect bites.
- Physical hazards include radiation, high exposure to ultraviolet rays, work at extreme temperatures, loud noise.
- Ergonomic hazards are the result of a type of work, body position or conditions that can affect the body. They can cause chronic diseases if there is a long term exposure. Some examples are inadequate workstations, frequent lifting, bad posture, repetitive movements, and vibration.
- Chemical hazards are present in cleaning products, paints, solvents, vapors, gases, flammable materials and pesticides.
- Organizational hazards comprise high workload, violence, lack of respect, flexibility, social support and sexual harassment [6].

HAZARD CONTROL

Controlling, managing and removing hazards imply a better work protection. Exposure is a main factor that needs to be considered in order to reduce hazards. Hazard controlling methods are:

- Engineering approach consists of redesigning and modifying workspaces, processes and equipment towards the reduction of workers' exposure. This method is preferred because it works independently of the workers. Engineering controls includes: substitution, when a less dangerous material is used or a process is changed; isolation restricts the exposure of the people working directly with the hazard by the inclusion of a containment structure; and ventilation implies a local exhaust system that eliminates the contaminant in the air thus it is not dispersed in the workplace.
- Working procedures and hygiene during job activities.
- Administrative approaches such as job rotation, break cycles, maintenance procedures.
- Effective usage of personal protective equipment at work such as hard hats, hear protectors and protective clothing [5].

Biometric science is mainly used as an engineering approach. The implementation of biometric devices contributes to controlling and minimizing hazards in the workplace. It is also a powerful tool for providing enhanced security to employees and to the work environment. Biometric management systems offer a variety of safety solutions to companies; additionally they can be used in different processes along the supply chain.

BIOMETRIC USES

Biometric Systems have been specially used in three different aspects:

1. For commercial uses such authentication in online banking services or ATM, credit card usage, e-commerce, mobile phone, distance learning, access to health care systems, etc.
2. For government purposes such as issuing ID cards, driver's licenses, social benefits, homeland security.

3. For forensic uses such as body identification, criminal purposes, parenting determination and lost persons [1].

CONVENTIONAL USES OF BIOMETRICS IN THE WORKPLACE

Biometric Systems provide safety to companies and employees building a safe and healthy work environment. In addition, they serve for numerous purposes listed below:

- Background Check, employers use biometric technology at the beginning of the recruiting process. In United States (US), companies perform employment screenings to candidates looking for a job position. FBI retrieves the criminal story of the applicants which helps the recruiter regarding a hiring decision. FBI uses two biometric fingerprint and two name-based background check [7]. It is important to know about the criminal records of candidates and employees because depending on the criminal offense, it can be a threat to the organization and to the other employees. Therefore, employee screenings can enhance the security in a company.
- Monitoring Staff, fingerprint recognition devices are mainly used for recording employees' time. These devices have built-in software that calculates accurately the working hours, punctuality, breaks, sickness, absence, over time and payroll. Other devices can deny access to company technology and networks after finishing the workday. Workers can clock in and out just by using their fingerprints in a faster way than traditional methods such as passwords or magnetic cards. Fraud and buddy punching is effectively reduced using this technology which enhances workers efficiency and productivity [8].
- Access Control, biometric data based devices are used for recognizing and grant access to authorized personnel by the authentication of their identity using biometric traits such as fingerprints, face recognition and eye scanning. They provide an additional security against trespassers by protecting buildings, computers and networks. In addition, biometric recognition restricts access to specific areas in the workplace such as facilities that contain dangerous, valuable materials or sensitive information. Keyless locks that utilize biometric traits track access and workers' activities and also prevent the access of intruders which offer a safety organizational climate [9].
- Biometric devices usage is effective on tracking company's property such as vehicles. They can provide valuable information such as: real time data on speed, location and different variables such as time for delivering companies. These devices can offer a trustworthy traceability report along the working schedule that can be useful in case of accidents and for claiming responsibility [4]. Moreover, biometric technology can track the employee in the workplace at any time which controls misconduct and behavior. It also promotes safe conducts among workers and enhances the usage of safety procedures while performing the work tasks.

POTENTIAL USES OF BIOMETRICS IN THE WORKPLACE

Introduction of biometric technology in the workplace have different uses listed above but also contributes to the development of various potential uses intended for the protection of workers. Some of them are explained here:

- As part of a health management program, biometric measures such as: height, weight, body mass index, waist and hip circumference, body fat blood pressure and

pulse rate are collected from employees. Biometric screenings are useful to identify health risks, modification of behavior, for implementing educational programs and changes in the work environment and culture. The measures are part of a work health assessment in which the company evaluates the worker health through the time in order to prevent work related diseases, reduce health costs and improve workers' health and productivity. The extraction of the biometric data creates an employee health baseline to prevent and perform health interventions, refer to health specialists, generate specific health programs, create awareness and direct actions to improve workers' health [10]. Employee wellness program is taking into consideration by employers because of the variety of health benefits to the workers that are translated in reduction of costs and creation of a healthy and safe environment inside and outside the workplace.

- Devices used in the workplace such as laptops, USBs and mobile phones have fingerprint detector systems. These systems authenticate users and provide traceability during the whole usage of the equipment. Windows Hello is a Microsoft's biometric authentication feature that allows employees to have access to company's devices and networks by using fingerprint and facial recognition. It can be used by multiple users that work with the same device. This method is backed with a PIN which is safer against credential theft [11]. The potential use of this feature is that can be implemented in any type of machinery. In automated machinery, it is important to have a record of the employees using the equipment in different cases such as work hours, maintenance, calibration and repair. In operations such as a lock out for maintenance, just the authorized personnel can turn on the machinery offering a protection to other workers around. The machine can have multiple users that allow special features to each one ensuring the safety of the procedures and the product.

BIOMETRIC TECHNOLOGY AT THE WORKPLACE

Biometric equipment is used mainly for fingerprint and facial recognition at the workplace. Different companies are developing devices and software for providing enhanced security in the workplace. The technology described below is just some examples of the variety of biometric options offered to industries in order to fulfill their employees' biometric authentication necessities.

- uAttend is a company that designs employee management systems and manufacturers affordable biometric devices and a cloud-based software that tracks worker's time and attendance. The software works with different applications such as clock, smartphone apps and web monitoring systems in one interface. It comprises different features such as tracking and reporting of overtime, holidays, different departments inside the company, vacations, sick leave, breaks and payrolls. The company specializes in manufacturing time clocks with fingerprint and facial recognition. Table 1 shows fingerprint time clock BN500 and facial recognition time clock MN1000. These devices provide time keeping solutions to small and medium enterprises [12].
- Kronos Incorporated is a company that provides workforce management concerning workers' time and attendance. It offers biometric identification and recognition when the employee clocks in and out or work. Moreover, it has several software features that allow employers to track time, efficiency, productivity and compliance among the workforce. Table 1 shows Kronos InTouch time clock which provides biometric

identification to validate employees' identity. Kronos Inc provides tailored monitoring solutions to small, medium and large enterprises [13].

- Privaris Incorporated designs and provides biometric authentication mobile devices which grant access to buildings, offices, computers, networks, websites, before connecting with an existing security system which provides an additional protection against intruders. Plus ID is one of its main products; it consists of a personal fingerprint device and a secure processor, the device recognizes the user and releases an access code or credential. It can store different information such as entry codes, passwords, credit cards, licenses, photographic images and additional biometric data. It is compatible with Bluetooth and radio-frequency identification (RFID) systems. Table 1 shows Privaris Plus ID key fob. This device is a powerful tool in the workplace because it provides an all in one solution to security by granting access to the physical facilities in a company but also access to computers and networks. It enhances safety since it works by the recognition of the biometric trait of the authorized user [14].

The Obuda University (OU) biometrics laboratory possesses different biometric recognition devices that can be used in the workplace. The devices are:

- ievo is a company that designs and manufactures biometric fingerprint products. The OU laboratory has ievo ultimate which is a fingerprint reader that provides reliable user identification. It can be used to grant access to buildings and high security areas. It also works in harsh conditions, for this reason it can be used in outdoor and indoor environment. It has a multi spectral imaging sensor that can obtain fingerprints in different conditions such as water, dust, oil, and latex gloves [15]. Table 1 shows ievo ultimate fingerprint reader device.
- Suprema is a company that manufactures different biometric devices used in the work place for access control and time & attendance fingerprint recognition. Suprema's BioEntry Plus, is an IP based fingerprint access control system. It can be used for indoor operations. Suprema's Face Station device provides safety by offering a contactless authentication. This device can be used in facilities where hygiene needs to be enhanced such as hospitals. It has an infrared camera for face recognition and a time and attendance function for worker's time keeping in the workplace [16]. Table 1 shows BioEntry plus fingerprint reader and Face Station facial recognition device.
- UBKEY innovation Inc, is a company that designs iris recognition systems. OU laboratory has mirror key iris recognition devices. These devices capture the image of the person's iris in order to authenticate the identity of an individual and grant access to different locations [17]. Table 1 shows an image of mirror key device.

Biometric technology is a powerful tool in the workplace; however privacy concerns are rising among the implementation of these systems in companies. The acquisition of a biometric trait such as fingerprints or iris that is unique for an individual, poses safety concerns between the workers. It is considered an invasion of their personal privacy; additionally there is a fear that the biometric information collected can be stolen or misused. In order to address these concerns, biometric recognition devices such as suprema's bioentry plus does not save fingerprints images, it stores a fingerprint template that consists of numeric data that cannot be reconstructed into a fingerprint image. This fact protects worker's rights and privacy against the possibility of stolen personal data and the usage of it for other purposes. Moreover, in many U.S. states the employer is liable to maintain the security of the biometric systems and biometric information collected from their employees. It is vital for a

successful implementation of biometric systems in an organization to inform, train the employees about the acquisition processes, the operation of the biometric devices and maintain a balance between monitoring and security.

Table 1: Biometric Equipment

Company	Equipment Name	Equipment Image	Source
uAttend	Fingerprint time clock BN500		[12]
	Facial recognition time clock MN 1000		[12]
Kronos	Kronos InTouch time clock		[13]
Privaris	Plus ID key fob		[18]
Ievo	ievo Ultimate		[15]
Suprema	BioEntry Plus		[16]
	Face Station: Model FSM		Image taken at OU Biometrics Laboratory
UBKEY	Mirror key Iris Recognition System		Image taken at OU Biometrics Laboratory

CONCLUSIONS

Biometric Science and OSH principles have a common goal which is provide an enhanced safety in different areas especially at the work place. Biometrics offers a variety of uses in several fields and is becoming more relevant in the work environment. Fingerprint and facial recognition devices are the most popular used in order to address organizations' needs. The usage of unique human traits to securely authenticate an individual's identity is a valuable safety solution for companies. Biometric recognition allows to securely grant access to authorized personnel into sensitive areas or information, control time and attendance and track employees and processes at all times. In addition, it brings safety to the work environment and promotes a safe culture among the workforce. However, privacy issues regarding the acquisition of biometric traits for different purposes is a concern, it is important to address these concerns and demonstrate how biometric technology protects personal data collected in the workplace.

Biometric systems are becoming relevant in organizations and offer a variety of options tailored to the final user. The challenge of OSH personnel at an enterprise is to choose the correct biometric option that accommodates to the company's requirements and necessities to guarantee a safe and health place for workers.

References

[1] A. K. Jain, A. A. Ross and K. Nandakumar, Introduction to Biometrics, ISBN : 978-0-387-777326-1, New York: Springer, 2011.

[2] B. O. Alli, Fundamental Principles of Occupational Health and Safety. ISBN: 978-92-2-120454-1, Geneva: International Labour Office, 2008.

[3] International Labor Organization, "Guidelines on occupational safety and health management systems, ISBN: 92-2-111634-4," ILO, Geneva, 2001.

[4] T. Vranjes, "Society for Human Resource Management," 16 March 2015. [Online]. Available: https://www.shrm.org/legalissues/stateandlocalresources/pages/workplace-biometric-technology-.aspx. [Accessed 22 April 2016].

[5] Ontario Ministry of Labor, "Ontario Ministry of Labor," 02 October 2013. [Online]. Available: http://www.labour.gov.on.ca/english/hs/faqs/hazards.php. [Accessed 22 April 2016].

[6] Occupational Safety and Health Administration, "Occupational Safety and Health Administration," [Online]. Available: https://www.osha.gov/dte/grant_materials/fy10/sh-20839-10/circle_chart.pdf. [Accessed 21 April 2016].

[7] U.S. Department of Homeland Security, "Immigration Benefits Background Check Systems," Department of Homeland Security, 2010.

[8] Attendance Enterprise , "Biometrics: Advantages for Employee Attendance Verification," Info Tronics Inc, Farmington Hills.

[9] M. James, "10 Ways Biometrics Technology Can Make your Workplace Safer," 11 September 2009. [Online]. Available: http://ezinearticles.com/?10-Ways-Biometrics-Technology-Can-Make-Your-Workplace-Safer&id=2908729. [Accessed 22 April 2016].

[10] American College of Occupational and Environental Medicine, "Biometric Health Screening for Employers," *Journal of Occupational and Environmental Medicine,* vol. 55, 2013.

[11] E. Ross, "Microsoft," 4 April 2016. [Online]. Available: https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-hello-in-enterprise. [Accessed 2 May 2016].

[12] uAttend, "uAttend employee management systems," [Online]. Available: https://www.uattend.com/. [Accessed 06 May 2016].

[13] Kronos Inc, "Kronos Incorporated," [Online]. Available: http://www.kronos.com/. [Accessed 06 May 2016].

[14] M. Prosner, "Automated Buildings," July 2006. [Online]. Available: http://www.automatedbuildings.com/news/jul06/articles/privaris/060629102101privaris.htm. [Accessed 6 May 2016].

[15] ievo, "ievo reader," [Online]. Available: http://ievoreader.com/. [Accessed 16 May 2016].

[16] Suprema, "Suprema Incorporated," [Online]. Available: https://www.supremainc.com/en/AccessControl-TimeandAttendance/Biometric-Devices/FaceStation. [Accessed 16 May 2016].

[17] UBKEY, "UBKEY Innovation," [Online]. Available: http://ubkey.com/eng/ps_all.html. [Accessed 16 May 2016].

[18] IDE, "IDE Inc," [Online]. Available: http://www.ideinc.com/work/privaris-plusid/. [Accessed 16 May 2016].

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Nguyen Huu PHUOC DAI
phuoc.daitt@bgk.uni-obuda.hu

FINGERPRINT DEVICE (SUPREMA) IS SAFE OR NOT?

Abstract

Fingerprint is one of the most important biometric techniques to identify personal information of an individual. For example: log in computers, network, a car and so on. This technique is primarily because people can operate and install this system easily. Finger authentication system is divided into four steps such as: using sensor, feature extraction, template matching and decision about authentication. In this article, the author used some measures in order to evaluate the safety of biometrics device, especially in Suprema device.

Az ujjnyomat alapú az egyik legfontosabb biometrikus azonosítási technika az egyén beazonosítására. Alkalmazható például: számítógépekbe történő bejelentkezéshez, hálózatokhoz, autókhoz, és így tovább. Ez a technika több szempontból is előnyös, az emberek könnyen tudják nem csak telepíteni de működtetni is a rendszert. Az ujjnyomat hitelesítési rendszer négy lépésből áll: szenzor alkalmazása, tulajdonság-kinyerés, sablon azonosítás és végül döntés az azonosságról. Ebben a cikkben a szerző bemutatja a biometrikus technológiákat, majd egzakt méréseket alkalmaz annak érdekében, hogy értékelje biometrikus eszközök a biztonságát. A méréseket Suprema eszközzel végzi.

Keywords: *biometrics, biometric device, fingerprint ~ biometria, biometrikus eszköz, ujjnyomat*

INTRODUCTION

In the past few years, biometrics used to identify people by using some figures from human being‘s physiology as fingerprint, hand geometry, iris, face recognition, voice and so on. Moreover, a biometric system is vitally a pattern recognition system that acquires biometric data from an individual, extracts features set from the acquired data and compares them with the template set in the database [1]. It is also used to verify individuals in groups that are under suspect. The biometric system based on the information extracted from the differences of people ‘s trait. Furthermore, biometric recognition is used for enrollment, verification and authentication of biometric template in biometric system [2]. In the enrollment process, the individual’s fingerprint are enrolled into the system by Suprema device. In verification process, the system is verified query human’s trait with enrolled human’s own biometric charecteristics. In authentication process, the system validates individual by comparing the entire enrolled fingerprints with the templates stored in the database. Fingerprint method is considered as the most reliable method because of some reasons such as: low cost of equipment, low time of procedure. In fact, in United states has Integrated Automated Fingerprint Identification system where above 51 million of criminal’s fingerprints are stored and about 1,5 million of civil fingerprints. Regarding that system database, it makes the crime investigation easier and minimizes the time a lot [3]. In short, while fingerprint technology offers a lot of benefits for the users, there are also many problems that should be aware of.

LITERATURE REVIEW

Definition

According to [4], biometrics technology is a term which came from Greek and this word can divide into two roots: “bio” – means life and “metrics” – to measure. It is a new authentication method to identify the user in three ways: something that person knows (password), something the person has (key, special card) and something the person is (fingerprints, footprint).

Moreover, biometrics technology is a method to verify or recognize the identity of an individual based on physiological or behavioral characteristic [5]. Based on the context, biometric has 2 modes: verification mode and identification mode.

Verification mode: the biometric system authenticates a person’s identity by taking his/her own biometric template stored in the database and comparing with the captured biometric data. In this system, an individual is required to use a PIN- personal identification number as username, a smart card, etc. and it manages one-to-one comparison to identify whether the captured user’s template is true or not. This mode is mostly used for positive recognition and it prevents multi-users using the same identity [6].

Identification mode: in contrast to verification mode, this mode indicates the individual by searching all templates of the users in the system database for a match. In another way, this system conducts one-to-many comparison to identify user’s identity and rejects someone if he/she is not enrolled in the database. Especially, this mode doesn’t require the users have a PIN as verification mode and its purpose to prevent a single person from using multiple identities [7].

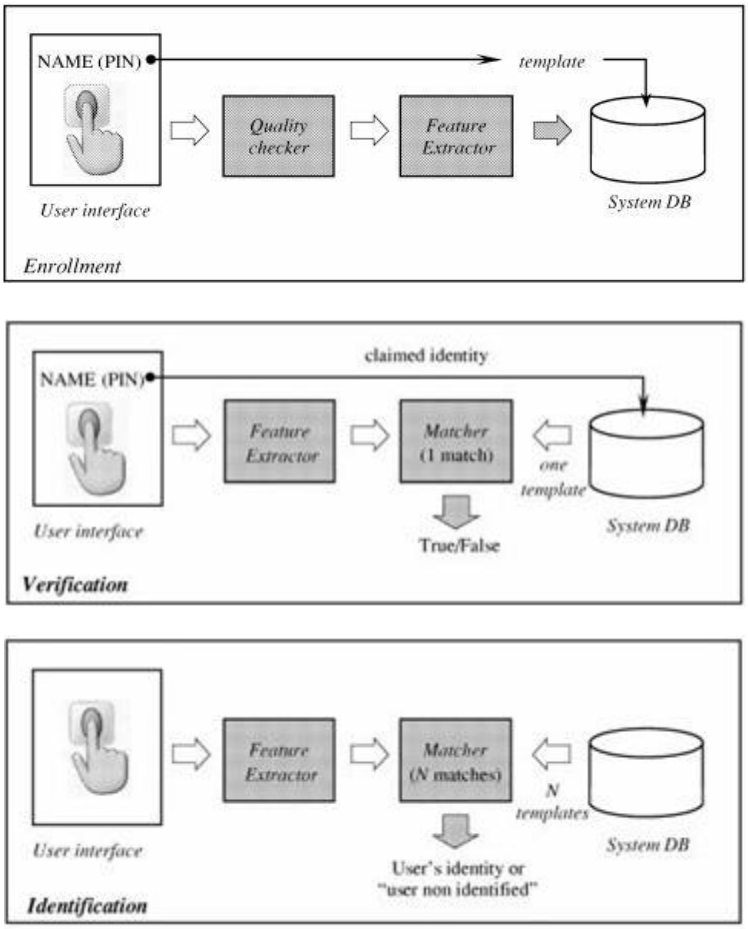


Figure 1: Block diagram of enrollment, verification and identification (source: Anil K. Jain et al.) [8]

Classification

There are two main categories of biometrics authentication system: physiological type and behavior type [3].

Physiological type

Fingerprint: is one of the oldest and popular method in biometrics authentication system. It used the picture of user's finger pattern from any surface that person touches. It can be said that fingerprints are strong evidences in investigating the crimes.

Face recognition: the system uses the 2D or 3D digital image of an individual. This method based on some factors of human being's face such as: distance between eyes, width of the nose, depth of the eye sockets, the shape of the cheekbones and the length of the jaw line.

DNA: similar to biometric based fingerprints, this method widely used in identify the criminals. It consists of four bases: Adenine (A), Guanine (G), Cytosine (C) and Thymine (T) which make DNA code of an individual. However, it only has one exception with the twins because of the same DNA structure.

Palm print: it refers to the palm region image of user's hand. It is similar to fingerprints and iris recognition method but their size is bigger and it has a limitation of using mobile devices. This method has three main factors as wrinkles secondary lines, ridges and especial in principle

lines of user's palm. Each different user's palm contains texture, indents and marks which are used to authenticate one with another.

Hand Geometry: the difference between one person and the other is the geometric shape of their hands, for example: height, length of the fingers, distance between joints, shape of the knuckles and surface area of the hand [9]. This method based on these factors in order to recognize the users but it is seldom used today because with young children, their geometric shape of the hands can change through time.

Iris recognition: the aim of this method is to analyze the iris's outer boundary where it meets white sclera of the eye, pupillary boundary and the center of pupil. This system makes the process fast and secure, but it also has some drawbacks for instance, it is impossible to recognize individual when scanning user's eyes from a distance or user's eye problems (blindness and cataracts).

Behavior type

Typing Rhythm: a technology to recognize the way of individual's typing on a keyboard. The main features of this technology such as latencies between successive keystrokes, duration of each keystroke, finger placement, pressure applied on keys and overall typing speed. When user access to the system, he/she types (login name, password…), and keystroke will capture data and compare with captured template in database.

Gait: this technology depends on the way of people walk, style of walk, pathology, etc. In another way, gait recognition analyze the movement parameters as knee, ankle movements, angles and spatial-temporal elements as the length or width of steps, the speed. Then, this technology figures out the difference in correlation between those parameters from one person to another person.[10]

Voice: Voice recognition is one of the fastest methods to authenticate individual. The voice is gained from different person because the wave of sound which comes from different human throat and mouth. The tone of the sound is established by tongue, gums, teeth, lips, the size of stream and so on. This method takes user's speech and stores them in database. Then in identification process, the captured sample is compared to the template in database, if the result matches, that person can be verified [11],[12].

Benefits

According to [4], biometric system offers some advantages in order to authenticate the users in the system. Firstly, the users can't pass their biometric characteristic to the other easily as they do with their passwords or smartcards. Moreover, it is more convenient than passwords/cards because the users don't need to remember the hard-to-memorize passwords or keep them. Secondly, with the boosting of biometric technology, it creates a new and secure method to make highly accurate verifications of individuals and it cannot be stolen as traditional authentication (password, card, token, and the like). In fact, the attackers may not break the user's fingerprint/iris pattern even using the fake or artificial biometric characteristics because most biometric techniques based on the thing that cannot be stolen or forgotten. Thirdly, this method can reduce management costs. For instance, with the new authentication method, the administrators don't need to reissue or issue password/card/token when the users have problems or losing them. Therefore, it can reduce a lot of time and cost for management. Finally, biometric authentication system may be faster than traditional method, for example: using iris-based recognition may take 2 or 3 seconds while find the smart card or typing the right password, it may take 4 or 6 seconds.

Drawbacks

Like all technology, biometrics comes with a lot of advantages; however, it also has some drawbacks as the cost, time-consuming, unsuitable with someone. Firstly, different biometric technology needs to have a range of cost to deploy in workplace. Moreover, individuals sometimes concern waiting in a long line in order to get inside the building, school or company. Secondly, some biometric method can't apply with someone [13], for example: fingerprint is impossible to authenticate someone with no hands, face recognition fails to identify individual for whole life because their face will change through time and age. Furthermore, when biometrics are common in everywhere in our life, all information are stored in database; therefore, there is no more privacy.

RESEARCH CONTENT

Methodology

This research mainly focuses on the way of biometrics device protecting user's database. Based on the purpose research, hypotheses are formulated at the beginning of the research and tested in this study.

Hypothesis

- H0: Biometrics device is not safe and it can be exploited from the hackers via sniffing attack.
- HA: Biometrics device is safe and it cannot be exploited from the hackers via sniffing attack.

The author used the fingerprint device – *Suprema* to do some experiments (figure 2).

Figure 2: Suprema - fingerprint device [14]

Regarding to this device, it can handle maximum 10000 templates and 5000 users. Firstly, the author registered the some test fingerprints templates into this device by using Biostar v.162 and Biostar server config software to connect between the device and computer via TCP/IP protocol (figure 3), (figure 4).

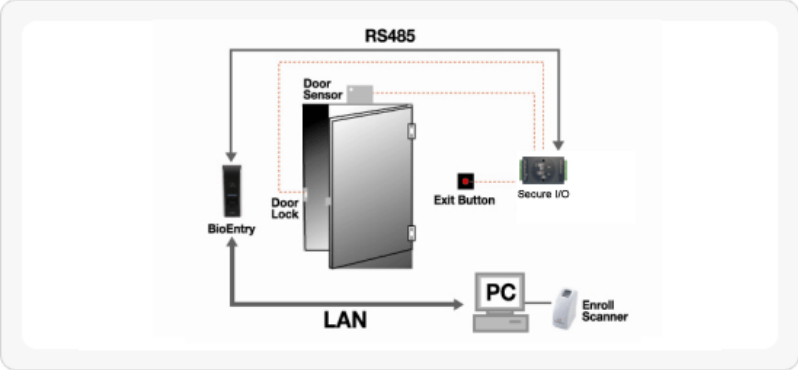


Figure 3: Standalone-secure configuration [14]

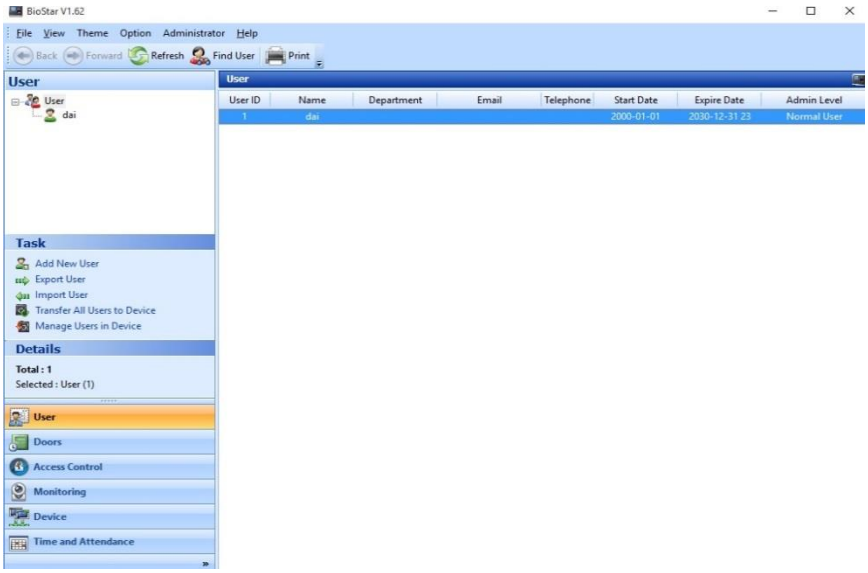


Figure 4.Biostar's interface. (source: own data)

Secondly, the author used Wireshark to capture the data between biometrics device and computer when they transmit the packets during register's session. The packets are the binary signals. Moreover, the captured data are analyzed to find the biggest length of packets (the encrypted information of the user's registration) between biometric device's transaction and laptop (figure 5). The registered templates are saved into *Suprema* memory through *Biostar v1.62*. Then, the next step is that deleting registered templates on the device's memory. Finally, the author tried to play back the captured signal via the biometrics device in order to evaluate the security of the device.

Research result

The author used *Wireshark* tool to capture the signal when the client register from the machine to computer (figure 5).

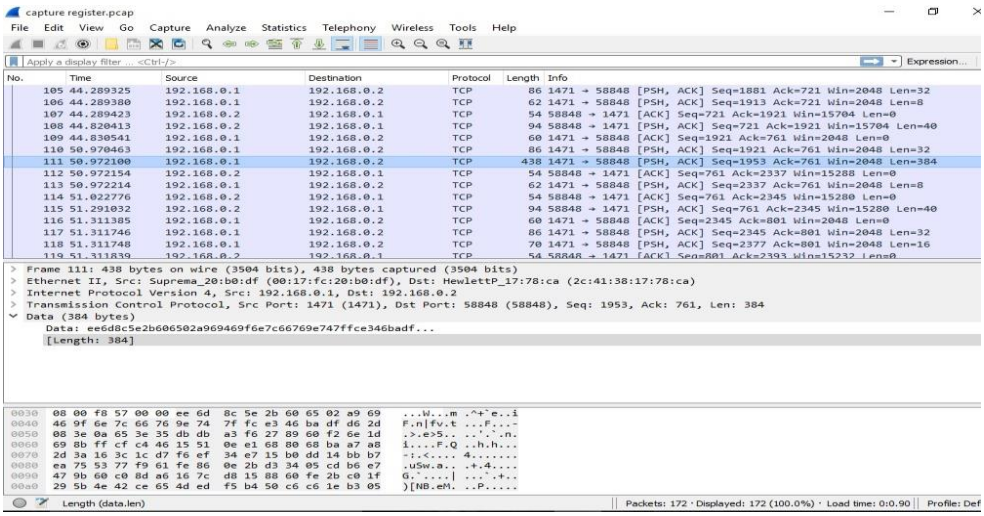


Figure 5. Signal in registration session. (source: own data)

After using *Playcap* tool to play back the signal from the captured data to computer many times, the biometric device couldn't recognize the user's authentication which is registered it before on the device. Therefore, the biometric device rejects the user's fingerprint.

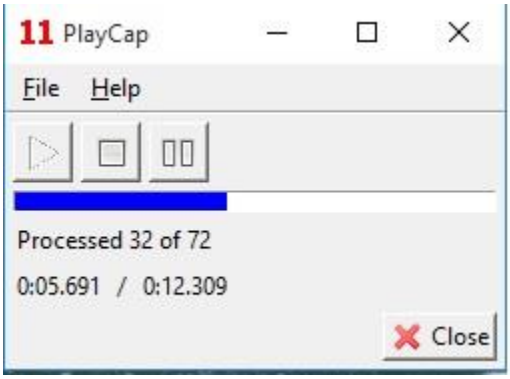


Figure 6. Play back signal to biometric device (source: own data)

In summary, regardings to the results of the attacks to the fingerprint device (figure 2), we accept *HA:* the biometric device is safe and it cannot exploit from hackers via sniffing attack.

CONCLUSION

Fingerprint plays an important role in authentication user's identification. With the benefits of this technology, it makes easier for the users and the implementers to deploy this technology in many aspects. The main contribution of this research is to evaluate the safety of biometrics device. Through the above analysis, this paper showed that biometrics device brings many benefits for the users. Furthermore, the fingerprint is quite safe and security. In the future work, the author uses some other measures to evaluate some different biometric device in order to ensure the safety and security of biometric devices.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2004.

[2] E. Mordini and D. Tzovaras, *Second Generation Biometrics: The Ethical, Legal and Social Context: The Ethical, Legal and Social Context (Google eBook)*. 2012.

[3] A. Babich, "Biometric Authentication . Types of biometric identifiers," pp. 1–56, 2012.

[4] C. Republic, "Biometric Authentication — Security and Usability," *Adv. Commun. Multimed. Secur. IFIP TC6TC11 Sixth Jt. Work. Conf. Commun. Multimed. Secur. Sept. 2627 2002 Portorož Slov.*, vol. 100, pp. 1–13, 2002.

[5] B. Miller, "Everything you need to know about biometric identification," *Pers. Identif. News 1988 Biometric Ind. Dir. Inc., Washingt. DC*, 1988.

[6] L.O'Gorman, "Seven issues with human authentication technologies," *Proc. Work. Autom. Identif. Adv. Technol.*, no. New York, pp. 185–186, 2002.

[7] D. Kumar and Y. Ryu, "A brief introduction of biometrics and fingerprint payment technology," *Proc. 2008 2nd Int. Conf. Futur. Gener. Commun. Networking, FGCN 2008*, vol. 3, pp. 185–192, 2008.

[8] J. Wayman, J. Wayman, A. Jain, A. Jain, D. Maltoni, D. Maltoni, D. Maio, and D. Maio, "An Introduction to Biometric Authentication Systems," *Biometric Syst.*, pp. 1 – 20, 2005.

[9] "Global Security org, Hand geometry and Handwriting. Available: http://www.globalsecurity.org/security/systems/biometrics-hand.htm"

[10] J. Boyd and J. Little, "Biometric gait recognition," *Adv. Stud. Biometrics*, no. July, pp. 19–42, 2005.

[11] "Authentify voice biometric authentication. Available: http://authentify.com/solutions/authentication-concepts/voice-biometric-authentication/"

[12] M. Khitrov, "Talking passwords: Voice biometrics for data access and security,"

Biometric Technol. Today, vol. 2013, no. 2, pp. 9–11, 2013.

[13] V. Burger, “Assignment 1 Biometric authentication”, thesis, 2005.

[14] https://www.supremainc.com/en/AccessControl-TimeandAttendance/Biometric-Devices/BioEntry-Plus

[15] https://www.supremainc.com/en/AccessControl-TimeandAttendance/Biometric-Devices/BioEntry-Plus)

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Szendi József
j.szendi@yahoo.com

IPARI ELJÁRÁSOK HONOSÍTÁSA AZ ÉLELMISZERIPARI VAGYONVÉDELMI KOCKÁZATELEMZÉS HATÉKONYSÁGÁNAK NÖVELÉSE ÉRDEKÉBEN

Absztrakt

A cikk a vagyonvédelmi kockázatelemzés egyik szegletét mutatja be néhány esetpéldával. Az elektronikai iparban és az autó iparban a kockázatelemzési technikák magas szinten kidolgozottak, de azokat jellemzően nem vagyonvédelemre alkalmazzák, hanem gyártási költségoptimálásra. Az eljárások átvételével – akár az élelmiszeriparban is- a vagyonvédelmi minőség biztosítás hatékonysága jelentősen fokozható. A cikk vizsgálja a modell hibáitól független vagyonvédelemre kiható elemzési hibákat is

This article describes a small segment of the risk analysis at the asset and property protection sector. In the electronic and car manufacturing sectors the risk analysis technics are very well developed, but they are used for cost optimization instead of asset protection. Even in the food manufacturing sector the efficiency of the analysis might be in-creased if the procedures are pulled over from other sectors. The article investigates some other risks are not included at the average risk assessments

Kulcsszavak: *kockázat elemzés, minőség biztosítás a vagyonvédelemben, integritás ~ risk analysis, quality assurance in asset protection sector, integrity*

BEVEZETÉS

Ipari környezetben a vagyonvédelem hatékonyságának növelése érdekében, valamint az új OTSZ (Országos Tűzvédelmi Szabályzat) [1] szerinti törvényes kötelezettségek miatt rendszeres bejárásokat, illetve tervszerű megelőző karbantartásokat szükséges tartani a vagyonvédelmi és tűzvédelmi rendszereken. Érintett berendezések a tűzjelzők, a füstcsappantyúk, a tűz gátló zsaluk, a vészkijáratok, a vonulási utak, a vészjelző berendezések és minden olyan infrastruktúra, amelyre az OTSZ kiterjed, de jelen felsorolásban nem szerepel.

A gyakorlatban azonos időben általános munkavédelmi bejárás és általános terepi szemle is történhet, így annak szakszerű dokumentálása – az úgynevezett Hibafeltáró Jegyzőkönyv készítése [2], – a felmerülő additív kockázatok becslésére is alkalmazható.

A KOCKÁZATELEMZÉS CÉLJA

A kockázat elemzés célja visszacsatolás biztosítás a menedzsment számára, megjelölve a feltárt fizikai vagy folyamathibákat. Lényeges eleme a kockázat elemzésnek a prioritások kijelölése. Belátható, hogy egy komplex tűzvédelmi rendszer meghibásodása, majd annak javítása nagyobb prioritást élvez, mint egy alárendelt helyen lévő ablakban tapasztalható üvegrepedés. Bár vagyonvédelmi szempontból a törött üveg egyértelmű biztonsági rés, a Marslow piramis [3] értelmében a teljes objektum biztonságára jelentősen tényezőként hat a tűzjelző hiánya, tehát előbbre kell tenni. Nem elég azonban az esetleges tüzet jelezni, nagyobb a kockázat, ha a vízellátás nem üzemel, ugyanis ekkor a valós tüzet nem lehet oltani.

Az élelmiszeriparban definiált elfogadható mértékű kockázat elve csak tervezési szakaszban működik egy objektum esetében, üzemeltetési szakaszban csak és kizárólag a feltárt hibák azonnali javításának elrendelése jöhet szóba az OTSZ szerint. A tervezési szakaszban is csak közvetve értelmezhető az elfogadható mértékű kockázat elve, hiszen a vonatkozó szabványok már eleve tartalmazzák az „elfogadható mértéket” a tervezési irányelvek lefektetésével, majd szabványos értékek meghatározásával. A hatóság rendkívül szigorú a szemléket illetően: többek között a 6 havi ciklusú füst csappantyú ellenőrzések esetén a következő ellenőrzési ciklusnak 6 hónap +- 1 héten belül kell lennie, különben büntethet a szakhatóság.

A kockázatelemzés célja alapvetően a fenti időtagok szűrése és visszaellenőrzése mellett olyan biztonsági rések feltárása, amelyre az objektum eredeti tervezésekor nem gondoltak. A környezet olyan radikális módon megváltozhatott, hogy indokolttá válik a kockázatok újra becslése. Ipari környezet esetén a problémakör jellemzően új beruházás tervezésekor, termelési kapacitás növelésekor, vagy esetleges részleges bezáráskor merül fel. Indokolt lehet akkor is, ha a technológiai fejlődés elavulttá tette a korábbi vagyonvédelmi technikákat.

Jellemző példa, hogy míg pár évtizeddel ezelőtt jelentős élőerős őrzés mellett valósítottak meg objektum védelmi feladatokat, addigra manapság a beléptető rendszerek [4] automatizálásával, vagy RFID rendszerek [4] bevezetésével csökkentik az élőerő igényt, illetve igyekszenek növelni a feltárás hatékonyságát

A kockázat elemzésnek léteznek jól kidolgozott tudományos technikái. Egyik iparág, ahol részletesen foglalkoznak kockázat elemzéssel az elektronika ipar, lévén az elemek integráltsága olyan mértéket öltött, hogy az áramkörön belül fejlesztendő hibaelhárító algoritmusok (végeredményben redundancia) lehetővé teszi a működést hibás egyedi elemeknél is. Másik iparág, ahol konzekvens kockázat elemzés történik a gyártás során az autó ipar. Az autóiparban a sorozat hibák rendkívül költségesek lehetnek, ezért a mai autókat élettartam optimálással [5][6] – más szemlélet szerint tervezett avulással [7] – tervezik, de a tervezett időtartamon belül adódó gyártásból eredő hibák számát igyekeznek minimálisra

csökkenteni. Klasszikus hosszú távú kockázat csökkentési módszer a karbantartás, amely a kádgörbe értelmében a tervezett élettartamot növeli.

A vagyonvédelmi rendszerek tartalmaznak mechanikus elemeket (autóipari analógia), elektromos elemeket (elektronika ipari analógia), így adja magát a lehetőség, hogy a két iparágban kidolgozott és eljárásokat kockázat elemzési technikaként alkalmazzuk a vagyonvédelmi kockázatok elemzése során.[12] Klasszikus kockázatelemzési technika vagyonvédelmi kockázatok becslésekor helyszíni szemlék tartása, majd szakértő általi kiértékelése a tapasztalati értékek és alapvető vagyonvédelmi szabályok követésével. A bejárás csak egyértelmű, szabad szemmel látható hibák kiértékelésére alkalmas, főleg akkor, ha a hibaesemény már bekövetkezett. Erre példa, hogy ha egy kapuszárny leesik, vagy egy kerítés megroppan, akkor a vagyonvédelmi kockázatok egyértelműen emelkedtek, hiszen illetéktelen bejutás lehetősége lényegesen nagyobbá vált. [11]

Autóipari analógiával azonban a hiba minőségbiztosítási gyökere már a kapu zsanérjának kopásával, a korrózió megjelenésével, a karbantartás elmaradásával, vagy tervezett élettartamból adódó elem alul méretezéséből is adódhat. Ezen folyamatokat, mint kockázat növelő paramétereket figyelembe véve becsülhető a várható érték, azaz az elromlás várható ideje, és az ekkor megjelenő vagyonvédelmi kockázat emelkedésének költségvonzata is. Nyugati terminológiában ezt „cost forecast”-nak hívják.

Kiemelve a zsanér esetét, annak jelentős túl méretezése az élettartamát lényegesen megnöveli. Hasonlóan az autóban alkalmazott kormány összekötő gömbcsap kalkulációjához, ahol gömb alakú alaki jelleg növelése megközelítőleg köbösen növeli a tervezett élettartamot, zsanér esetében is tervezhető, hogy az átmérő növelésével az alaki jelleget figyelembe véve a kopásból eredő hibák száma megközelítőleg négyzetesen csökken.

Ergo, ha egy kapunál az ipari átlagot meghaladó csap méretet ír ki a beruházó, a hiba várhatóan máshol (alapozásból adódó süllyedés, vagy zár hiba) jelentkezik. A zárak duplikálásával merev konstrukció alkalmazásával gyakorlatilag a kapu élettartama olyan mértékben megnőhet, hogy tervezett szerkezeti karbantartást a gyár életében (30 év) nem is kell rá tervezni. Egyetlen hátránya az így gyártott elemeknek, hogy általában drágábbak.

Azonos elvet figyelembe véve RFID leolvasók mechanikai védelmével, a kábelezés mechanikai rögzítésével, a kontakthibák lehetőségének kizárásával a vagyon védelmi kockázatok jelentős mértékben csökkenthetőek, de a kockázatértékelési kalkuláció árulja el, hogy menynyire. A kockázatelemzés szintén kimutatja, hogy a költségek minden határon túl való csökkentése mennyivel emeli meg a vagyonvesztésből adódó károkat.

A VAGYON VÉDELMI KOCKÁZATOK ELEMZÉSÉNEK METÓDUSAI

A kockázat elemzés tudományos módszerei felsőfokú matematikai modellek és technikák alkalmazásával valósulnak meg. Kockázatelemző eljárások felsőfokú valószínűség számítás eljárások alkalmazásával fejleszthetőek, de a kifejlesztett eljárásokat és dokumentációkat a napi rutin során alacsonyabb végzettségű szakemberek is alkalmazhatják. A gyakorlatban tehát a heti ismétlődő bejárásokat végezhetik a dolgozók, de a rendszer jellegű hibákat ismétlődő éves auditokkal szűrik a gyártók. A folyamatauditok tartása ISO és ISF minősítések feltétele.

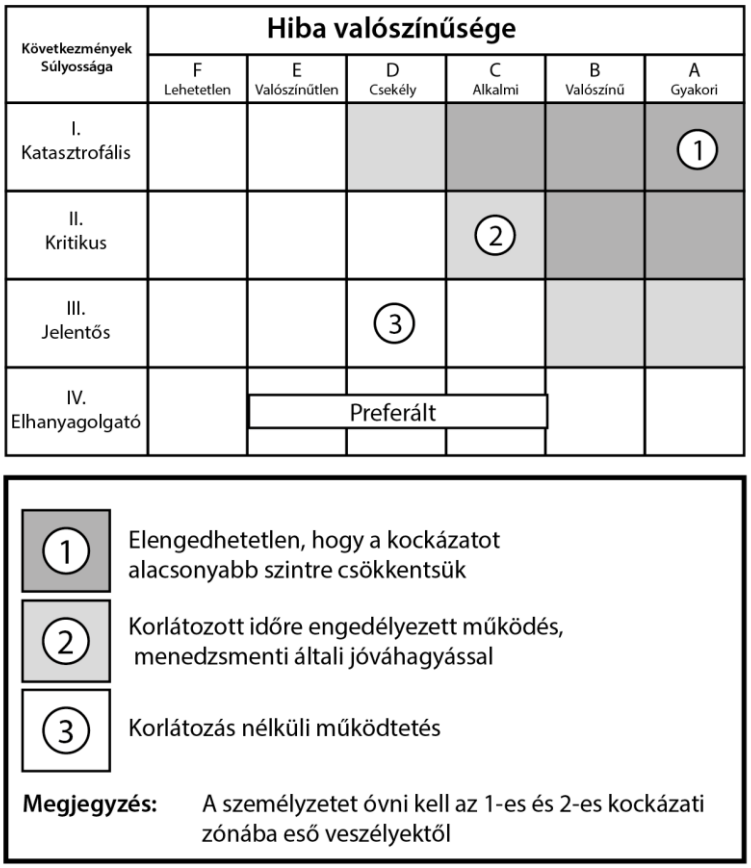
A tudományos elemzés hiába tökéletes, ha az abból adódó vagyonvédelmi kockázatokra adott műszaki tartalom gazdasági érdekek miatt csökkentésre kerül. Klasszikus példa a fukushimai erőmű robbanásának esete [8]. Adott erőmű haváriára vonatkozó kockázat elemzése egyértelműen alá becsülte a lehetséges szökőár magasságát. A helyes matematikai modellek felállításával, majd azok emberi gondolkodással történő (élőerős) elemzésével és szükséges felülbírálásával csökkenthető a vagyonvédelmi kockázat az elfogadható mértékű kockázat szintjére. [13]

Kutatásaim alapján a gyökér oka a vagyonvédelmi kockázatok emelkedésében a politikai és gazdasági felülírásban keresendőek, míg a matematikai modellezés relatíve pontosan képes előre jelezni probléma köröket. Összességében ez emberi hiba.

A kockázatelemzésnek több egyéb metódusa is ismert és jól kidolgozott.[9] A feladat függvényében kell eldönteni, hogy mely metódus hozza költséghatékonyan a legjobb várható eredményt. Élelmiszeripari kockázat elemzés és audit menedzsment részletes leírásaival a [10] forrásban találkozhat az olvasó. A vagyonvédelmi kockázat elemzés része az IFS és HACCP éves auditoknak.

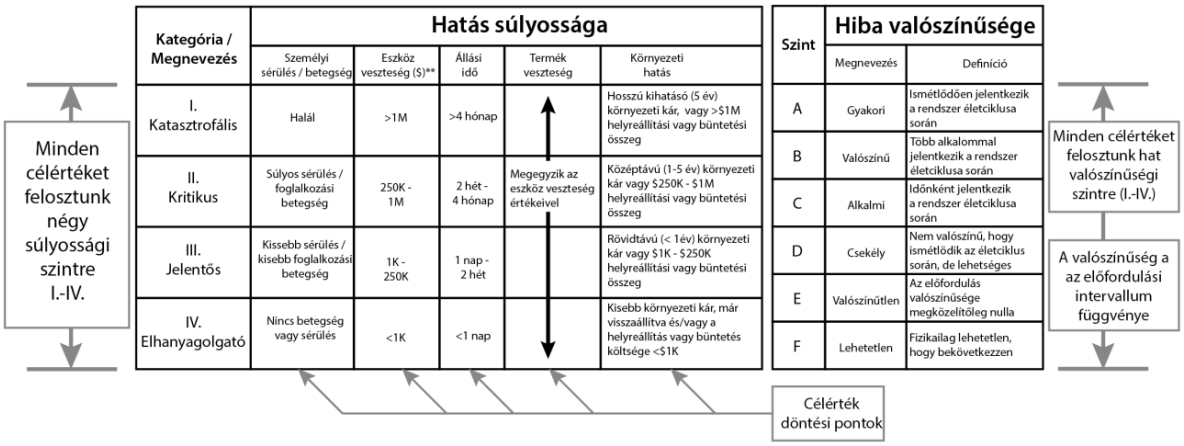
Kockázati mátrix felállítása

A vagyonvédelmi eljárások kiértékelésére kiválóan alkalmazható a kockázati mátrix felállítása. Az eseményeket súlyossági fokozat szerint összevetjük a hibák valószínűségével. Az így kiadódó mátrix elemzésénél a folyamatokat optimálni szükséges, amíg a preferált mezőbe érünk. Az 1. ábra szerint elkészült kockázati mátrix vázlat alapján a lehetséges eseményekre sorokat veszünk fel a bejárások során és a beavatkozó szerv eleve fókuszálni tud a gyakori katasztrofális, majd a kevésbé kockázatos hibákra.



1. ábra. Példa kockázati mátrixra a MIL–STD–882C szabvány alapján. [9]

A kiértékelésnél a valószínűség mellett figyelembe érdemes venni az állási időt illetve a termék veszteségre vonatkozó vagyonvédelmi elemeket is. A személyek védelme elsődleges, de ha vagyonvédelmi hiányosságok merülnek fel egy telephelyen, a kisebb értékű egységek védelmét hátrébb kell helyezni.

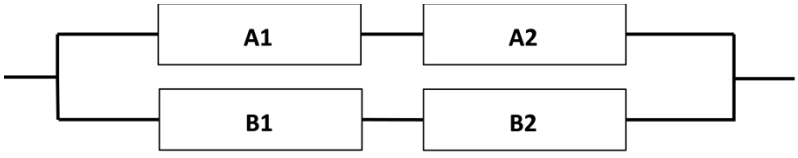


2. ábra. A kockázati mátrix esete környezeti terhelésre. [9]

A fentiekre ellentétes metódus, ha a vagyonőr a portán élelmiszert zsebben kiszállító dolgozót tetten éri, míg egy digitális rendszerrel követett áruforgalmi rendszerben kézi szállítólevéllel egy kamionnyi árut kienged a kapun. A gyakorlatban a vagyonvédelmi mátrix felírásánál a megrendelő szerepe (például a menedzsment) kritikus paraméter, ugyanis a megrendelő igényei szerint felírt mátrix eleve integritás hibát tartalmazhat magában. A kockázati mátrix idő taggal és termék veszteséggel ellátott verziójára példa a 2. ábrán látható.

1002, 1003 rendszer felállítása

Redundáns rendszerek vagyonvédelmi eszközöknél is napi alkalmazásban vannak. Mechanikai rendszereknél a redundáns kiépítésre példa a vészkijáratok számának meghatározása, amennyiben egynél több a kijáratok száma. A kijáratok számának növelésével a menekülési keresztmetszet nő, de a végtelenségig nem növelhető a menekülési utak száma, hiszen akkor szélsőséges esetben az épület funkciója megszűnne és végértéként csak menekülési útból állna (matematikai szélsőérték).



3. ábra. A1002 rendszer. [9]

A metódus használható tűzjelző rendszerek, beléptető rendszerek, kapumozgatók analízisére. Amennyiben a vagyonvédelem részének tekintünk egy folyosói világítás rendszert, kiértékelhetjük, hogy a meghibásodások esetén mely események elfogadhatatlanok. A világító rendszer esetén elfogadhatatlan, ha az őr is botlás veszélynek van kitéve (teljes sötétség), de időtaggal ellátott javítás esetén (pl. 24 órán belül) elfogadható, ha a világítás megközelítőleg a csak felére csökken. A példában négy világító testet vettem fel egy L alakú folyósóra értelmezve, amelynek mindkét szárnyában két-két lámpa van. A válaszfüggvény a [9] alapján 4. ábrán látható

A1	A2	B1	B2	
0	0	0	0	Nincs hiba
0	0	0	1	
0	0	1	0	
0	0	1	1	
0	1	0	0	
0	1	0	1	Elfogadhatatlan
0	1	1	0	Elfogadhatatlan
0	1	1	1	Elfogadhatatlan
1	0	0	0	
1	0	0	1	Elfogadhatatlan
1	0	1	0	Elfogadhatatlan
1	0	1	1	Elfogadhatatlan
1	1	0	0	
1	1	0	1	Elfogadhatatlan
1	1	1	0	Elfogadhatatlan
1	1	1	1	Elfogadhatatlan

4. ábra. A1002 rendszerben a válaszfüggvény értékelése világítás példára. [9]

BEAVATKOZÁSI TERV KÉSZÍTÉSE, AUDITOK

A feltárt kockázatok csökkentésének lehetőségei között az azonnali eseti beavatkozás mellett az ismétlődés ellenes intézkedések meghozása is szükséges. Módszerek lehetnek az éles tesztek mellett a biztonsági rések kutatása, valamint a feltáró auditok tartása.

Élelmiszeripari környezetben a feltáró audit szerepe rendkívül fontos, ugyanis az audit tényét az IFS eleve elvárja. Az éles tesztek elvégzése nem életszerű. A valódi vagyonvédelmi teszteket tartani elsősorban a fizikai berendezések tesztelésével lehet. Ilyen próbák az alábbi keresztmetszeteket vizsgálhatják. Érdemes az életszerűséget, mint paramétert felvenni a kockázati mátrix készítésekor. A lista nem teljes körű.

1. Kerítés elemeinek tesztelése. Jellemzően vízszintesen kívül bordázott kerítés vagyon védelmi szempontból még nagy magasság esetén is jelentős kockázatnak tekinthetőek. A vízszintes elrendezésű bordákon könnyű felmászni. Adott eszköz életszerű mászási teszttel vizsgálható: ha egy 30 alatti átlagos testalkatú férfi könnyen veszi az akadályt az elrendezés nem alkalmas élőerő kizárására. Ilyen kerítések például az acél hegesztett vashálók, vagy az alacsony hálók, de a családi házaknál tapasztalható léccel burkolt vízszintes bordát tartalmazó zártszelvény is potenciálisan gyenge védelem.
2. Nem életszerű a tűzvédelmi berendezések tesztelése éles tűz gyújtásával. A kockázatelemzés része itt a működés tesztelésében, és a helyes kiépítés ellenőrzésében merül ki. Utóbbit az OTSZ részletesen szabályozza.
3. Nyomástartó edényeknél az ellenőrzés módja a Kazán Biztos által készített felülvizsgálati jegyzőkönyvek szemléje. Emelőgépeknél is a szakértői szemle jegyzőkönyvének ellenőrzése a helyes eljárás. A Kazán Biztos eljárásait, mint ultrahangos mérések, tapasztalati értéken adódó szemle, a helyi bejárásokon érdemes felülvizsgálni, de beavatkozni csak ismételt szakvélemény bekérése után lehetséges, ugyanis a szemléző (kockázat elemzést végző csapat tagja) kompetenciája általában nem terjed ki a berendezések szakértésére.

4. Rendszer szemléletű hiba, ha maga az eredeti jegyzőkönyv hamis. A szerző vett részt olyan villámvédelmi mérések átvételén, ahol egyetlen mérési pont sem volt igazolható (rozsdás kötések, nem volt nyoma mérési hely kiépítésének). A valóságban a kockázat emelkedése teljesen életszerű (áramütés veszélye), de a kockázat emelkedés okozója a megrendelő oldalon tapasztalható integritás hiány volt és nem az eljárás műszaki tartalmának hibája. Adott hiba rendkívül körülményesen igazolható, ugyanis ha mérési jegyzőkönyv van pecséttel, annak hamis eredetiségét körülményes igazolni az építő iparban.
5. A fentieken felül a zárakat, világítást, közlekedő utakat, készleteket (útszóró só, hótoló téli gázolaj stb.) mind együtt komplexen kell szemlézni, elsősorban a szabványokat illetve és az életszerűséget szem előtt tartva.

A fentiek és hasonló a szemlék alapján a problémákat priorizálva, a pénzügyi források függvényében, a lehető legrövidebb idő alatt ki kell javítani, vagy az adott területet el kell zárni.

SZŰK KERESZTMETSZETEK

A kockázatok feltárása, számítása, kiértékelése nem elegendő feladat. Sokkal nagyobb kockázat, ha a feltárt hibák agresszív HR stratégia, szűk költségvetési elhatárolás vagy hibás felsővezetői döntés értelmében ignorálásra kerülnek. Míg a tűzvédelmi szabályok az új OTSZ [1] értelmében rendkívül szigorúak lettek, addig a vagyonvédelemnek vannak olyan részei, amelyek rendkívül kitettek az integritássértési szándék előtt. A valós beavatkozásokat a napi politika, a lokális önkormányzat, a felügyeleti szervek összessége és a rendszerek méretéből adódó folyamat lassúsága együttesen visszafogja. Jelen cikk terjedelmi határai miatt a fentiekből a vállalati menedzsment szemléletének hibáit emelem ki.

Egy olyan gyártói környezetben, ahol a dolgozók útiköltség térítése eleve az un. fekete kasszából van finanszírozva, nem életszerű hogy a vagyonvédelmi biztonsági rések feltárása valódi menedzsment által elrendelt igény. Szintén azonos megítélés alá esik, ha a dolgozók úgynevezett belső értékesítésen számla kiállítása nélkül tudnak vásárolni az őrszolgálat jelenlétében, míg a leltárból nem hiányzik semmi. Azonos cég a munkavédelmi kockázat elemzési eredményeket – például más vállalkozó bevonásával –, menedzsment igényére ignorálni is képes.

Ha a valódi gyökérfolyamatokat keressük – amely végeredményben a vagyonvédelmi kockázatelemzés kiterjesztett verziója, – a gyökér ok (root case) a menedzsment integritásának hiánya. Ez utóbbi eddigi kutatásaim szerint és a téma szakértőjének [10] iránymutatása alapján csak a komplex vállalati kultúra fejlesztésével küszöbölhető ki.

ÖSSZEGZÉS

A vagyonvédelemben alkalmazható kockázat elemzési technikák széles palettája általában az éves auditok részeként. A kockázat elemzési technikák lehetnek a kockázati mátrix felállítása mellett az eseményfa, vagy egyéb matematikai modell, mint például a 1002 1003 rendszer felállítása, elemzése és kiértékelése. A teljes analízis alatt kritikus paraméter a menedzsment és a beszállítók integritása, és a beavatkozáshoz szükséges forrás jelenléte. A teljes folyamat nem racionalizálható megfelelő vállalati kultúra nélkül.

Felhasznált irodalom:

[1] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról

[2] Laza Bálint: 70 éves a Marslow piramis, Index.hu, 2013 http://index.hu/tudomany/2013/07/01/hetveneves_a_maslow-piramis/ (Letöltés ideje: 2016.05.27)

[3] Bodrácska Gyula- Berek Tamás: Megelőző intézkedések szerepe a komplex vagyonvédelem területén, építőipari beruházások során, Hadmérnök, V. 1. 2010. http://hadmernok.hu/2010_1_bodracska_berekt.pdf (Letöltés ideje: 2016.05.27)

[4] Berek Tamás –Takács Zoltán: RFID technológia mint a kórházbiztonság területén megvalósuló intézményi rend biztosításának eszköze, Hadmérnök, 2013, VIII. 2. http://hadmernok.hu/132_01_berekt_tz.pdf (Letöltés ideje: 2016.05.30)

[5] Dr. Móga István: Építmények öregedéskezelésének előkészítése, Nukleon, I. évf. 2008. május. p. 5.online: file:///C:/Users/SzendiJ/Downloads/Nukleon1_1_Moga.pdf, (Letöltés ideje: 2016.05.21)

[6] Pálik János: Erőművi rendszerek üzemeltetésének és élettartamának optimálása, Az üzemfenntartás általános kérdései, 2003, http://www.omikk.bme.hu/collections/mgi_fulltext/uzem/2003/04/0401.pdf (Letöltés ideje: 2016.06.05)

[7] HVG.hu: A franciáknál csalásnak minősül a tervezett elavulás, HVG.hu, 2014.10.28 http://hvg.hu/gazdasag/20141028_A_franciaknal_csalasnak_minosul_a_terveze (Letöltés ideje: 2016.05.20)

[8] World Nuclear. org: Fukushima Accident, 2016, http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-accident.aspx (Letöltés ideje: 2016.06.02)

[9] Dr. Abonyi, János - Dr. Fülep, Tímea: Biztonságkritikus rendszerek, Egyetemi Jegyzet, 2014 Pannon Egyetem http://docplayer.hu/18213188-Biztonsagkritikus-rendszerek.html (Letöltés ideje: 2016.06.04)

[10] Dr. Syposs Zoltán: A kockázat elemzés szerepe az élelmiszeripari minőségbiztosításban Szent István Egyetem Áruforgalmi Tanszék, Doktori Értekezés http://phd.lib.uni-corvinus.hu/490/1/de_1627.pdf (Letöltés ideje: 2016.06.02)

[11] Berek Lajos: Biztonságtechnika, Budapest, NKE, 2014 http://real.mtak.hu/19709/ (Letöltés ideje: 2016.06.05)

[12] Dávidovics Zsuzsa-Berek Lajos: Vízbázisvédelem, ivóvízbiztonság, Bolyai Szemle XXI. 2. 2012 http://uni-nke.hu/downloads/bsz/bszemle2012/2/02.pdf (Letöltés ideje: 2016.06.04)

[13] Berek Lajos-Vass Attila: Gázturbinás erőművek objektumvédelme, Hadmérnök IX. 2. 2014. http://hadmernok.hu/142_01_berekl.pdf (Letöltés ideje: 2016.06.06)

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Tóth Attila
atoth@tvt.hu

A MAGÁNBIZTONSÁGI ÁGAZAT MINŐSÍTÉSI RENDSZERE

Absztrakt

A magánbiztonsági ágazatban működő vállalkozásokat minősítő rendszer kidolgozása napjaink aktuális problémája. Szükséges egy olyan objektív minősítési rendszer bevezetése, amelynek segítségével hazánkban a vagyonvédelem területén, a magánbiztonsági ágazatban tevékenykedő összes vállalkozás kategorizálható, minősítési osztályba sorolható. A rendszer bevezetése egyrészt kiszűrné a jogszerűtlenül működő vállalkozásokat, másrészt segítené a Megrendelőket az adott feladat ellátására alkalmas cégek kiválasztásában, a pályázati követelmények megfogalmazásában, hosszútávon pedig az egész ágazat fejlődését eredményezi. Későbbiekben a minősítési tevékenységet ki lehet terjeszteni. Komplett biztonsági auditok során lehet vizsgálni például a telepítésre kerülő biztonságtechnikai rendszerek terveit, illetve a már üzemelő rendszereket.

Elaborating a system of qualifying enterprises operating in the private security sector is a topical problem nowadays. It is necessary to introduce an unbiased qualification system with which every Hungarian enterprise operating in the field of property protection within the private security sector can be properly categorised and classified. On the one hand, the introduction of the system would rule out enterprises that are operating illegally, and on the other hand it would provide assistance to the Principals in selecting the companies being appropriate to carry out the task in question, in wording tender requirements, and in the long run it would result in the improvement of the entire sector. Later on the rating activity could be extended. During complete safety audits, the plans of security systems, for example, could be inspected, alongside with the already functioning systems.

Kulcsszavak: *minősítés, magánbiztonság, tervezés, biztonságtechnika ~ qualification, private security, planning, security technology*

BEVEZETÉS

A magánbiztonsági ágazatban működő vállalkozások és tevékenységeik minősítésének igénye már hat-nyolc évvel ezelőtt megfogalmazódott. Akkoriban a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara[1] elnökségi ülésein több alkalommal napirendre kerültek javaslatok a szakmai minősítési rendszer kidolgozására. Készültek különféle minősítési szempont rendszerek, azonban ezek soha nem kerültek elfogadásra.

A szakmai minősítési rendszer bevezetésével szemben igen nagy ellenállás mutatkozott az ágazat egyes szereplői részéről. A rendszer bevezetését ellenzők leggyakrabban azt hozták fel kifogásként, hogy a szakmai tevékenységet kizárólag a szakmát gyakorlók tudják megfelelő színvonalon auditálni, a piaci szereplők részéről viszont elfogadhatatlan, hogy egy konkurens vállalkozás szakembere hajtson végre náluk ellenőrzést, aki betekint a cég folyamatiba, dokumentumaiba.

A szakmai minősítő rendszer bevezetésének és elfogadtatásának kulcsa egy objektív szempontrendszeren alapuló értékelő rendszer kidolgozása, valamint az önkéntes részvétel a minősítésben. Első körben a vállalkozásokat kell kategorizálni[2], majd később egyes foglakoztatási ágakban ez kiterjeszthető lesz az egyénekre is (pl. vagyonőrök esetében).

A bevezetést követő feladat a rendszer széleskörű megismertetése a magánbiztonsági szolgáltatásokat igénybe vevőkkel, a Megrendelőkkel. A minősített vállalkozások köre akkor fog igazán kibővülni, amikor a Megrendelők elkezdik böngészni a minősített vállalkozások jegyzékét, amikor pályázati kiírásaikban minimum megfelelési követelményként előírják valamelyik szakmai minősítési szint meglétét.

Ez a folyamat felgyorsítható, ha a Biztosító társaságok biztosítási feltételként írják elő, hogy meghatározott objektumokba telepítendő biztonságtechnikai rendszereket, legalább milyen minősítési kategóriába sorolt céggel kell telepíttetni, illetőleg megteszi ugyanezt az élőerős őrzésre vonatkozóan is. A MABISZ VKB[3] és a minősítést végző szervezet együttműködése igen fontos a rendszer bevezetésének sikeressége érdekében. A MABISZ VKB jelenleg különféle biztonságtechnikai termék csoportok minősítését végzi[4], valamint a minősített eszközök alkalmazására egy saját technikai követelmény rendszert[5] határoz meg védelmi kategóriák és kockázatvállalási értékhatárok alapján [1], de a tervezést és a kivitelezést végzőkkel, a különféle vagyonvédelmi szolgáltatókkal nem foglalkozik.

KI MINŐSÍTSEN?

Joggal vetődik fel a kérdés, hogy ki dolgozza ki a minősítési rendszert, ki végezze a minősítést? A kérdésre egyszerű a válasz, amit a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény 38.§ (1) d) bekezdésében találunk: „A Kamara az e törvény hatálya alá tartozó tevékenység végzésére jogosító, külön jogszabályban meghatározott szakképesítések tekintetében a rendészetért felelős miniszterrel kötött megállapodás alapján kidolgozza és gondozza a szakmai és vizsgakövetelményt, a szakmai minősítő rendszert, közreműködik a szakképzésben és a vizsgáztatásban, valamint javaslatot tesz az állam által elismert szakképesítésre, a szakmai vizsgaszabályzatra, a szakmai vizsga szervezését engedélyező, valamint a vizsgaszervezési tevékenységek elle-

[1] a továbbiakban: SzVMSzK
[2] minősítési osztályba sorolni
[3] Magyar Biztosítók Szövetsége Vagyonvédelmi és Kármegelőzési Bizottság
[4] értéktárolók, mechanikai-fizikai védelem elemei, biztonsági üvegek, fóliák, elektronikai jelzőrendszerek elemei, videotechnikai és beléptető eszközök minősítésével foglalkozik
[5] ez a követelmény rendszer nincs összhangban az Európai Unióban érvényben lévő erre a szakterületre vonatkozó szabványokkal

nőrzése során szakértőként kirendelhető személyekre.” [2] Tehát a Szakmai Kamara felelős a Magánbiztonsági ágazatba tartozó szakképesítések esetében a szakmai és vizsgakövetelmények, valamint a szakmai minősítő rendszer kidolgozásáért.

A fentiek alapján logikusnak tűnik, hogy független szakmai szervezetként a vállalkozások minősítő rendszerét is a Kamara dolgozza ki és működtesse, illetve a minősített Vállalkozásokat nyilvántartsa, közzé tegye.

Az OKJ-s szakképzési rendszerben [3] szerepet vállaló vállalkozások minősítésére ki is dolgozott a Kamara egy minősítő rendszert. [4] Ez a minősítő rendszer azonban csak a Belügyminiszter ágazatába tartozó olyan szakképesítésekben szerepet vállaló cégekre vonatkozik, amely cégek az adott OKJ-s szakképzésben előírt szakmai gyakorlat idejére gyakorlati helyet biztosítanak. Tehát ez a rendszer kizárólag a „szakképesítés megszerzésére irányuló szakképzés összefüggő munkahelyi szakmai gyakorlati képzése folytatására jogosult vagyonvédelmi gazdálkodó szervezetek feljogosító eljárása, tanúsítása, nyilvántartása és ellenőrzése” [4] céljából készült.

KIT KELL MINŐSÍTENI?

A minősítési rendszer bevezetése több féle módon lehetséges. Egy megvalósítható bevezetés lépései a következők lehetnek:

Első lépésben a magánbiztonság különböző területein működő vállalkozásokat kell minősíteni, a cégek által megadott adatok alapján. A bekért adatokhoz a közbeszerzési eljárásoknál megszokott módon, az igazoló dokumentumokat, nyilatkozatokat is be kell kérni. A beküldött adatok alapján a cégek minősítése-kategorizálása elvégezhető (akár automatizált módon is). Ebben a fázisban a bevallást önkéntesen beküldő vállalkozások bekerülhetnek egy minősítési kategóriába, egy nem ellenőrzött jelöléssel. Ez még csak egy tájékoztató jellegű minősítést jelent.

A minősítési kategóriába sorolt vállalkozások kérhetik a minősítő szervezettől (SzVMSzK) a benyújtott adatok igazoló ellenőrzését, amelyet egy független szakértői csoport – a cég dolgozói létszámának arányában növelendő a szakértői csoport létszáma – végez el egy helyszíni audit keretében. A szakértői csoport ilyenkor – hasonlóan egy beszállítói audithoz – ellenőrzi a cég által benyújtott adatokat, a cég folyamatait, a minőségirányítási rendszer működtetését stb. A helyszíni audit költsége az ellenőrzést kérő céget terheli. Az audit eredményeképpen kerülhet kiállításra az elért minősítési kategória igazolására szolgáló tanúsítvány.

A későbbiekben a minősítési rendszer akár tovább finomítható, a vállalkozások különböző tevékenységeik, különböző kategóriába sorolásával. Például nem minden biztonságtechnikai rendszereket telepítő cég foglalkozik tervezéssel vagy nem mindegyik telepít automatikus tűzjelző rendszereket. Hasonló példa lehet egy élőerős őrzéssel foglalkozó cég, amelyik néha telepít kisebb behatolás jelző rendszereket, mert van két-három hozzáértő, biztonságtechnikai rendszerszerelő OKJ-s képzettséggel és biztonságtechnikai szerelő rendőrhatósági engedéllyel rendelkező alkalmazottja, de ez a tevékenység nem összemérhető azzal a céggel, amelyik 40-50 fővel végzi ugyanezt a tevékenységet pl. nagy ipari objektumokban. Ezeknek a több tevékenységi körrel rendelkező vállalkozásoknak a különféle tevékenységeit külön lehetne kategorizálni.

A következő fontos lépés lehet a biztonságtechnikai rendszereket tervező-telepítő cégek tervdokumentációinak, kivitelezési folyamatainak auditálása. Ez nagyon fontos, mert jó terv alapján, jó eszközökből is lehet szakszerűtlen kivitelezéssel nagyon rossz rendszert kialakítani és rossz tervdokumentáció alapján, jó eszközökből a jó Kivitelező se tud biztonsági rések nélküli, hibátlan rendszert építeni. Nagy biztonsági kockázatú objektumok esetében a tervdokumentációk-kivitelezések független szakértői ellenőrzése nagyon fontos lenne.

Ugyanez az élőerős területen is napi aktuális problémaként jelentkezik. A biztonsági személyzet, vagyis a humán tényező az objektumvédelem nagyon fontos biztonsági eleme. Az adott feladatra megtalálni azt a feladatot ellátni képes vagyonőrt, aki ebben a feladatban ki is tud teljesedni és, aki ez által megfelelően motiváltan tudja a munkakörét ellátni, nagyon nehéz feladat. Jelenleg nem működik olyan minősítési rendszer, amely a vagyonőröket képességeik-képzettségeik szerint kategóriákba sorolná, pedig egy ilyen rendszer óriási segítséget jelentene a Munkáltatóknak a munkavállalók kiválasztásában, valamint a Megbízóknak – az őrzésvédelmi szolgáltatást igénybe vevőknek – az alkalmazandó vagyonőrökkel szemben támasztott követelmények megfogalmazásában. [5]

A MINŐSÍTÉSI SZEMPONTRENDSZER

A minősítési szempontrendszer összeállításánál legfontosabb, hogy olyan adatokat kell bekérni, amelyek alapján objektíven kategorizálhatók a különféle vállalkozások.

A magánbiztonsági ágazat különféle területein működő vállalkozások nem kategorizálhatók azonos minősítési szempontrendszer alapján. Teljesen más szempontok alapján kell minősíteni egy élőerős őrzéssel foglakozó vállalkozást vagy egy biztonságtechnikai rendszereket tervező vállalkozást. Ugyanúgy nem követelhetjük meg egy élőerős őrzéssel foglalkozó cégtől, hogy rendelkezzen biztonságtechnikai mérnök végzettségű, tervezői engedéllyel rendelkező alkalmazottal, mint ahogy a biztonságtechnikát tervező-, telepítő cégtől se kérhetünk például 10-20 főállású személy-, és vagyonőrt. Természetesen a példában említhettük volna a magánnyomozással foglalkozó cégeket is, amelyekkel szemben megint más követelményeket kell támasztani.

A szempontrendszernek szakmai területenként egyedinek, de területen belül általánosan alkalmazhatónak kell lennie. A területenként egyedi követelményrendszer biztosítja a területen belüli általános alkalmazhatóságot.

A szempontrendszer kialakítása ideális esetben úgy történik, hogy az ágazat különböző szereplőinek műszaki-technikai felszereltségét, gazdasági jellemzőit jól ismerő munkacsoportokat hoznak létre. A munkacsoportokat ágazatonként kell kialakítani. (pl. magánnyomozó szempontrendszert összeállító munkacsoport, biztonságtechnika szempontrendszert összeállító munkacsoport stb.) A munkacsoportok tagjai egyénileg összeállítanak egy-egy értékelési szempontrendszert. Az egyének által egymástól függetlenül összeállított szempontrendszerek összesítését követően a szempontok között találunk olyanokat, amelyeket a munkacsoport több tagja is leírt és lesznek olyanok, amelyekre csak egy-egy személy gondolt. A végeredmény mindenképpen egy kezelhetetlenül nagy halmaz lesz. Ezt a halmazt kell kezelhető méretűre csökkenteni oly módon, hogy a szempontrendszer teljessége megmaradjon, tehát a megmaradó szempontok alapján az adott ágazat szereplői teljes mértékben értékelhetők legyenek. A halmaz a Pareto-elv alapján[6] jelentős mértékben csökkenthető. A szempontok közül ki kell szűrni azokat, amelyek ugyanarra a tulajdonságra vagy funkcióra kérdeznek rá, mert ezek az értékelés során torzíthatják a kapott eredményeket. Ki kell szűrni továbbá az ellentmondásos értékelési szempontokat, amelyek egymást kizárhatják. Nagyon fontos, hogy a kialakult szempontrendszernek jól érthető legyen, pontos, de egyszerű definíciókat tartalmazzon és lehetőség szerint 15 elemnél többől ne álljon[7]. [6] A kellő mértékben leegyszerűsített, az ágazat szereplőit teljes mértékben körülíró szempontrendszer még nem alkalmas a szempontrendszert kitöltő vállalkozások kategorizálására, minősítésére. Ez könnyen belátha-

[6] Pareto azt állította, hogy a megtermelt javak 80%-a a társadalom 20%-ához kerül a vagyonelosztás során, ez az elv az élet sok más területén is igaznak bizonyult. pl. a problémák 80%-a visszavezethető az okok 20%-ára, vagy esetünkben a kialakult sok elemből álló szempontrendszer 20%-a lefedi a cégek minősítését befolyásoló tényezők 80%-át.

[7] Ennek fontosságára a szempontok súlyozásának meghatározásánál visszatérek.

tó, hiszen a különféle értékelési szempontok, különböző fontosságúak a cégek megítélésnek szempontjából. Ahhoz, hogy a szolgáltatás minőségét kevésbé befolyásoló tényezőket kisebb mértékben vegyük figyelembe az értékelés során, az értékelési szempontrendszer elemeit fontosságuk arányában súlyozni kell.

A súlyozás mértékének meghatározása legalább annyira fontos feladat, mint a jó szempontrendszer összeállítása. A súlyszámok meghatározásakor ki kell zárni minden szubjektív hatást, cégektől és egyénektől független súlyozási rendszert kell kialakítani. A súlyszámok meghatározását a szempontrendszer kialakításhoz hasonlóan, az adott területet jól ismerő szakértőkből álló munkacsoportnak kell megalkotni. A súlyszámok meghatározására közgazdászok és matematikusok számos módszert dolgoztak ki, ezek közül a fontosabb különbségek megértése érdekében hármat mutatok be.

A legegyszerűbb módszer a közvetlen becslés módszere: ennél a módszernél súlyszám meghatározását végző szakértő becsléssel állítja fontossági sorrendbe a szempontokat. n számú szempont esetén, minden szemponthoz 1/n súlyszámot rendelve úgy, hogy a súlyszámok végösszege 1 legyen. Néhány értékelési szempont esetén még alkalmazható ez az eljárás, de már 10-15 szempontnál nagyon nagy koncentrációt és következetességet igényel. Könnyen belátható, hogy ennél a módszernél a szakértő szubjektivitása nem zárható ki. Több szakértővel elvégeztetve a közvetlen becslést, a szakértők következetessége, egyetértésük vizsgálható (rangkorrelációs együttható). Ebben az esetben a szakértők által felállított szempontok sorrendisége jó esetben meg fog egyezni, de a becsült súlyszámok eltérőek lesznek, nem lesznek pontosak. [7]

A pontosság növelésére dolgozott ki Churchman és Ackoff 1957-ben két eljárást [8], amelyet a szakirodalomban Churchman-Ackoff-féle eljárásként neveznek. Ez a módszer a fontossági sorrendbe állított szempontok páros összehasonlításán alapul. A súlyszámok meghatározásánál az első szempont (legfontosabbnak ítélt szempont) súlyát 1-nek tekintjük és ehhez hasonlítjuk az összes többi szempontot, amelyekhez egy az első szempont fontosságához mért relatív súlyszámot rendelünk. Ezt követően a szempontokból csoportokat hozunk létre és vizsgáljuk, hogy a csoportba rendelt szempontok súlyszámainak összege hogyan aránylik egy fontosabbnak ítélt szemponthoz, majd annak megfelelően módosítjuk a csoportban a súlyszámokat vagy a fontosabb szempont súlyszámát. Ezt minden szempont bevonásával elvégezzük, végül a kialakult súlyok normalizálásával meghatározzuk a végleges súlyozást. Ekkor a normalizált súlyszámok összege 1 lesz. A módszer hátránya, hogy nagyon munkaigényes, éppen ezért 7 szempont felett már nem is ajánlott az alkalmazása. [9] Nagyobb számú szempont összehasonlítására Churchman és Ackoff egy második módszert javasol, amelyben legfeljebb 5 szempontból álló csoportokat alakítunk ki, mindegyikhez hozzárendelünk egy meghatározott szempontot, amelynek súlyát egynek vesszük, minden csoportban elvégezzük az első módszer szerinti kiértékelést, majd megvizsgáljuk, hogy az eredményül kapott sorrend megfelel-e az felállított fontossági sorrendnek. Ha nem felel meg, akkor meg kell ismételni az eljárást más szempont kiválasztásával. Ha megfelel, akkor a kialakult súlyok normalizálásával meghatározzuk a végleges súlyozást.

Az eddig bemutatottaknál egyszerűbben használható a Guilford-féle módszer [10], amelyet a magánbiztonsági ágazatban kidolgozásra kerülő minősítési szempontrendszer egyes szempontjai súlyszámának meghatározásához javasolok. A módszer a páros-összehasonlítás elvén alapul. A minősítési szempontokat egy $n \times n$ mátrixba rendezzük, ahol minden egyes szempontot összehasonlítunk az összes többivel. Ha feltételeket C-vel jelöljük, akkor a mátrix (i, j)-edik $(i \neq j)$ eleme 1, ha Ci fontosabb Cj -nél és 0, ha Cj fontosabb Ci-nél. Önmagával egyik szempontot se vizsgáljuk, ezért a mátrix főátlójában nincsenek elemek. A mátrix sorösszegei megadják, hogy az adott szempont, hány másik szempontnál volt fontosabb. A sorösszegek normalizálását követően megkapjuk az 1 összegű súlyszámokat. [6] A súlyszámok tovább finomíthatók, ha a kialakult súlyozást a normális eloszlás alapján áttranszformáljuk,

tehát a súlyozott átlagokat normalizáljuk. [11] A módszer alkalmazása 12-15 szempont esetén egyszerű, de odafigyelést és következetességet igényel. Nagy előnye, hogy vizsgálható a kitöltő szakértő következetessége, kiszűrhetők vele a kitöltő által elkövetett hibák, (pl. körhármasok kialakulása). Több szakértő esetén a szakértők együttes véleménye is kialakítható pusztán matematikai módszerek alkalmazásával. [7] A minősítési szempontrendszer így elkészített súlyozása objektívnek tekinthető.

A MINŐSÍTÉSI RENDSZER HATÁSA A MAGÁNBIZTONSÁGI ÁGAZATRA

Mikor elérjük a bevezetőben említett pontot, amikor is a Megrendelők ajánlatkéréseikben és pályázati kiírásaikban minimum megfelelési feltételként írják elő valamely minősítési kategória meglétét, akkor éri el a minősítési rendszer a célját. Ekkor egy öngerjesztő-önfenntartó fejlődési folyamat fog elindulni a magánbiztonsági ágazatban. A ma még engedély nélkül működő vállalkozások rendőrhatósági engedélyt fognak kérni, hogy bekerülhessenek a minősítési rendszerbe, ezt követően már ellenőrizni fogja tudni a tevékenységüket a rendőrség. A minősítési megszerzése érdekében regisztrálni fognak a Szakmai Kamarába, ha tevékenységükkel kapcsolatban panasz érkezik a Kamarához, akkor annak Etikai bizottsága eljárást indít ellene [12], aminek következménye akár a kamarai regisztrációjának felfüggesztése is lehet, ezzel kikerülhet a minősítési rendszerből, így nem tud majd részt venni pályázatokon.

A vállalkozások szeretnének minél magasabb minősítési szinteket elérni a nagyobb – jobban fizető – megbízások reményében, ennek érdekében fejleszteni fogják vállalkozásukat, képezni fogják munkavállalóikat. A munkavállalók pedig szívesebben mennek majd a magasabb minősítéssel rendelkező cégekhez dolgozni, mivel tudni fogják, hogy ott magasabb jövedelemre számíthatnak. A magasabb minősítési szinteket elérő vállalkozások ez által nagyobb munkaerő kínálatból választhatnak, kiválogathatják a legjobban képzett, az adott feladat elvégzésére legalkalmasabb munkavállalókat. Ezzel a munkát keresőket is önképzésre ösztökélik.

Hosszútávon a szakmai minősítési rendszer bevezetése és következetes működtetése jelentheti a magánbiztonsági ágazat letisztulását, „kifehéredését”, az ágazatban tevékenykedő vállalkozások fejlődését, a szakma megbecsültségének emelését. Mindezek következményeképpen pedig várhatóan az ágazat által nyújtott szolgáltatások értéke is emelkedni fog.

Felhasznált irodalom

[1] M. VKB, „Betöréses lopás- és rablásbiztosítás technikai feltételei ajánlás,” Magyar Biztosítók Szövetsége, Budapest, 2002. február, Utolsó módosítás: 2015. április 24.

[2] 2005.évi CXXXIII. tv. a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.

[3] 20/2013. (V. 28.) BM rendelet a belügyminiszter ágazatába tartozó szakképesítések szakmai és vizsgakövetelményeiről.

[4] E. Bakur, 18 02 2015. http://szakmaikamara.hu/files/images/Orszagos/Kabinet/minosites/a_maganbiztonsag_minositesi_szabalyzata_1_fejezet.pdf. [Hozzáférés dátuma: 19 május 2016].

[5] G. Csege és T. Gáll, „Az élőerős vagyonvédelem problematikája,” Hadmérnök, pp. 6-7, 2014. december.

[6] S. Bozóki, „Súlyozás páros összehasonlítással és értékelés hasznossági függvényekkel a többszempontú döntési feladatokban,” Budapesti Corvinus Egyetem, Budapest, 2006.

[7] J. Gyarmati, „Többszempontos döntéselmélet alkalmazása a haditechnikai eszközök összehasonlításában,” Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003.

[8] C. Churchman, R. Ackoff és Arnoff E.L., Introduction to Operations Research, John Wiley & Sons: New York, 1957.

[9] J. Kindler és O. Papp, Komplex rendszerek vizsgálata – összemérési módszerek, Budapest: Műszaki Könyvkiadó, 1977.

[10] J. Guilford, Psychometric Methods, New York: McGraw-Hill Book, 1936.

[11] J. Dr. Kata, Mérnöki módszerek a pedagógiában, Budapest: Typotex Kiadó, 2013.

[12] SzVMSzK, „Kamarai Szabályzatok,” http://szakmaikamara.hu/files/Etikai_szabalyzat_2016-01-15.pdf. [Hozzáférés dátuma: 20. május 2016.]

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Somosi Vilmos
vilmos.somosi@hungarocontrol.hu

LÉGIFORGALMI IRÁNYÍTÓI SZOLGÁLTATÁS DELEGÁLÁSA LEHETŐSÉGEINEK ÉS FELTÉTELEINEK ÁLTALÁNOS VIZSGÁLATA

Absztrakt

Az elmúlt évtizedben az európai polgári léginavigációs szolgáltatói környezetben felértékelődött a delegált, illetve távoli (remote) légiforgalmi szolgáltatások kialakításának szükségessége. Ezen szolgáltatásoknak a polgári légiközlekedésben várható jelentős intenzitású elterjedése új feltételeket és körülményeket teremt a légtérellenőrzés és légtérvédelem, illetve a polgári-katonai szakmai együttműködés terén. A cikkben a légiforgalmi irányítói szolgáltatás delegálásának indokai és módozatai kerülnek bemutatásra, egyben a szerző rávilágít a szolgáltatások és a légtérellenőrzési folyamatok közötti kapcsolatára is.

The European civil air navigation service providers have revalued the needs of delegated air traffic services in the last ten years. The possible intensive expansion of these solutions will determine new conditions and circumstances regarding airspace control, air defense and also in the civil-military cooperation. The article introduces the reasons and modalities of air traffic service delegation and the author highlights the linkage between those services and airspace control procedures

Kulcsszavak: *légiforgalmi irányítás, légtér, távoli irányítás, virtuális torony, delegált légtér ~ air traffic service delegation, airspace, remote control, remote TWR, delegated airspace*

BEVEZETÉS

Az 1990-es évek politikai és világgazdasági változásai a légiközlekedésre és légtérellenőrzésre is jelentős hatást gyakoroltak, így az elmúlt negyed évszázadban soha nem látott mértékű növekedés volt tapasztalható a nemzetközi légiközlekedésben is. Ezt a növekedést kiválóan szemléltetik azok a számadatok, melyet a légi fuvarozók nemzetközi szövetsége az IATA[1] publikált. E szerint világviszonylatban 58 millió munkahelyet, és 2,4 billió USD GDP-t biztosító légiközlekedési szektorban 2014. évben 3,3 milliárd utas és 50 millió tonna teheráru mozgása valósult meg [1][2].

A növekvő igényeket és egy hatékonyabb európai légiközlekedési infrastruktúra létrejöttét az Európai Bizottság (több mint tíz éve már) az egységes európai égbolt[2] kezdeményezésen keresztül tervezi megvalósítani, többek között az európai államok szuverén légtereinek optimalizált kihasználásán keresztül. A bizottsági elképzeléseket, különösen a légtér kapacitásának korlátjainak feloldását, a hasznosítás lehetőségeinek kiaknázását és a forgalmi trendek előrejelzését a nemzetközi szakmai szervezetek jelentéseikkel, tanulmányaikkal és javaslataikkal támogatják (pl. az Amerikai Egyesült Államok légügyi hivatala[3,] a Bizottság és az EUROCONTROL[4] által az észak-amerikai és az európai kontinens légiközlekedési infrastruktúrájának hatékonyságát összehasonlító elemzések [3]).

Az intézmények munkái mellett nemzetközi viszonylatban évtizedek óta születnek értekezések a jelentősen tagolt (fragmentált) európai légtér és légiforgalmi szolgáltatás kapcsolatáról [4]. D. Learmount 1989-ben közétett igazolása [5] már előre vetítette, milyen problémákat jelentenek a légtérszervezés kialakításában és a műszaki berendezések beszerzésekor alkalmazott eltérő nemzeti stratégiák. Több kutató is elemezte a megnövekedett légiforgalom és a kapacitási problémák, illetve a légiforgalmi késések kapcsolatát [6]. A szuverenitásnak a légiforgalmi szolgáltatókra gyakorolt hatásaira rávilágított R. Schwenk 1998-ban végzett elemzése is, [7] míg 2004-ben a légtérszervezés és felhasználás problémáinak tényezőit M. S. Nolan összegezte [8].

A légiközlekedés jogi kérdéseivel, [9] a légiforgalmi szolgáltatási környezettel, [10] az európai egységesítési folyamatokkal [11] és a légi útvonal-hatékonyságnövelés [12] lehetőségeivel összefüggésben, hazai környezetben is születtek tudományos munkák, a légiforgalmi irányító szolgáltatás delegálás és annak polgári-katonai vonatkozású hatásai viszont eddig nem képezték részét mélyreható nemzeti és nemzetközi kutatásoknak.

Az erre irányuló elemzések szükségességét alátámasztja annak a kérdésnek a vizsgálata, hogy a szolgáltatók közötti szakmai kapcsolati rendszer formálódása, illetve az iparágban tervezett liberalizáció eredményeként a földrajzi értelemben függetlenné váló (távoli vagy központosított) légiforgalmi irányítási, kommunikációs, navigációs és légtér-felügyeleti funkciók milyen formában illeszkednek a Magyar Honvédség légiforgalom-szervezési rendszeréhez, [13] melyben szintén kiemelt helyen szerepel a polgári-katonai együttműködés [14] kérdése.

További válaszokat igényel, hogy a fentiek miként szavatolják a NATO Integrált Légvédelmi Rendszerébe (NATINADS[5)] légtér-ellenőrzési és légtérrendészeti kötelezettségeinek maradéktalan teljesítését békeidőben és minősített időszakban.

A kérdéskör kutatáshoz szükséges információkat különösen a HungaroControl Magyar Légiforgalmi Szolgálat Zrt. szakmai és üzleti adatbázisából, a Nemzeti Közszolgálati Egyetem könyvtárából, valamint a légiközlekedésben vezető szerepet játszó nemzetközi

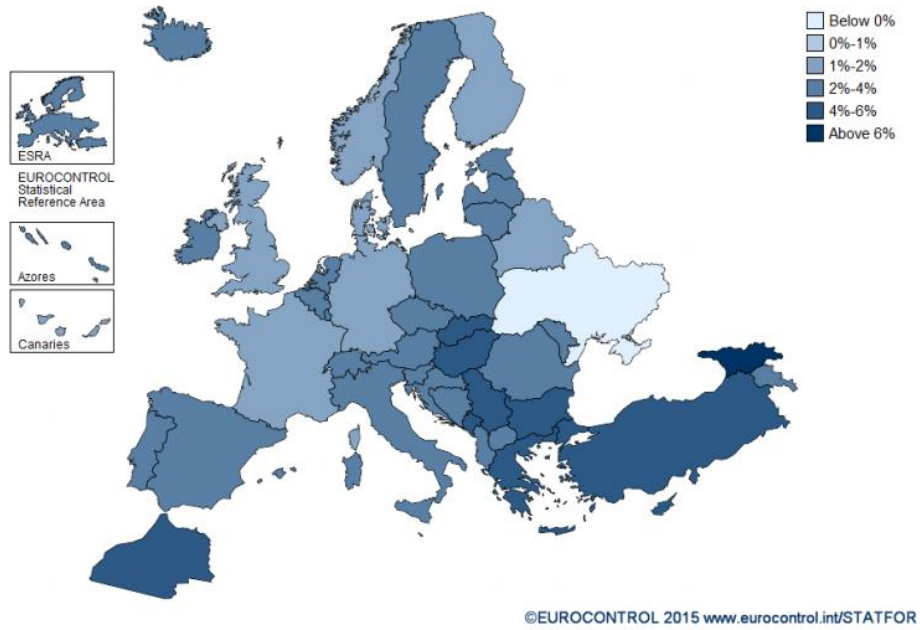
[1] International Air Transport Association - 260 légitársaságot tömörítő nemzetközi szervezet
[2] Single European Sky (SES) I és II. jogszabályi csomagok
[3] FAA – Federal Aviation Administration
[4] Európai szervezet a légiközlekedés biztonságáért
[5] NATO Integrated Air Defence System

szervezetek és a vonatkozó jogszabályok internetes forrásaiból gyűjtöttem, rendszereztem és dolgoztam fel. A rendelkezésre álló információk alapján végezetül egy sajátos szolgáltatás-delegálási csoportosítást alkottam, melyeket nemzetközi példákon keresztül szemléltetek.

A LÉGIFORGALOM ÉS A LÉGTÉRELLENŐRZÉS KAPCSOLATA

A főleg a közel-keleti és ázsiai térségben tapasztalható gazdasági fejlődés és az Európával határos térségek konfliktusai következményeként átrendeződő forgalmi trendek napjainkra azt is eredményezték, hogy az európai légtér (különösen a délkelet-északnyugati áramlási irányultságban érintett légiforgalmi irányítói szektorok) kapacitásának maximumához közelít, mely a jelenlegi technológiai háttérrel és infrastruktúrával közép- és hosszú távon nem lesz biztonságosan fenntartható és kiszolgálható.

A légi forgalom áramlásának felügyelete és szabályozása azonban nem csak a polgári légifogalmi irányítói szolgálatok, hanem a nemzeti és a szövetségi légtérellenőrzésért felelős katonai egységeknek is a feladata, melyből adódóan felértékelődig a polgári-katonai együttműködésben a nemzeti légvédelem légtér-ellenőrzési és légtérrendészeti kötelezettségeinek maradéktalan teljesítésének szavatolása. Ennek vizsgálata különösen abban az esetben válik kiemelten fontossá, amikor az adott nemzeti légtérben már nem két fél (nemzeti honvédelmi és polgári szervezetek), hanem egy harmadik (nemzetközi) szereplővel is ki kell alakítani a béke és minősített időszaki együttműködés feltételeit.



1. ábra Hét éves európai légiforgalmi előrejelzés [15]

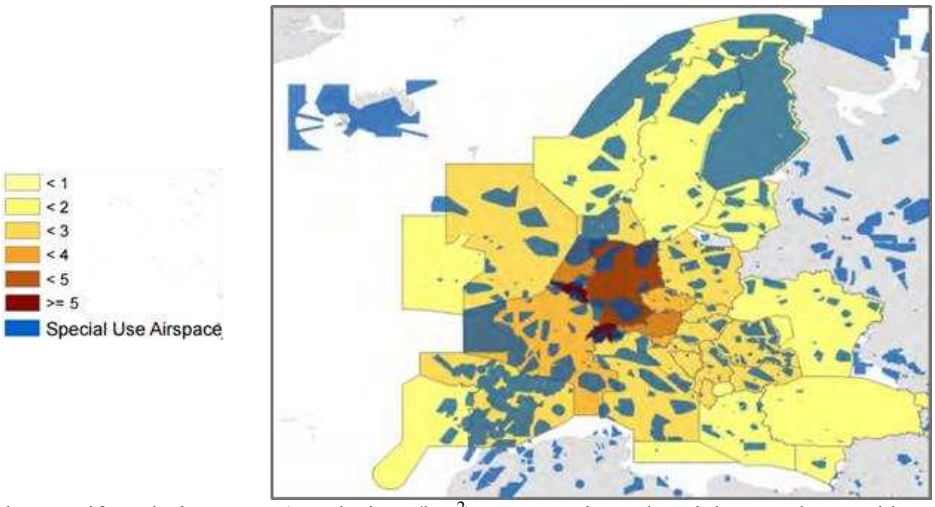
FRAGMENTÁLT EURÓPAI LÉGIFORGALMI KÖRNYEZET

Az Európai Bizottság és az IATA álláspontja szerint az európai légiközlekedés fejlődésének és fenntarthatóságának legkritikusabb eleme a töredezett légtér és a hozzá kapcsolódó széttagolt légiforgalmi irányítói szolgálatok (ATS[6]) infrastruktúrája. Ennek elsődleges magyarázata, hogy az 59 szuverén európai állam [16] önálló légiforgalom-szervezési és léginavigációs környezet alakított ki, melyben a szolgáltatásért felelős nemzeti

[6] Air Traffic Services

monopóliumok (léginavigációs szolgáltatók, ANSP[7]-k) egyenként, de egymással valamilyen relációban biztosítják a szolgáltatásaikat a szuverén nemzeti légterekben, illetve a repüléstájékoztató körzetekben.

A NATO országok esetében fontos megemlíteni a nemzeti polgári léginavigációs szolgáltatók azon kötelezettségét is, miszerint radar és repülési adatokat kötelesek szolgáltatni a nemzeti katonai légtérellenőrző szolgálatokon és rendszereken keresztül a NATO Integrált Légvédelmi Rendszerébe. Mindezeken túl, a töredezettséget tovább fokozzák az államok katonai felhasználású légterei (SUA[8]) is, melyek térben és időben egyaránt korlátozzák a nemzetközi polgári légi forgalom célállomások közötti optimális áramlását.



2. ábra Légiforgalmi sűrűség (repülési óra/km^2) az európai repüléstájékoztató körzetekben [3]

A fenti kritikák markáns jelenléte három befolyásos légitársasági szövetség által 2013 nyarán közétett állásfoglalásban is tetten érhető, ahol a légtérfelhasználók egyértelműen jelezték, költségeikben közel 4 mrd EUR többletkiadás keletkezik az európai léginavigációs infrastruktúrához kapcsolhatóan (2 mrd EUR késés, 1,2 mrd EUR a többlet-útvonal és 0,6 mrd EUR a léginavigációs szolgáltatási díjak) [17].

Ráadásul jövőképük szerint az európai légtérben a jelenlegi évi ~10millió ellenőrzött (légiforgalmi irányítói szolgáltatásban részesülő) repülés biztonságos végrehajtásáért felelős 63 irányító központ helyett elegendő lenne (a tíz-húsz éven belül prognosztizált ~20milliós forgalom mellett is) legfeljebb 40 irányító központ jelenléte (állításukat nagyobb nyomatékot adva az Amerikai Egyesült Államok 20 irányító központját említették összehasonlításként, mely összevetés több szempontból sem tekinthető teljes körűen megalapozottnak) [17].

A fenti dokumentum szerint a légitársaságok további javaslata, hogy a csökkentett központszámot továbbra is a jelenlegi kb. 16 700 légiforgalmi irányítói létszám fenntartása mellett vizionálják, [17] álláspontom szerint a további markáns üzeneteket hordozza magában:

1. a légitársaságok drasztikus léptékű optimalizációjából hiányzik az a technológiai előrelépés, amely valóban lehetővé tenné egy kevésbé töredezett légtérstruktúrában a kétszeres légiforgalom kezelését, ezért továbbra is az egy légiforgalmi irányító/irányítói szektor kapacitásértékből építik fel a jövő európai légtérszerkezetét, infrastruktúráját;

[7] Air Navigation Service Providers
[8] SUA - Special Use of Airspace - ideiglenesen elkülönített/korlátozott légtér

2. a vízió egy olyan üzenetet is hordoz a légiforgalmi irányítói szakszervezetek irányába, mellyel a légitársaságok elkerülhetik az állásfoglalás okán esetleg kirobbanó légiforgalmi irányítói sztrájkot, amely gyakorlatilag azonnal visszahatna a légitársaságok működésére, pénzügyi eredményességére;
3. a légitársaságok a légiforgalmi rendszerek üzemeltetői állományának 40 300 főről 26 720 főre történő létszámcsökkentését [17] vizionálásával szintén utalnak az integráció és az infrastruktúra-reform szükségességére.

A légtérfelhasználók ilyen formában először nyíltan kimondott központ-csökkentési elképzelései összhangban vannak az Európai Bizottság SES koncepciójának részét képező ún. funkcionális légtérblokk (FAB[9]) elgondolással, miszerint a FAB az *„a működési követelményeken alapuló, az államhatároktól függetlenül kialakított légtérblokk, ahol a léginavigációs szolgálatok és a kapcsolódó tevékenységek teljesítményalapúak és optimalizáltak, annak érdekében, hogy valamennyi funkcionális légtérblokkban a léginavigációs szolgáltatók között fokozott együttműködés vagy adott esetben egy integrált szolgáltató jöjjön létre.”* [18][19].

3. ábra Az Európa légterét kilenc részre felosztó FAB struktúra és a Közép-európai Funkcionális Légtérblokk (FAB CE[10]) tagjai (készítette: a szerző)

A FAB koncepció és az említett jogszabályi kötelezettség alapján Európa légtere kilenc részre került feloszlásra, ahol a fenti meghatározás értelmében az együttműködő államok, nemzeti felügyeleti hatóságaik és a léginavigációs szolgáltatók – a nemzetek katonai szereplőivel közösen – igyekeznek megfelelni a bizottsági elvárásoknak [20].

A fentiek alapján tehát megállapítható, hogy a felhasználók mellett a jogalkotó szándéka is egyértelműen az optimalizáció, így a törekvések a jelenlegi nemzetenkénti léginavigációs szolgáltatás (irányító központok) számának csökkentése irányába mutatnak. Fontos azonban hangsúlyozni, hogy a tagállamok és a szolgáltatók a FAB együttműködési kereteken belül önállóan határozhatták meg az együttműködés formáját, illetve annak mélységét (*bottom-up approach*), így a skandináv együttműködés (NUAC[11]) kivételével nyolc FAB a léginavigációs szolgáltatók közötti fokozottabb együttműködés megvalósítását választotta az integráció helyett. A NUAC vonatkozásában azonban fontos kihangsúlyozni, hogy a dán és svéd léginavigációs szolgáltatók egyesülésével létrejött új irányító szervezetben továbbra is az

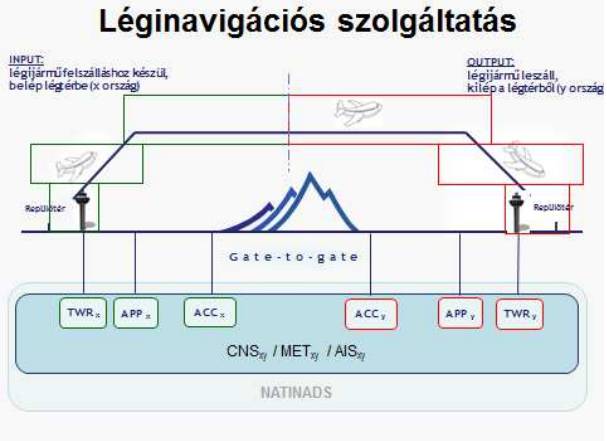
[9] FAB – Funcional Airspace Block
[10] FAB CE – Funcional Airspace Block Central Europe
[11] NUAC – Nordic Unified Air Traffic Control.

eredetileg működő (egy dán és két svéd) irányító központok jelenleg is ugyanabban a légtér-megosztási struktúrában végzik a légiforgalmi irányítási feladatokat, mint előzőleg.

Szintén megemlítendő, hogy az Európai Bizottság a FAB-ok megvalósításának 2012. december 4-re tervezett bevezetési határidejekor csak NUAC és a NEFAB[12] blokkokat ismerte el a jogszabályi kötelezettségek függvényében, majd később, 2015 nyarán a felmutatott eredmények alapján (a DANUBE FAB vonatkozásában) megszüntette a román és bolgár állammal szemben megindított kötelezettségszegési eljárást. A maradék hat FAB esetében viszont továbbra is fennáll a Bizottság azon kifogása, miszerint a kialakított környezet nem felel meg a jogszabályi követelményeknek, mert a felek nem tettek elég lépést az optimalizáció, de különösen az integráció érdekében. A legtöbb érintett uniós nemzet fő érvelése viszont, hogy a jogszabályi környezet kellően tág kereteket biztosított az együttműködési forma megválasztására, így megalapozatlan a Bizottság kritikája, hivatkozása.

A LÉGIFORGALMI IRÁNYÍTÓI SZOLGÁLTATÁS ÁLTALÁNOS JOGI HÁTTERE ÉS DELEGÁLÁSÁNAK ELVI LEHETŐSÉGEI

Az európai teher és személyszállításban résztvevő napi 27 000 légijármű ellenőrzött mozgásához [21] kötelező légiforgalmi (repülésirányítói) szolgáltatást nyújtani. Az ICAO alapokmánya [22] szerint az adott országot megillető szuverenitás joga alapján a tagállamok önmaguk szabályozzák és biztosítják a nemzeti léginavigációs szolgáltatást a repülés minden fázisában (felszállás-útvonali repülés-leszállás). Fontos szempont, hogy az adott légtérben, egy időben mindig csak egy felelős irányítói egység működhet.



Jelmagyarázat

ANSP	léginavigációs szolgáltató
TWRxy	x és y országok ANSP-i által működtetett repülőtéri irányító torony szolgálatok
APPx	x és y ország ANSP-i által működtetett közelkörzeti irányító szolgálatok
ACCxy	x és y ország ANSP-i által működtetett körzeti irányító szolgálatok
CNS xy	x és y ország ANSP-i által működtetett kommunikációs, navigációs és felderítési szolgáltatások
MET xy	x és y ország ANSP-i által működtetett meteorológiai szolgáltatások
AIS xy	x és y ország ANSP-i által működtetett légiforgalmi tájékoztatási szolgáltatások

4. ábra Az ellenőrzött légi forgalmat kiszolgáló légiforgalmi szolgálati egységek általános szemléltetése (készítette: a szerző)

Ahogy a nemzetközi környezetben, úgy hazánk vonatkozásában is jogszabályban rögzített a magyar légtér légiközlekedés céljára történő kijelölése, [23] illetve annak alkalmazási főszabályai, [24] továbbá az ATS felelőse – a légiközlekedésről szóló 1995. évi XCVII. törvény 61. § szerint a HungaroControl Magyar Légiforgalmi Szolgálat Zrt. biztosítja a légiközlekedés biztonsága érdekében a magyar légtérben légiforgalmi szolgálatok fenntartását, így az 5. ábrán is szerepeltetett ún. ATS szervezeti egységeit (TWR, APP, ACC)[13].

[12] NEFAB – North European Functional Airspace Block
[13] TWR – Tower control, APP – Approach control; ACC – Area Control

A Társaság feladatai között szerepel az adatszolgáltatás is a Magyar Honvédség erre kijelölt szervezete részére a nemzeti és szövetségi légtérellenőrzéshez [25] és légtérfelügyelethez szükséges azonosítás elősegítése érdekében, továbbá a (NATO elvárásokon[14] is alapuló és az állami célú repüléseket is kiszolgáló) légtérgazdálkodás, illetve a stratégiai légtér-gazdálkodási feladatokban való közreműködés is.

A léginavigációs szolgáltatók között eddig elsődlegesen az alaprendeltetésszerű (operatív) működés hatékonysága érdekében születtek kezdeményezések és megoldások az delegált irányítói környezet kialakítására, szemben a Bizottság szándékával, mely – megítélésem szerint – ugyan kihangsúlyozza a működési hatékonyság növelését, de az inkább politikai és pénzügyi-gazdasági indíttatású, mintsem hogy a két egymással szomszédos irányító egység kapacitás-optimalizálásának fokozását célozza.

A LÉGIFORGALMI IRÁNYÍTÓI SZOLGÁLTATÁS DELEGÁLÁSÁNAK MEGOLDÁSI LEHETŐSÉGEI

Az európai környezetben a különböző légiforgalmi szolgáltatásoknak és az általuk viselt felelősség átadására/delegálására több megoldási lehetőség is mutatkozik. A továbbiakban ezek elvi, vagy már meglévő formáját, illetve példáját mutatom be.

ATS delegáció és integráció vertikális megosztás szerint, szomszédos irányítói egységek között

Belgium, Luxemburg, Hollandia és északnyugat-Németország magaslégterében[15] az EUROCONTROL által létrehozott MUAC[16] biztosítja a szolgáltatást, míg a nevezett országok alacsonyabb légtérrészében a felelősség megmaradt a nemzeti szolgáltatók felelősségi körében [26].

Vertikális és horizontális légtérmegosztás szomszédos irányítói egységek között

A Bosznia-Hercegovina légterében 1995 óta fennálló helyzet feloldására az ICAO[17] is tett ajánlásokat, [27] majd 2014. november 13-án az újonnan megalakult nemzeti léginavigációs szolgáltató (BHANSA[18]) első lépésként átvette a légi forgalom irányítását a FL100-FL325 közötti magasságtartományban, az a feletti (FL325-FL660) légtérrészben egyelőre továbbra is a Szerbia és montenegrói (SMATSA[19]), valamint a horvát (CCL[20]) körzeti légiforgalmi irányító szolgálatok tevékenykednek [28].

Vertikális megosztású ATS delegáció nem szomszédos irányító egységek között

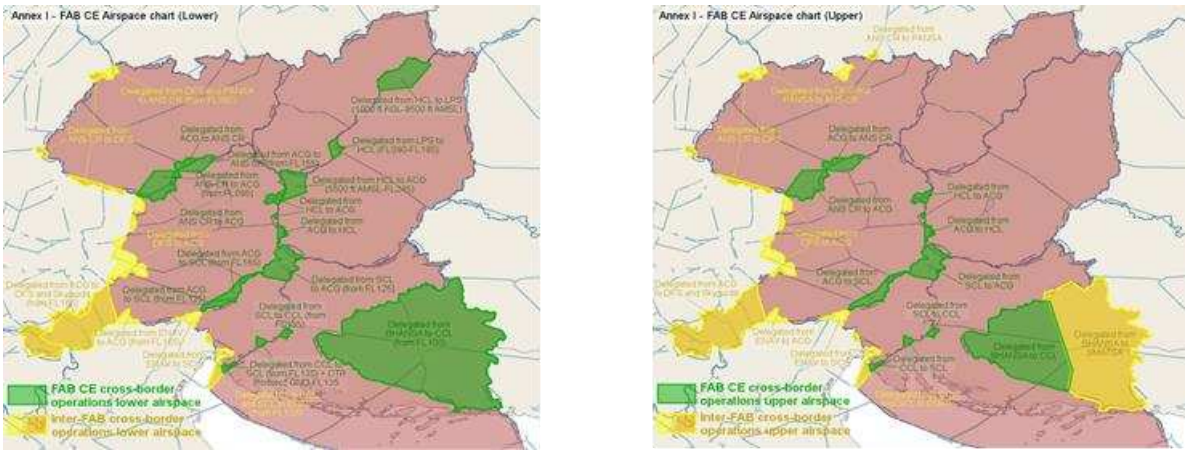
A balkáni légtér normalizációját több mint tizenöt éve tervezik a nemzetközi szakmai és politikai szervezetek. A térség politikai és gazdasági stabilizációjának keretében a polgári légiközlekedés reformjait is tervezték, [29] melynek részeként 2014 áprilisában (a NATO, az EUROCONTROL, az érintett szomszédos országok és szolgáltatóik, továbbá Magyarország részvételével) megnyílt a Koszovó feletti magaslégtér (FL205-FL660 repülési szint között). A kialakított konstrukció egyedülálló a maga nemében, ugyanis a NATO által 2001 óta

[14] NATO – AJP 3.3.5 Allied Joint Doctrine for Airspace Control
[15] FL245-FL660 repülési szintek (Flight Level) közötti magasságtartomány
[16] MUAC – Mastricht Upper Area Control Centre
[17] ICAO – International Civil Aviation Organisation
[18] BHANSA – Bosnia and Herzegovina Air Navigation Services Agency
[19] SMATSA – Serbia and Montenegro Air Traffic Services
[20] CCL – Croatia Control Ltd

fenntartott repülési tilalmi zónát 2014 áprilisában feloldották, és az újranyitott légtérben – a helyi nemzeti vagy szomszédos szolgáltatóval ellentétben – a HungaroControl Magyar Légiforgalmi Szolgálat Zrt. biztosítja a körzeti irányítói feladatokat [30]. Az alacsonyabb szomszédos légtérben a pristinai léginavigációs szolgáltató tevékenykedik, a térségben a repülés szabályait a NATO külön dokumentumban szabályozta [31].

Horizontális ATS delegáció a légtér adott részében, szomszédos irányító egységek között

Ennek egyik példája az uniós kötelezettség alapján, nemzetközi megállapodással [32] létrejött Közép-európai Funkcionális Légtérblokk (FAB CE), ahol a légiforgalmi irányítói szolgáltatást továbbra is ugyanaz a hét állami tulajdonú nemzeti szolgáltató biztosítja. A nemzeti légterekben egyelőre továbbra is a korábbi – a tagnemzetek által kijelölt – szoláltatók felelősek a szolgáltatás nyújtásáért, de amint az a FAB CE uniós tagállamaival szemben indított kötelezettségszegési eljárásban, 2014. novemberben a Bizottságnak megküldött hivatalos válaszlevélben is szerepel, a működési optimalizáció részeként a FAB CE légtér ~15%-ában a légiforgalmi irányítási szolgáltatás már nem országhatár-függő, mert a felelősség már delegálásra került a vele szomszédos léginavigációs szolgáltató részére.



5. ábra A FAB CE együttműködés delegált légtérrészei (alacsony és magas légtér) [33]

Közelkörzeti irányítás országhatáron átnyúló kiterjesztése

Hazánk vonatkozásában a nemzeti légtér két részében külön légterek kerültek kijelölésre a kassai és a bécsi induló/érkező forgalom hatékonyabb kezelésére. Ezekben a légterekben a szlovák és osztrák közelkörzeti légiforgalmi irányítói egységek kiterjedtebb légtérben képesek feladataik ellátására. Fontos megemlíteni, hogy a bécsi forgalom hatékonyabb kezelését támogató magyarországi (ún. LESMO) légtérrész szomszédos az MH Pápa Bázisrepülőtér katonai közelkörzeti légterével, aminek okán elengedhetetlen volt az osztrák polgári és a magyar katonai légiforgalmi szolgálatok közötti együttműködési eljárások kialakítása, illetve a bázisrepülőtér jövőbeni fejlesztései [34] esetén is az érintett (magyar és osztrák polgári és a magyar katonai) felek között a koordináció további folytatása.

Repülőtéri légiforgalmi irányítói szolgáltatás delegálása

A német léginavigációs szolgáltató (DFS[21]) az elnyert közbeszerzési pályázattal 2015. évtől tíz éven biztosítja a Gatwick Nemzetközi Repülőtér irányítói szolgáltatását, melyet korábban a brit NATS szolgáltató nyújtott. [35] A szolgáltatás delegálásának elvi lehetőségét jelentős mértékben növelheti majd az a jelenleg fejlesztés alatt álló ún. távoli (remote) TWR

[21] DFS - Deutsche Flugsicherung

technológia, mellyel a repülőtéri irányítói szolgáltatás nem feltétlenül a repülőtéren vagy közvetlen környezetében felépített irányító toronyból, hanem bármilyen más kitelepített (távoli) környezetből lenne biztosított. A technológiai innováció első alkalmazására Svédországban került sor, [36] azonban a számos kiaknázatlan fejlesztési terület kutatásának és megvalósításának egyik úttörője a HungaroControl Magyar Légiforgalmi Szolgálat is, amely a Liszt Ferenc Nemzetközi Repülőtéren tervezi 2017-től a helyszíntől független, repülőtéri légiforgalmi irányítást biztosító ún. „virtuális" torony működtetését. [37] A Társaság – egy négytagú konzorcium tagjaként – részt vett a Dubai Nemzetközi repülőtérre szánt tartalék irányítótorony terveinek elkészítésében is, mely terv a magyar remote TWR elgondolás alapjaira épült.

Országhatáron átnyúló katonai légtér megosztott légvédelmi irányítói felelősséggel

A FABEC együttműködés[22] keretében indított South-East projekt [38][39] keretében kerülnek kialakításra azok a francia-svájci és német-francia országhatárokon átnyúló katonai légterek, amelyekben az irányítói felelősség – a légtér aktív működésekor – a légteret igénybe vevő valamely nemzeti légvédelmi irányítói szolgálathoz kerül delegálásra.

Eseti légtér kijelölése távoli légvédelmi irányítói szolgáltatással

Az ENSZ Biztonsági Tanácsának 2011. március 17-én hozott 1973. számú határozata alapján Líbia felett Repüléstilalmi Zónát (NFZ[23]) rendeltek el, és a térségben folytatott NATO légi műveletek a Málta FIR-re is jelentős hatást gyakoroltak [40]. A szövetségi feladatokhoz szükséges légtérfelhasználás a szövetségi műveleti légtér-gazdálkodási elvek szerint történt[24]. A műveletek idejére eseti jelleggel kijelölt légterekben végrehajtott műveleti repülési feladatokat légtérellenőrző repülőgépekről, korai előrejelző rendszerekről vezették, irányították.

ÖSSZEGZÉS

A fenti csoportosítás alapján megállapítható, hogy a szolgáltatás delegálása elsődlegesen egymással szomszédos légiforgalmi szolgáltatók között valósult meg, és kifejezetten a kapacitás és/vagy a polgári (katonai) műveleti hatékonyság javítását célozzák.

Mivel a szolgáltatás delegálása (tágabb dimenzióban, akár nem szomszédos légiforgalmi szolgálatok között is) katalizátorai az európai léginavigációs szolgáltatói környezet átalakulásának, és a légtér töredezettség-mentesítésén keresztül felgyorsítják a nemzeti léginavigációs szolgáltatók közötti versenyhelyzet kialakulását, ezért fontos felkészülni – a szabályozási környezet változásai eredményeként – már nem csak szakmai, de piaci alapon nyugvó szolgáltatások megjelenésére.

A felkészülés során kiemelt figyelmet kell szánni az iparági technológiai fejlődéssel megjelenő, a nem szomszédos szolgáltatók közötti szolgáltatás-delegálás aspektusaira, különösen a légtérnek, mint kritikus infrastruktúrának a védelmére, a légiforgalmi szolgáltatásban és a NATINADS keretében a honvédség és a Szövetség részére átadott információk biztonságára, illetve a nemzeti légtér ellenőrzése során a felek közötti együttműködés folyamataira.

A szolgáltatás delegálása minden esetben hatást gyakorol a nemzeti légvédelmi és légtérellenőrző, illetve a jogszabályban kijelölt nemzeti légiforgalmi szolgáltató szakmai

[22] Belgium, Luxemburg, Hollandia, Németország, Franciaország, Svájc, EUROCONTROL Maastricht Upper Area Control Centre (MUAC) együttműködésével megvalósuló funkcionális légtérblokk
[23] NFZ – No-fly Zone
[24] ATP 40 (C) Doctrine for airspace control in times of crisis and war

viszonyára. E kapcsolat változásait a fenti kategorizáláson keresztül külön vizsgálatokkal szükséges elemezni, annak érdekében, hogy teljes körű képet alkothassunk a légiforgalmi szolgáltatás részleges vagy teljes delegálásának (kiszervezésének):

- a béke- és minősített időszaki viszonyairól, lehetőségekről és korlátairól, illetve
- a legszükségesebb nemzeti és szövetségi feltételrendszeréről.

A kérdések megválaszolásához további részletes vizsgálatok szükségesek annak vonatkozásában is, hogy a polgári légiközlekedési szektorban alkalmazott (vagy tervezett) szolgáltatás-delegálások vajon átültethetők-e a NATO légiforgalom-szervezési rendszerébe, és a távoli irányítást biztosító technológiák alkalmazhatóak-e a NATO műveleti térségeiben.

Felhasznált irodalom

[1] Economic Growth: Aviation benefits. http://aviationbenefits.org/economic-growth (2015. november 2.)

[2] IATA: *Annual Review 2015.*(http://www.iata.org/about/Documents/iata-annual-review-2015.pdf (2015. november 2.)

[3] FAA-European Commission-EUROCONTROL: *Comparison of Air Traffic Management related operational performance: U.S./Europe.*

[4] C. Gresnigt: Addressing European airspace fragmentation. *Skyway*, 9 38 (2005), 26–27.

[5] D. Learmount: European air traffic congestion 'world's worst', says IATA. *Flight International*. Number 4164, Volume 135. ISSN 0015-3710. (1989), 6.

[6] C. L. Wu, R. Caves: The punctuality performance of aircraft rotations in a network of airports. *Transportation planning and technology* 26, 5, (2003), 417–436.

[7] W. Schwenk – R. Schwenk: Aspects of International Co-operation in Air Traffic Management. *Kluwer Law International, The Hague* (1998), 310.

[8] M.S. Nolan: Fundamentals of air traffic control. *Thomson Learning High Holborn House*, *London* (2004), 560.

[9] Moys P.: *Nemzetközi Légijog*. 3,14 L Nyomdaipari és Szolgáltató Kft., Budapest (2006), 341.

[10] Mudra I.: *3-L: légterek, légiforgalmi szabályok, légiforgalmi szolgálatok*. HungaroControl, Budapest (2008), 261.

[11] Orlóczi Zs.: Egységes légtér az egységes európai piac felett. *Közlekedéstudományi Szemle*, Budapest LVI. évf. 4. sz. (2006), 149-153.

[12] Sztrunga E.: A légiközlekedés útvonalhatékonyságának fejlesztése az európai légtérben. PhD értekezés. Pécs, PTE. 2015

[13] Kovács L.: Légiforgalom-szervezés a Magyar Honvédségben, tanulmány, NKE HHK, 2012

[14] Palik M. - Vajda A.: Polgári-katonai együttműködés a légiforgalmi szakszemélyzetek képzésében, Repüléstudományi Közlemények 2008 (1), Szolnok, 15-24., *Repüléstudományi Konferencia 2008: 70 éves a légierő,* http://www.repulestudomany.hu/kulonszamok/2008_cikkek/Vajda_Andras_Palik_Matyas.pdf (2015.10.20.)

[15] EUROCONTROL: *Seven year forecast September 2015* (Edition:15/09/04-48)

[16] ICAO: *Member states Europe*. http://www.icao.int/EURNAT/Pages/member_states.aspx (2015.06.25.)

[17] IATA-AEA-ERA: *A Blueprint for the Single European Sky*. https://www.iata.org/pressroom/pr/Documents/blueprint-single-european-sky.pdf (2015. 10. 20.)

[18] *Az Európai Parlament és a Tanács 551/2004/EK rendelete (2004. március 10.) a légtérnek az egységes európai égbolt keretében történő szervezéséről és használatáról.*

[19] *Az Európai Parlament és a Tanács 1070/2009/EK rendelete (2009. október 21.) az 549/2004/EK, az 550/2004/EK, az 551/2004/EK és az 552/2004/EK rendeletnek az európai légiközlekedési rendszer teljesítményének és fenntarthatóságának javítását célzó módosításáról.*

[20] Somosi V.: Az európai légtérszerkezet racionalizációja – a FAB CE Program és a magyar állami célú légiközlekedés kapcsolata. *Repüléstudományi Közlemények*, 2 (2009), (Különszám: Repüléstudományi Konferencia 2009. 50 év hangsebesség felett a magyar légtérben.) www.repulestudomany.hu/kulonszamok/2009_cikkek/Somosi_Vilmos.pdf (2015. 10. 20.)

[21] EUROCONTOL: *About the Network Manager.* http://www.eurocontrol.int/articles/about-network-manager (2015.11.19.)

[22] *A nemzetközi polgári repülésről Chicagóban, az 1944. évi december hó 7. napján aláírt Egyezmény és az annak módosításáról szóló jegyzőkönyvek kihirdetéséről szóló 1971. évi 25. törvényerejű rendelet.*

[23] *A magyar légtér légiközlekedés céljára történő kijelöléséről szóló 26/2007. (III.1.) GKM-HM-KvVM együttes rendelet.*

[24] *A magyar légtér igénybevételéről szóló 4/1998. (I. 16.) Kormányrendelet.*

[25] Pék T.: A NATO csatlakozás hatása a Magyar Honvédség légtérellenőrző, valamint a légivezetési és irányítási rendszerére. Budapest, NKE HHK, 2013.

[26] Mastricht Upper Area Control Centre (MUAC): As the crow flies, Free Route Airspace Maastricht. *EUROCONTROL*, March 2011. https://www.eurocontrol.int/sites/default/files/article/files/2011march-free-route-airspace-maastricht.pdf (2011.03.20.)

[27] European and North Atlantic Office: *Transfer of Bosnia and Herzegovina airspace control*. International Civil Avaiation Organization (ICAO). 2007 http://www.icao.int/EURNAT/News%20Archives/2007/20070420-Transfer%20of%20Bosnia%20and%20Herzegovina%20Airspace%20Control.pdf (2011.03.20.)

[28] Bill Carey: Bosnia Herzegovina Says It Can Manage Its Own Airspace. *Ainonline.* 8 January 2015. http://www.ainonline.com/aviation-news/air-transport/2015-01-08/bosnia-herzegovina-says-it-can-manage-its-own-airspace (2015.11.17.)

[29] Office for South East Europe: *The European Common Aviation Area and the Western Balkans: Domestic Reforms and Regional Integration in Air Transport.* European Commission, World Bank, 2007 http://ec.europa.eu/transport/modes/air/studies/doc/international_aviation/2007_02_09_see_air_transport_en.pdf (2015.10.10.)

[30] A NATO/KFOR ismét megnyitotta a Koszovó feletti magas légteret a polgári átrepülő légi forgalom előtt. *HungaroControl*. http://www.hungarocontrol.hu/download/990cb90561052e9207beb0fd574ed7b4.pdf (2015.10.11.)

[31] *NATO CAOC TJ - Regulations for aircraft operating as general air traffic (GAT) in the Balkans (14 November 2014)* http://www.aco.nato.int/resources/site7423/general/documents/balkans%20unclas%20spins%20ver%203_0.pdf (2015.10.10.)

[32] *Közép-európai Funkcionális Légtérblokk létrehozásáról szóló Megállapodás kihirdetéséről szóló 2011. évi LXV. törvény*

[33] *A Magyar Kormány 2014. november 06-i válasza a Bizottság kötelezettségszegési eljárásban érkezett hivatalos felszólítására*

[34] Bódai Miklós: Az állami repülések célját szolgáló repülőtér (Pápa) továbbfejlesztésének kihívásai a légiforgalom szervezés (ATM) tekintetében. Diplomamunka. NKE, 2014

[35] DFS subsidiary to take over tower services at London Gatwick. DFS. 18 July 2014. https://www.dfs.de/dfs_homepage/en/Press/Press%20releases/2014/18.07.2014.-%20DFS%20subsidiary%20to%20take%20over%20tower%20services%20at%20London%20Gatwick/ (2015. 10. 11.)

[36] Sweden first in the world with remotely operated air traffic management. *LFV*. 21 April 2015. http://www.lfv.se/en/News/News-2015/Sweden-first-in-the-world-with-remotely-operated-air-traffic-management/ (2015.08.20.)

[37] Startol a magyar „virtuális" torony megvalósítása. HungaroControl. http://www.hungarocontrol.hu/sajtoszoba/hirek/startol-a-virtualis-torony (2015.11.02.)

[38] http://www.fabec.eu/fabec_homepage/en/Projects/South%20East/E-fabec-south-east-project-web.pdf

[39] http://www.lw.admin.ch/internet/luftwaffe/fr/home/themen/cba.html

[40] Amiee Turner: Libyan conflict put Malta's ATC to the test. *Air Traffic Management*. 30 April 2012 http://www.airtrafficmanagement.net/2012/04/malta/ (2015.11.03.)

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Csősz László
csosz.laszlo@uni-nke.hu

FELSZÍNI VIZEK KŐOLAJSZENNYEZÉSEINEK VIZSGÁLATA

Absztrakt

Földünk jelentős részét alkotják, nyílt tengerek és óceánok. A tengerek mindig is fontos szerepet töltöttek be a kereskedelemben és a szállításban, amelynek következtében számtalanszor ártalmas és veszélyes anyagok kerültek a nyílt vizekbe. Továbbá a XX. században bekövetkezett technológiai fejlődés következtében a gáz és a kőolaj-kitermelés egyre jelentősebb szerephez jutott a nyílt vizeken. A hatalmas víztömegek láttán azt gondolhatnánk, tetteinkkel úgysem tudunk kárt okozni bennük. Ez azonban korántsem igaz, a tengerek olajjal történő elszennyezése partvidékeket pusztít el, egész tengeri madárkolóniákat írt ki, kioltja az életet a tengerekben. Az olajszennyezés hatalmas károkat tud okozni. Sajnos mindig fennáll a veszélye, hogy egy tankhajó zátonyra fut vagy egy olajfúrótorony megsérül vagy éppen megsemmisül. Egy-egy ilyen baleset alkalmával rengeteg olaj ömlik egyszerre a tengerbe, hatalmas ökológiai katasztrófát okozva ezzel. A tengerek mellett a folyók is hasonló veszélyeknek vannak kitéve. Hazánkban például a Duna és a Tisza gyakran esik áldozatul a különböző olajszennyezéseknek, egyrészt uszálybalesetek következtében, másrészt a hajók illegálisan a folyóba ürített fenékvize miatt, amely jelentős mértékű elhasznált olajat tartalmaz.

A significant portion of Earth, oceans and high seas. Seas have always played an important role in trade and transport, owing to which several times harmful and hazardous materials have ingresses into open waters. Further due to the technological development occurred in the 20th century gas and mineral oil production has received a more significant role on open waters. Seeing the huge water amounts we could think, we cannot harm them with our actions. However it is not true, the contamination of seas with oil destroys complete coasts, whole sea bird colonies are killed, and life is demolished in the seas. Oil contamination can cause huge damages. Unfortunately the risk always exists that a tanker runs aground or an oil derrick gets damaged or even destroyed. Upon such an accident enormous quantity of oil flows into the sea at once, causing huge ecological disaster. Beside seas rivers are also exposed to similar risks. In our country for example the rivers Danube and Tisza often fall a victim to different oil contaminations, on the one hand due to barge accidents, on the other hand due to the bilge-water of ships emptied illegally into the river, which contains significant amount of refuse oil.

Kulcsszavak: *olajszennyezések, olajszennyezések kárelhárítása, alternatívák ~ oil spills, remediation of oil spills, alternatives*

BEVEZETÉS

Az olaj jelenleg nélkülözhetetlen energiaforrás. Az iparosodott országok gazdasága összeomlana olaj nélkül. Például Németország energiaszükségletének legnagyobb részét, 36,7%-át az olaj fedezi, a maradék részt pedig szén (25%), földgáz (22,2%), és atomenergia (12,5%) teszi ki [1]. Az olaj közel fele a közlekedésben kerül elégetésre, egyharmadával fűtenek, és nagyjából egy hatodát a vegyipar használja fel. A német közlekedés 90%-ban az olajtól függ. Németország az USA, Kína, Japán és Oroszország mögött a világ 5. legnagyobb olajfogyasztója. Annak ellenére, hogy a 70-es évek olajválsága arra ösztönözte az ipart, hogy alternatív energiákra építsen, a háztartások és a közlekedés olajfelhasználása tovább növekedett, a függőség egy cseppet sem csökkent.

A gazdaságban jelen lévő veszélyes anyagok tárolása, feldolgozása és felhasználása magában hordozza a súlyos ipari balesetek kialakulásának kockázatát. Az élővizek olajos elszennyeződésének okozói gyakran a különböző hajóbalesetek, uszályok sérülései, szennyvíztisztítási hiányosságok, csővezetékes szénhidrogén-szállítással kapcsolatos problémák [2]. Hazánk nemzetközi szintű multinacionális olajtársasága a Magyar Olaj- és Gázipari Nyrt. (MOL). Annak ellenére, több olajszennyezés is érintette hazánkat, hogy MOL hosszú távú, stabil, fenntartható működésének egyik alappillére a felelős környezethasználat, így a működésével, illetve tevékenységével összefüggésben kialakuló környezeti terhelések, környezeti kockázatok minimalizálása az elérhető legjobb technológiák alkalmazásával valósul meg. Ezek leginkább szállítási balesetek, például uszálytöltések vagy éppen az olajvezetékek illetéktelen személyek haszonszerzés céljából elkövetett rongálása okán fordultak elő. Éppen ezért fontosnak tartom, hogy feltárjam a katasztrófa elhárítás, kárfelszámolás eszközeit, illetve alkalmazott módszereit. A kárfelszámolásból nyert tapasztalatok feldolgozásával lecsökkenthető a későbbiekben bekövetkező katasztrófák kárelhárítási idő intervalluma.

OLAJSZENNYEZÉS JELLEMZÉSE ÉLŐVÍZI KÖRNYEZETBEN

A szennyező anyagok, amelyek a felszíni vizeket szennyezik, egy sajátos csoportja azok az anyagok, melyek közvetett hatásúak. Ezen anyagok a vízbe kerülve a vízi élet tényezői közül a fizikai elemeket blokkolják, illetve kizárják. Tehát fizikai úton gátolják a légzést, elzárják a vizeket a fénytől, valamint az alacsonyabb rendű szervezetekben bevonatokat képeznek. A legismertebb és előfordulási arányát tekintve a rendkívüli szennyezések szennyező fajtái közül a leggyakrabban előforduló (37,4%) szennyező anyagok a kőolaj és annak származékai, gyűjtő néven a szénhidrogének [3]. Az olaj Földünk szilárd kérgében fellelhető természetes eredetű, élő szervezetek bomlásával, átalakulásával létrejövő ásványi anyag. Főbb alkotói a folyékony halmazállapotú szénhidrogének, de lelőhelyükön, azok földrajzi helyzetétől függően oldatban, nyomás alatt gáznemű, valamint szilárd halmazállapotú szénhidrogéneket is tartalmazhatnak kisebb-nagyobb mennyiségben. A felszínivizekhez kapcsolódó olajszennyezéseknek minden formája egyaránt káros hatású. A vízfelszínen úszó olajréteg megakadályozza a vizek természetes oxigénforgalmát és ezzel a légzésre és a fotoszintézisre is egyaránt káros hatást fejt ki. Az olaj már egészen kis mennyiségben elzárja a víz felszínét, és ezáltal gátolja mind a természetes oxigén felvételét a légkörből, mind pedig a képződő gáznemű anyagcsere termék távozását a légkörbe. A vízbe kerülő olaj, ha nem ütközik akadályba, gyorsan szétterül és vékony filmszerű réteget alkot, létrejön az olajfedettség, ami 1

mm vastagságú. Tiszta vízben ez a fedettség terjed és fokozatosan 0,2 mm-nél alacsonyabb hártyává alakul. A szennyezett víz akadályozhatja az olajhártya szétterülését, de ebben az esetben is 1 mm körül marad a rétegvastagság.

Az olaj vízbekerülésekor nyolc különböző folyamattal kell számolni [4]: a szétterüléssel, a párolgással, a diszperzióval, az emulzifikációval, az oldódással, az oxidációval, az ülepedéssel, illetve a biodegradációval.

- Szétterülés: A kiömlést követően az olaj szétterül a vízfelszínén – a szétterülés gyorsaságát alapvetően az adott olaj viszkozitása szabja meg. A kiterülő olajfolt vastagsága természetesen mindenhol nem lehet uniform, egyforma, mivel a távol eső területekre csak foszlányokban ér el az olaj. A kiterülést megszabó környezeti tényezők: szélsebesség, vízhőmérséklet és a hullámzás.
- Párolgás: Sebessége az olaj gőznyomásának függvénye. Így például a petróleum, kerozin és dízel olajok csaknem teljesen elpárolognak néhány nap alatt a vízfelszínről. Erős hullámzás és szél, illetve magasabb hőmérséklet erősíti a párolgást.
- Diszperzió: A hullámok és a vízfelszín turbulenciája az olajpaplant aprítja, diszpergálja egymástól független kisebb cseppekre. A kisebb cseppek szuszpenzióban maradnak (O/V) míg a nagyobbak (fajsúlykülönbség) újra a felszínre emelkednek. A diszperzió sebességét alapvetően az olajfajta és a víz állapota (hullámzás, szélsebesség) határozza meg. A leggyorsabb a diszperzió erős hullámzás és alacsony viszkozitású, könnyű olajok esetében.
- Emulzifikáció: Az emulzió két folyadék elegyedésekor jön létre. A nyersolajok esetében a vízcseppek szuszpendálódnak az olajban, ennek eredménye egy nagyon viszkózus anyag képződése, amit olajgöbecsnek, vagy „olajcsokinak” neveznek. Az emulziók újra olajakat alkothatnak pl. napfény hatására (reverzibilis emulzifikáció), amelyek majd újra „olajcsokivá” alakulhatnak a parti zónákban.
- Oldódás: Az olaj vízoldékony komponenseit oldja a víz. Ez a folyamat az adott olajfajta összetételétől és állapotától egyaránt függ, ám leggyorsabban akkor megy végbe, ha az olaj finom diszperzióban szétárad a víz vertikális, illetve függőleges rétegeiben. A leginkább oldódó összetevők a könnyű, aromás szénhidrogének, mint például a benzol, valamint a toluol. Ezek szintén könnyen párolognak, amely folyamat körülbelül 10-100x gyorsabb folyamat az oldódásnál. A beoldódott vegyületek között rendkívül sok a rákkeltő anyag.
- Oxidáció: Az olaj az oxigénnel reagálva oldható komponensekre bomlik. Ezt a folyamatot a napfény is elősegíti (függően a környezeti körülményektől: hullámzás, diszpergáltság foka). Ez rendkívül lassú folyamat, és még erős napfényben is a vékony olajfilmeknek csak körülbelül 0.1%-a bomlik le naponként.
- Ülepedés: Bizonyos finomított nehézolajok nehezebbek a víznél, ezért lesüllyednek (a legtöbb nehézolaj azonban nem süllyed le). A lesüllyedés többnyire akkor történik, amikor lebegőanyag és üledékszemcsék épülnek be az olajba. A partra került olaj keveredve a homokkal és üledékkel visszamosódva a vízbe (hullámzás, áradás) szintén lesüllyed.
- Biodegradáció: A felszíni vizek mindig tartalmaznak olyan mikroorganizmusokat, amelyek részlegesen vagy teljesen képesek az olaj vízoldékony komponenseit lebontani. Bizonyos vegyületek azonban biológiailag bonthatatlanok. A biodegradációt befolyásoló főbb tényezők: a tápanyagok (nitrogén és foszfor), hőmérséklet és oldott oxigén. A biodegradáció oxigénigénye miatt a folyamat csak az olaj-víz határfelületen megy végbe, mivel az olajban nincs oldott oxigén.

A terjedés, evaporáció, diszperzió, emulzifikáció és oldódás folyamatai elsősorban a kiömlést követő rövid időszakban játszanak fő szerepet. Az oxidáció, ülepedés és biodegradáció folyamatai inkább hosszabb távon jelentenek hatást az olaj végső, további sorsára.

AZ OLAJSZENNYEZÉSEK KÁRELHÁRÍTÁSA

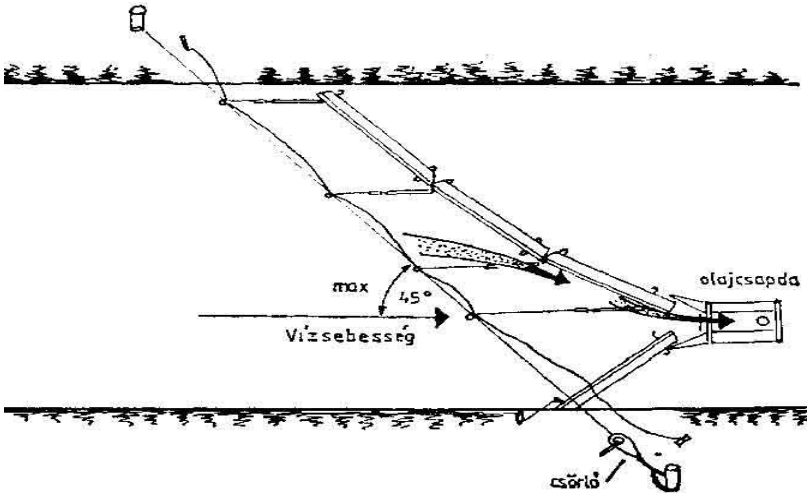
Az olaj okozta vízszennyezés esetén a védekezési műveletek általában három részből állnak [5]:

- a szennyezés lokalizálása;
- a lokalizált szennyező anyag eltávolítása a vízfelszínről;
- a szennyező anyag biztonságos deponálása vagy megsemmisítése.

A szennyezés lokalizálásában alapvető fontossága van a védekezés helyének, módszerének és az eszközök megválasztásának. Az olajszennyezés lokalizálását szerte a világon ún. merülőfalas olajzárakkal, illetve az azt helyettesítő anyagokkal oldják meg. A merülőfalak egyébként olyan - a víz felszínén úszó - szerkezetek, amelyeknek egy része a víz felszíne fölött van, másik része pedig a vízfelszínhez közeli rétegbe nyúlik le. Ezek a merülőfalak azon az elven működnek, hogy a vízfelszín közelébe eső réteg lezárásával megakadályozható a felszínen úszó anyagok továbbhaladása.

A vízfelszínen az olaj szétterjedését kell megakadályozni, ezért a szennyezett területet körül kell határolni merülőfalakkal. A szennyezések lokalizálása kisebb vízfolyásokon és kis vízsebességek esetén a vízfolyás közelében fellelhető anyagokból készült egyszerűbb módszerekkel is megvalósítható, például rőzséből vagy nádból 3-4 m hosszú, úgynevezett „kolbászokat" készítenek és rögzítik a vízfolyásokon, vagy szalmabálákat összekötözve alakítanak ki egyszerű olajterelőket. Az olajszennyezések gyakoriságának vizsgálata azt bizonyította, hogy a nagyobb vízfolyásokat sokkal inkább fenyegeti az olajszennyezés. Célszerű tehát gondosan tervezett és előre gyártott berendezésekkel felkészülni, hogy szükség esetén a helyszínen szerelhessék össze.

Hazánkban az 1. ábrán bemutatott „T" típusú merülőfal terjedt el leginkább [6]. Ezek fából készülnek, fekvő T alakú elemekből állnak, amelyeket függőleges tengelyű, csuklós vasalások erősítenek össze. A merülőfal a vízfolyás fölött kifeszített kötélhez rögzíthető. Ez a típus legfeljebb 200 m szélességű vízfolyásokon, patakokon, csatornákon alkalmas olaj terelésére, a gyakorlati mérések szerint kb. 0,7 m/s vízsebességig. Nagyobb vízfolyásokon többlépcsős elrendezésben alkalmazhatók az elemek, egy-egy merülőfalegység 40—50 m-es hosszúságú, lépcsőzetes elrendezésével [7].



1. ábra: A „T" profilú merülőfal elhelyezése a vízfolyáson [6]

A vizek olajjal történő elszennyezésének esetében két fő típust különböztethetünk meg az egyik a szállítási balesetek csoportja a másik pedig a kitermeléshez köthető szennyezések csoportja. Számtalan szállítási baleset történt már az évek folyamán, gondoljunk csak az Exxon Valdez tankhajó balesetére [8]. 1989. március 24-én az Exxon Mobil hajózási vállalat Exxon Valdez nevű tankhajója zátonyra futott. Egy jéghegy észlelését követően nem hajtották végre időben az iránymódosítást, majd az utolsó pillanatban próbálva kikerülni azt, a hajó zátonyra futott. A baleset következtében 40 millió liternyi olaj szabadult ki a tankhajóból, súlyos ökológiai katasztrófát okozva. Ez a katasztrófa volt az első olyan nagymértékű következményekkel és káros hatásokkal járó esemény, amely után szükséges volt a tanulságok levonása a jövőbeni hasonló események megelőzése érdekében.

A kitermeléshez köthető szennyezések száma is igen jelentős. Az egyik legsúlyosabb ilyen eset a British Patrol (BP) olajtársaság Deepwater Horizon olajfúró tornyának a felrobbanása és elsüllyedése. A Mexikói-öbölben történt, az olajfúrótorony 1500 méteres mélységben bekövetkezett robbanásakor, több mint tízszer annyi olaj került a nyílt vízbe, mint az Exxon Valdez tankhajó balesetekor [9]. 2010. április 20-án több mint 700 millió liter olaj ömlött ki a nyílt vízbe.

A felszíni vizek olajszennyezésekor alkalmazható beavatkozási lehetőségek és technológiák [10]:

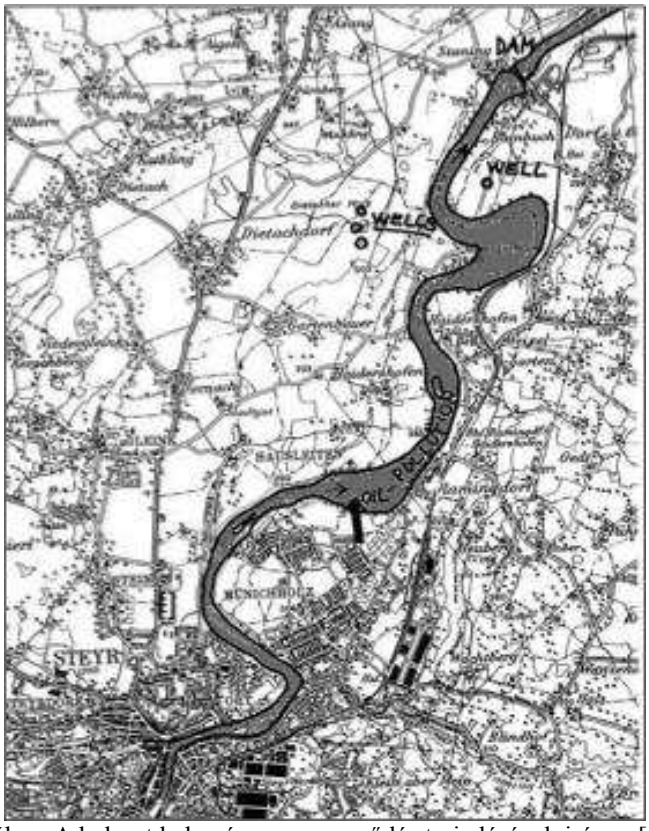
- detektálás és követés;
- merülőfal telepítése;
- lefölözés és összegyűjtés.

AZ ENNS FOLYÓ ELSZENNYEZÉSE

1998. május 31-én Ausztriában egy motorgyártó cég telephelyén található nagy, 1000 m3 kapacitású tárolótartály, amely fűtőrendszerhez használt diesel olajat (fűtőolajat) tartalmazott, szivárogni kezdett [11]. Az érintett telephely az Enns folyó partján található, amely folyó a Duna mellékfolyója Steyr városától délre. A Staning vízerőmű zárógátja ugyancsak az áramlás irányában található. Továbbá ugyanezen a területen, a folyó bal partján ivóvízállomás található kinyerő kutakkal annak közvetlen közelében, ami kb. 50 000 lakos számára biztosít ivóvizet.

A tartályt ellenőrző vizsgálatnak vetette alá az üzemeltető, a két fal közötti teret feltöltötték vízzel. Az ellenőrző vizsgálat során úgy tűnt, hogy a belső tartály, amely 700 m3 olajat tartalmazott, mentes az anomáliáktól. Az éjszaka során a tartály alján lévő szelep kinyílt és a vizsgálat során használt víz a folyó felé áramlott a burkolatok között lévő vízelvezető csövön.

Reggel halászok értesítették a rendőrséget, hogy az Enns folyó elszennyeződött. A szennyeződés nagy része a Staning gát által kialakított tóban volt fellelhető, így közel az ivóvizes kút területéhez, ahogy a 2. ábrán is látható. Három nap és három éjszaka a vízügyi hatóságok és a tűzoltóság szakemberei azon dolgoztak, hogy felfogják a szennyeződést. Lebegő gátakat alkalmaztak a szennyeződés felfogásához. A szennyeződés 35 km-re terjedt ki, érintve a területen belül elhelyezkedő 3 vízerőmű gátját. A baleset után 9 héttel az ivóvíz kutak jelentős szintű szénhidrogén szennyeződést mutattak. A szénhidrogén szennyeződés azonban rövid ideig tartott és alacsony koncentrációjú volt. Végül, a balesetet követő 6 hónapban számos a környéken lévő kút került kivizsgálásra.



2. ábra: A baleset helye és a szennyeződés terjedésének iránya [12]

A 3. ábra jól prezentálja, a tagállamok illetékes hatóságának bizottsága által 1994 februárjában hivatalossá tett mérleg 18 paraméterének besorolási szabályozását alkalmazva, ami a „SEVESO" irányvonal alkalmazását ellenőrzi, a baleset a következő 4 mutatóval jellemezhető, a rendelkezésre álló információk alapján:

3. ábra: Az ipari balesetek Európai skáláján ábrázolva az eset mértéke [12]

Az esemény összegzése

Az ellenőrző vizsgálat során senki nem észlelte a főtartály, tehát a szénhidrogéneket tartalmazó tartály alján lévő hegesztési varratszakaszon lévő repedést. Ennek eredményeként több mint 70 m3 olaj áramlott a folyóba a vízelvezető szelepen keresztül. Annak ellenére, hogy a kérdéses tárolótartály speciális kialakítású, bizonyos tanulságok levonhatóak a balesetből:

- az elfolyás jelenségét fokozta a külső tartály vizsgálata, mivel a szénhidrogénok szivárgásában az elfolyó víz közreműködött;
- az elvezetési műveletet a nap folyamán kell végrehajtani, hogy a lehetséges baleset megelőzhető vagy a helyszíni személyzet által ellenőrizhető legyen;
- a szerelvény kialakítása, közvetlenül a folyóba ürítő öblítéssel nem megfelelő.

A DAUGAVA FOLYÓ ELSZENNYEZÉSE

2007. március 23-án Lettország jelzést kapott Fehéroroszországtól, hogy az „Unecha-Venstpils" olajvezetékből szivárgás történt 130 km-re Lettország határától [13]. Fehéroroszország hivatalosan március 24-én, másnap tájékoztatta Lettországot az Ulla folyóba történt olaj kiömlésről, 17 órával azután, hogy a kiömlés megjelent és az olajréteg elkezdett lefelé áramlani a Daugava folyón. A Daugava folyó, Lettország legnagyobb folyójának fehérorosz mellékfolyója. A szivárgás Vitebsk területén (Észak-Fehéroroszország) következett be, közel az Ulla folyóhoz. A Daugava Lettország legnagyobb folyója, a Balti-tenger nyúlványa, ami keresztül folyik Rigán és az ország második legnagyobb városán, Daugavpils-en. A 377 mm olajvezeték repedése 5 órán keresztül kb. 120 tonna fűtőolaj kiömlését eredményezte az Ulla folyóba, azt követően pedig a Daugava folyóba. A tűzoltó egységek ahogy a 4. ábrán is látható úszógátakat alkalmaztak, hogy megakadályozzák az olajszennyezés továbbterjedését. A csővezeték tulajdonosa nem jelentette azonnal a hatóságoknak a kiömlést. A szennyeződés két országot, Fehéroroszország és Lettországot érintette. Továbbá a kb. 120 tonna fűtőolaj szivárgása elszennyezett 1,2 ha földet is a forráshelyen. Az olajréteg 100 km-re terült el, a folyó szélességének kb. 30%-át érintette a kiömlés. A tisztítási művelettel sikerült megelőzni jelentősebb hosszú távú sérülést.

A balesetért felelős olajcég 170.000,- €-t fizetett a sürgősségi intézkedések költségeiért és a környezet közvetlen károsításáért. Ugyanekkor néhány környezettudós úgy becsülte, hogy a baleset általános költségei Lettországban, beleértve a környezeti károkat, a környezetre gyakorolt közvetett hatásokat és a tisztítási műveletet kb. 440 000,- €-t tettek ki.

A tisztítási művelet során nemzetközi segítség érkezett, Észtország 6 önkéntes munkást küldött, Svédország pedig oszlopokat küldött, amelyeket a Daugava folyóra telepítettek.

A Lett Állami Környezetvédelmi Szolgálat a növény- és állatvilágra gyakorolt közvetlen hatásokat, az ország tudósainak bevonásával becsülte meg. Megmértek olyan paramétereket, mint olajtartalom a vízben/lerakódások, víztoxicitás, a folyó állat-/növényvilágának ökotoxicitása, oxigénigény, a biológiai vizsgálatok olyan fajokat foglaltak magukba, amelyeket érzékenynek és reprezentatívnak tekintenek és vizsgálatokat foglaltak magukba az akut toxicitás, krónikus toxicitás, bioakkumuláció lehetősége tekintetében. Ennek eredményeként kiszámításra került a környezet közvetlen károsítása az érintett folyó állat- és növényvilág mérlegének értékelésével. A Lettországi Egyetem kutatásának eredményei a szennyeződés által nem jelentős hosszan tartó hatást igazoltak a környezetre nézve. Továbbá, a szennyeződés hatásának értékelése a halak természetes táptartalékai vonatkozásában (biomassza analízis, fajok változatossága és állatkerti planktonok valamint víz alatti élet) nem mutatott jelentős károsodást, valószínűleg a kora tavaszi időszak miatt.

4. ábra: A Lettországi tűzoltó egységek a védekezés során [14]

Az 5. ábrán látható, hogy a baleset a rendelkezésre álló információk alapján a 4 mutatóval, miként jellemezhető:

5. ábra: Az ipari balesetek Európai skáláján ábrázolva az eset mértéke [14]

Az esemény összegzése

Lettországot és Fehéroroszországot a szovjet korban készült csővezetékek kapcsolják össze, amelyek orosz olajt szállítanak a balti kikötőkbe. Azonban az infrastruktúra nagy része elavult és komoly felújításra szorul. Ebben az esetben is az elöregedés volt a baleset kiváltó oka. Továbbá a tavaszi időszak miatt erős volt az áramlás és nagyon magas volt a vízszint. Nem volt stabil a folyópart talaja, amely így lehetetlenné tette az oszlopok elhelyezését közvetlenül Lettország és Fehéroroszország közé a határokon átívelő szennyeződés megakadályozása érdekében.

ÖSSZEGZÉS

Az olaj egyre kisebb mennyiségben áll rendelkezésre, és egyre drágább, továbbá a kitermelése károsítja a természetet. Azonban egyre több lehetőség, alternatíva áll rendelkezésünkre az olaj kiváltására. A közlekedésben rövid távon a környezetkímélő földgáz, hosszú távon pedig a hidrogén válthatja fel, a háztartásban pedig egyre nagyobb szerepük lesz a különböző megújuló energiáknak, illetve az energiahatékonyságnak.

Az összes megújuló (nap, szél, víz, biomassza) energiaforrásból nyert energia a globális energiafogyasztás mindössze 9%-a volt 2008-ban [15]. Ezt az arányt 40-50-szeresére kellene növelni a jelenlegi energiaigények kielégítése érdekében. 1980 és 2008 között, azaz 28 év alatt mindössze 2%-al nőtt a megújulók részaránya a világ energiafelhasználásában, az 1980-as 7%-ról 9%-ra.

Az iparban és a gazdaságban jelen levő veszélyes anyagok tárolása, feldolgozása és felhasználása magában hordozza a súlyos ipari balesetek kialakulásának kockázatát. A már bekövetkezett olajkatasztrófák elemzése, vizsgálata nélkülözhetetlen a "biztonságos" jövő eléréséhez. Csak ezek tapasztalataival lehet egy esetlegesen bekövetkező újabb katasztrófát megelőzni, vagy a már megtörtént katasztrófák esetében a kárfelszámolás területén hatékonyabban közreműködni a beavatkozás időintervallumát jelentősen csökkenteni.

A veszélyes anyagok felhasználása területén az irány egyértelmű, törekedni kell a megújuló energiaforrások nagyobb arányú felhasználására, és általában a hatékonyság növelésére. Addig is az átmeneti időszakban pedig biztosítani kell a hagyományos energiaforrások (olaj, gáz, atom) környezetbarát és takarékos felhasználását. A szükséges átalakulás csak a politika és a gazdaság összefogásával lehetséges, és persze kizárólag nemzetközi szinten. Fokozatosan el kell hagyni a veszélyes anyagok alkalmazását és áttérni környezetbarát energiaforrások alkalmazására. Ha csökkentjük a veszélyes anyagok alkalmazását, csökken a bekövetkezhető katasztrófák száma is.

Felhasznált irodalom

[1] Németh Ágnes: *A megújuló energiaforrások kiaknázásának ösztönzése az Európai Unióban és Németországban*, Budapesti Gazdasági Főiskola, Budapest, 2010. http://elib.kkf.hu/edip/D_15118.pdf (2016.08.01.)

[2] Pátzay György – Dobor József: *Ipari tevékenységekből eredő veszélyforrások és elhárításuk*, Nemzeti Közszolgálati Egyetem, Katasztrófavédelmi Intézet, Egyetemi Jegyzet, Budapest, 2016. ISBN 978-615-5527-91-3

[3] Dr. Szoboszlay Sándor: *Katonai tevékenységek során a talajba és a talajvízbe kerülő szénhidrogén szennyezések kármentesítésének környezetbiztonsági követelményei*, PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Katonai Műszaki Doktori Iskola, Budapest, 2003. http://uninke.hu/downloads/konyvtar/digitgy/phd/2003/szoboszlay_sandor.pdf (2016.08.02.)

[4] Pregun Csaba - Juhász Csaba: Vízminőségvédelem. Debreceni Egyetem Agrár- és Gazdálkodástudományok Centruma (AGTC), Mezőgazdaság-, Élelmiszertudományi és Környezetgazdálkodási Kar, Víz- és Környezetgazdálkodási Intézet, Debrecen, 2010. ISBN: 978-615-5138-34-8

[5] Thyll Szilárd: *Vízszennyezés, vízminőségvédelem.* DATE Víz- és Környezetgazdálkodási Tanszék, Debrecen, 1998.

[6] Jolánkai Zsolt: *Környezeti kárelhárítás rendkívüli szennyezések esetén*. Budapesti Műszaki És Gazdaságtudományi Egyetem, Vízi Közmű és Környezetmérnöki Tanszék, Budpest, 2014.

[7] Fekete Endre: A vízszennyezés ökológiája. Pro Natura Kiadói Kft. Budapest, 1991. ISBN: 963-8045-39-6

[8] Nagy Szilvia: *Az Exxon Valdez olajszállító hajó katasztrófája, tanulságai.* Műszaki Katonai Közlöny, XXI. évfolyam, Budapest, 2011. http://www.hhk.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/eloadasokpdf/1csop/Nagy%20Szilvia%20Exxon.pdf (2016.08.18.)

[9] Earl Boebert - James M. Blossom: *Deepwater Horizon, A Systems Analysis of the Macondo Disaster.* USA, 2016. ISBN 9780674545236

[10] Dr. Fleit Ernő: *Olajszennyezések kárelhárítása.* Budapesti Műszaki és Gazdaságtudományi Egyetem, Vízi Közmű és Környezetmérnöki tanszék, Budapest, 2014.

[11] ARIA: *Polltution of the river ENNS following leakage from hydrocarbon storage tank.* http://www.aria.developpement-durable.gouv.fr/wp-content/files_mf/FD_32322_steyr_1998_ang.pdf 2016.08.26.

[12] ARIA: *Lessons learnt from industrial accidents.* http://www.aria.developpement-durable.gouv.fr/accident/32322_en/?lang=en 2016.08.26.

[13] ARIA: *Transboundary pollution accident River Daugava (Latvia).* http://www.aria.developpementdurable.gouv.fr/wpcontent/files_mf/FD_35836_latvia_2007_ang.pdf 2016.08.28.

[14] ARIA: *Lessons learnt from industrial accidents.* http://www.aria.developpement-durable.gouv.fr/accident/35836_en/?lang=en 2016.08.28.

[15] Hetesi Zsolt – Szám Dorottya – Végh László: *Utolsó kísérlet - Híradás a föld állapotáról.* Budapest, Kairosz Kiadó, 2008. ISBN: 9789636620264

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Halász László
halasz.laszlo@uni-nke.hu

ELVESZETT ÉRTÉKEK (BEFEJEZETLEN VEGYIVÉDELMI ESZKÖZFEJLESZTÉSEK A HM HADITECHNIKAI INTÉZETNÉL)

Absztrakt

Jelen cikkben áttekintésre kerülnek a vegyivédelem területén kidolgozott olyan eszközök, amelyek végül nem kerültek rendszeresítésre vagy alkalmazásba vételre, vagy ha mégis, akkor gyakorlatilag nem használták. A legtöbb ilyen eszköz a rendszerváltozáshoz köthető koncepcióváltás és a csökkenő kutatási, fejlesztési és beszerzési költségvetések áldozata lett.

In this study those developed items of NBC defence equipment system will be surveyed which were not taken into the system, or if they were taken in and had never been used. Most of such type of equipment were the „victims" of the change of NBC defence concept due to change of society system and the decreasing budgets for research, development and procurement.

Kulcsszavak: *vegyivédelem, kutatás-fejlesztés, ~ NBC (Chemical) Defense, research and development*

BEVEZETÉS

Jelen cikk szerzőjeként elmondhatom, hogy 1967 és l983 között dolgoztam a Honvédelmi Minisztérium Haditechnikai Intézetében tudományos kutatóként, majd ugyanitt 1983-tól 1997-ig tudományos osztályvezetőként. Ekképpen személyesen lehettem részese három évtized vegyivédelmi technikai eszközfejlesztési kísérleteinek, melyeket olykor siker, máskor kudarc jellemzett. Legfájóbb emlékeim közé tartoznak azok a projektek, amelyek a kutatás-fejlesztés fázisán sikeresen végigfutottak, legtöbbjükből készültek is jól működő kísérleti vagy csapatpróba példányok, mégsem kerültek be a hadsereg eszköz rendszerébe. Ezeket joggal nevezhetjük elveszett értékeknek. Ezek zöme vegyivédelmi anyag illetve eszköz volt, de volt köztük álcázástechnikai eszköz is. A vegyivédelmi eszközöket tekintve az egyéni védőeszközök között volt két ilyen fejlesztés, mindkettő a bőrvédő eszközök közé tartozott.

Bőrvédő eszközök

Röviden tekintsük át az akkori követelményeket:

- védőképesség mérgező harcanyag gőzök, aeroszolok ellen legyen legalább 12 óra,
- védőképesség mérgező harcanyag cseppek ellen legyen legalább 2 óra,
- viselhetőségük legyen minimum 4 óra,
- a szilárdsága biztosítsa a tartós viselhetőséget,
- a védőruha viselése a tevékenységet ne csökkentse 30%-nál jobban,
- a védőruha legyen legalább tíz évig tárolható.

A ’60-as évek végén indult egy fejlesztés a rendszeresített 60 M illetve 67 M vegyivédelmi védőruhák felváltására. Ezek a ruhák oppanollal (poliizobutilénnel) bevont textilből készült szigetelő típusú ruhák voltak. Az alapanyag egyrészt túl nehéz volt (350 g/m2), másrészt mivel az oppanol nem térhálósítható polimer, ezért hideg folyása volt és tárolás alatt a ruhák egyes helyein elvékonyodott a védőréteg. Részletesen tanulmányoztuk a mérgező harcanyagok műanyagokon való áthatolását és megállapítottuk, hogy ez beoldódási, majd diffúziós, végül deszorpciós folyamatból áll. Ebből következett, hogy a belső határfelületek megnövelik az átütési időt. A kidolgozott szigetelő típusú alapanyag textil hordozóra felvitt butilkaucsukból és az azt fedő neoprénből állt. Az anyag négyzetméter súlya 210 g volt és kielégítette az előzőekben felsorolt követelményeket [1]. Kenéses technológiával legyártottunk 120 m anyagot, amelyből 12 védőruhát készítettünk el, és ezeket haditechnikai vizsgálatnak vetettük alá, ahol mindenben megfelelőnek minősültek. A kenési technológia nem volt gazdaságos, ezért a gyártó vállalat egy mártógép beszerzése mellett döntött. A beruházás a ’70-es évek végére valósult meg. A sorozatgyártás nem valósult meg, mert a „0” sorozat gyártás során súlyos minőségi problémák jelentkeztek. Az alapvető ok az volt, hogy a gyártó a technológiai sort megszakítva az impregnáló oldatokat alvállalkozóval készíttette el.

A szállítás és tárolás során nem lehetett biztosítani az oldatok stabilitását.

A másik rendszeresítésre nem került védőruházat az M89 jelű védőkészlet volt. Ez a ’80-as évek közepétől általánossá vált szűrő védőruházat hazai variása volt. Az M89A1 a gyakorló ruha helyett viselhető zöld vagy tereptarka ruha volt, amelynek védőrétege egy önkioltó habba bevitt aktív szén volt. (1. ábra) [2,3]

1. a. és b. ábrák: M89A1 védőruha (A szerző archívumából)

A ruha család másik tagja volt az M89A2 alsóruházat, amelyet a gyakorló ruházat alatt lehetett viselni. (2 .ábra)

2. a. és b. ábrák: M89A2 légáteresztő alsóruházat (A szerző archívumából)

A ruházat kiegészítője volt a csepp elleni védelmet biztosító M89 védőköpeny, amely anyaga polietilén volt. (3. ábra)

3. a. és b. ábrák: 89 M fólia védőlepel és csizma és az M 89 kesztyű (A szerző archívumából)

A kesztyű anyaga és a csizma lábfej része butilkaucsukból készült. A védőruházatból 120 készlet került legyártásra, majd csapatpróbára, ami sikeresnek bizonyult. A 120 készletet alkalmazásba vették és használták, de több nem került legyártásra.

Vegyi felderítő eszközök

A legtöbb kifejlesztett és sorozatgyártásba nem került eszköz a vegyi felderítés területéhez tartozott. A vegyi felderítő eszközök az alábbiak szerint csoportosíthatók [3]:

- egyszerű eszközök;
- kézi és félautomata eszközök;
- automaták;
- távfelderítő eszközök;
- laboratóriumok.

Az egyszerű eszközök közé tartoznak az indikátor papírtok és indikátor csövek. A ’90-es évek elején került kifejlesztésre a Double Way indikátor papír. A papír alkalmas volt idegméreg (Vx, szarin, szomán) és hólyaghúzó (kénmustár és luizit) cseppek kimutatására. A megbízhatóság növelésére minden mérgező harcanyagot két indikátor papír elszíneződésével lehetett kimutatni. A papírok hátoldala ragasztó anyagot tartalmazott ezzel lehetett rögzíteni járművekre. A 4. ábra mutatja az indikátor papírt.

4. ábra: Double Way indikátor papír (A szerző archívumából)

A kísérleti sorozat 10 készletből állt. A további gyártási fázisra a rendszerváltás okozta koncepcióváltozás miatt nem került sor.

A ’80-as évek fő fejlesztési területét az automata készülékek jelentették. Az elektronika fejlődése lehetővé tette a kisméretű, nagy sorozatban gyártott, viszonylag olcsó eszközök kidolgozását. Az első ilyen eszközünk az ionmozgékonyságon alapuló GVJ-1 készülék volt, amelyből sorozatgyártás is folyt. Ennek továbbfejlesztett változata volt a GVJ-2 [5].

A készülék idegméreg és hólyaghúzó mérgező harcanyag gőzök kimutatására volt alkalmas. Az egyszerű ionkamrás berendezéshez képest a specifikussága és érzékenysége jobb volt. Az ionkamrába kettős rács került beépítésre. Az elektródák és a rács hengeres házban helyezkedtek el egymástól teflon gyűrűkkel elszigetelve Az alfa-sugárforrás a hengerpaláston helyezkedett el. A kettős rács két alkotója egymástól elektromosan elszigetelt volt. Az elektródokra adott feszültség 30 V, a rácsok közötti feszültség 2 V volt. A rácsra adott feszültséget rácsonként eltérő fázishelyzetű 0-tól 15 kHz-ig terjedő frekvenciával moduláltuk. Az ionizált részecskék a légáramlás és a gyenge elektromos mező hatására a kamrában hosszirányban mozogtak. A kettős rács potenciáljának modulációja keresztirányú elektromos mezőt létesített, az ionok a változó frekvenciájú elektromos mezőben oszcilláló mozgásba kezdtek a rácsok között. Adott frekvencián a legnagyobb amplitúdójú, oszcilláló mozgást végző részecskék a kettős rácsba csapódva rekombinálódtak, így a frekvencia

változásával jellegzetes spektrumot kaptunk. Az ionizációs kamra feszültség és frekvencia értékeit a mérő- és mérésvezérlő egység szabályozta és mérte az elektródokon az ionáramot. Az adatgyűjtést mikroprocesszor végezte, a mérési eredményeket ionáram-frekvenciagörbeként tárolta, és különbséget képezett a levegő görbével.

Jellemzői:

Érzékenysége:	idegmérgekre	5·10-6 mg/l
	hólyaghúzókra	2·10-3mg/l
Kimutatási idő:		10 s
Működési hőmérséklettartomány:		-25 és + 50 oC között.

5. ábra: GVJ-2 készülék (A szerző archívumából)

A GVJ-2-ből 5 db készült, átesett haditechnikai ellenőrző vizsgálaton, de alkalmazásba vételre nem került a rendszerváltás és koncepcióváltozás miatt. Ugyanennek az időszaknak terméke volt a GVJ-3 és az AVJ-2 műszer. A GVJ-3 kifejlesztésekor a cél egy egyszerű, olcsó, kisméretű berendezés volt. Erre a legalkalmasabbnak látszott a piezoelektromos kristály használata. Ha a kristályt bevonjuk egy olyan anyaggal, amely elnyeli a vizsgálandó anyagot, akkor a tömegváltozásnak megfelelően megváltozik a rezgőkörbe kapcsolt kristály saját frekvenciája. A GVJ-3 hárompár piezokristályt tartalmazott, három bevonatos és három referencia kristályt. A bevonatos kristályok kimutatták a Vx-et és a többi idegmérget, illetve a hólyaghúzókat. A mérés után a készülék felfűtötte a bevonatos kristályokat, így távolította el az abszorbeált anyagot. Egy példány készült el, amit haditechnikai ellenőrző vizsgálatnak vetettünk alá, ahol megfelelő minősítést kapott, de sorozatgyártásra nem került. Az AVJ-3 fejlesztésekor a cél egy olyan eszköz volt, ami objektumok védelmét tudja ellátni. Ez egy fotoakusztikus infravörös spektroszkópiás módszert alkalmazó berendezés volt, amely az alábbi leegyszerűsített metodika alapján működött:

- A környező levegő mintát a berendezés vizsgáló kamrájába szivattyúzzuk;
- Egy infravörös fényforrásból az illető gázra jellemző abszorpciós hullámhosszú fénnyel megvilágítjuk;
- Az elnyelt infravörös sugár hatására a minta melegszik;
- A felmelegedés tágulással jár, a térfogat-növekedés pedig a hallható tartományba eső, az adott anyagra jellemző hangot ad (20 Hz – 20 kHz);
- A hangot érzékeny mikrofonok rögzítik;

- A rögzített jel erőssége arányos a gáz koncentrációjával.

Egy kísérleti minta készült el, amely később a BME Atomfizikai tanszékén oktatási célt szolgált.

Vegyi távfelderítő eszközök [6]

A távfelderítő eszközök alkalmasak a vegyi szennyezettség érzékelésére és meghatározására a szennyezett térrésztől nagy távolságból. Fontos jellemzőjük, hogy segítségükkel meg lehet határozni a mérgezőanyag-felhők mozgását. A fejlesztést igen komoly alapkutatás előzte meg, amely során vizsgáltuk a mérgező harcanyag felhők terjedési folyamatait, meghatároztuk a mérgező harcanyagok infravörös és Raman-spektrumait. Az előkísérletek alapján a differenciál-abszorpciós eljárás bizonyult célravezetőnek.

Működési elvét tekintve a berendezés két választható hullámhosszon bocsátott ki sugárzást a vizsgált térrészbe, közös optikai úton. Mindkét sugárzás valamely topografikus tárgyról szóródott vissza, amelyet ismét a kivetítő optika vezetett a sugárzást érzékelő detektorra. A sugárzás így kétszer haladt keresztül az átvilágított térrészen a LIDAR-tól a topografikus tárgyig és vissza. Útközben az átvilágított térrészben lévő szennyező anyag a két hullámhosszon különböző módon abszorbeálta a sugárzást, így az egyes hullámhosszokon más teljesítmény jutott vissza a LIDAR vevőrendszerébe.

Két változat került kialakításra, az egyik helikopter fedélzeti (LRS-2), a másik telepíthető változatban (VTB-2).

Főbb harcászati-műszaki adatok:

Idegmérgek kimutatási távolsága:		10 km
Érzékenysége:	szarinra:	50 mg/m2
	Vx-re:	150 mg/m2
Energiaigénye:		2 kW

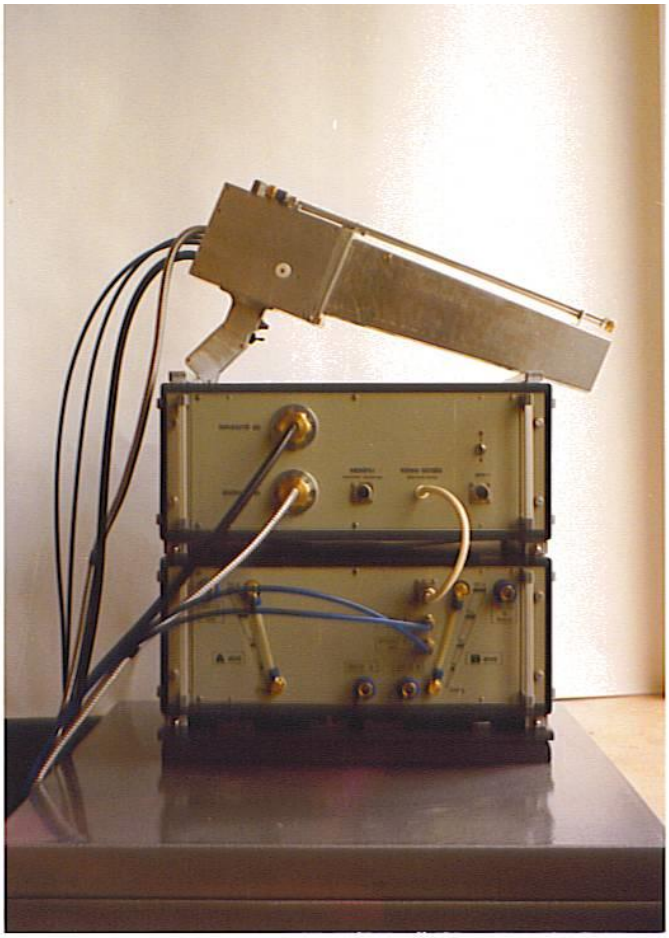
6. ábra: LIDAR-berendezés (VTB-2) (A szerző archívumából)

A berendezések 1995-ben részt vettek egy nemzetközi összehasonlító vizsgálaton Vyskovban. Kiderült, hogy egyedül a mi berendezéseink voltak képesek 10 km-ről megfelelő pontossággal kimutatni a mérgező anyagokat. Ennek ellenére a sorozatgyártás nem történt meg, a két példányt a BME Atomfizikai Tanszéke használta oktatási célra.

VSJ-1 felületi vegyi szennyezettség mérő

A fejlesztés célja a felületi vegyi szennyezettség kimutatása volt járművek, objektumok és a talaj felszínén, valamint a mentesítettség ellenőrzése. A berendezés egy reagenst juttatott a felületre, ezt speciális fénnyel megvilágítva a mérgező harcanyag jelenléte esetén fluoreszcencia jelentkezett, ami mérhető volt. A berendezés három egységből állt.

- reagens ellátó rendszer,
- érzékelő fej,
- elektronikai egység.



7. ábra: VSJ-1 felületi vegyi szennyezettség mérő (A szerző archívumából)

Kimutatási határ:	idegmérgekre:	0,001 mg/cm2
	hólyaghúzókra:	0,01 mg/cm2
Válasz idő:		10 s
Működési tartomány:		-10 és + 50 oC között
Tömeg:		3,5 kg

Egy példány készült el, amelyet haditechnikai ellenőrző vizsgálatnak vetettünk alá. A berendezés megfelelt a követelményeknek, de a koncepcióváltozás miatt nem került sorozatgyártásra.

VLG 90 laborgépkocsi

A laborgépkocsi egy Rába alvázra épített vegyi labor konténerből és egy utánfutóra telepített radiológiai laboratóriumból állt.

A vegyi laboratórium főbb eszközei:

- mintavevő készlet,
- minta előkészítő eszközök
- GC-MS berendezés,
- vékony réteg kromatográf,
- nagynyomású folyadék kromatográf,
- adatfeldolgozó számítógép.

A radiológiai laboratórium főbb eszközei:

- IH-90 többfunkciós sugárzásmérő,
- mintavevő készlet,
- minta előkészítő eszközök,
- radioaktív szennyezettséget mérő műszer,
- adatfeldolgozó számítógép.

8. ábra: Vegyi labor konténer (A szerző archívumából)

A fejlesztés érdekessége volt a BME Atomfizika Tanszékkel közösen fejlesztett GC-MS (gázkromatográf-tömegspektrométer) mérőrendszer. A kísérleti összeállítás 2 példányban készült el, amelyből az egyik a vegyi labor konténerbe került, a második példányát a HTI

egyik laborjában állítottuk fel. Utóbbi feladatai az ellenőrzés, illetve a módszer fejlesztés voltak. A kísérleti járművet a vegyivédelem egy évekig húzódó próbának vetette alá, de felhasználására nem került sor, a vegyivédelmi szertár udvarán állt és végül az enyészet végzett vele.

Automatizált vegyi- és sugár felderítő rendszer (K90). [7]

A rendszer a ’70-es évek közepétől került fejlesztésre és az első változatot (K80) a ’80-as évek közepén csapatvizsgálatnak vetették alá. Ennek tapasztalatai alapján került továbbfejlesztésre a rendszer. A rendszer feladata:

- az atomrobbanások paramétereinek mérése;
- a vegyicsapások jelzése;
- a talaj menti meteorológiai adatok mérése;
- a szennyezett terep sugárszintjének mérése;
- felderítési útvonal helykoordinátáinak folyamatos meghatározása;
- a mért adatok kódolt vagy szöveges információval történő kiegészítése;
- a mért és a kiegészítő adatok gyűjtése és rendezése;
- az adattovábbítás és annak vezérlése;

A rendszer egy ZIL-131/K1 gépkocsira épített adatfeldolgozó és értékelő központból, és 12 db VSBRDM-2 felderítő gépkocsiból állt. A központ eszközei:

- központi számítógép;
- digitalizáló asztal;
- színes grafikus display (2 db), amelyből az egyik 200 méterre kihelyezhető volt;
- adatbeviteli eszköz a felderítő gépkocsiban rögzített adatok utólagos betáplálására;
- háttértároló;
- sornyomtató;
- R-l 11 rádióállomás (2 klt.);
- R323 rádióvevő;
- TBK (távbeszélő) a harcállásponttal való összeköttetéshez;
- 220 V-os fedélzeti aggregátor;
- akkumulátorok a rádiókhoz;
- akkumulátor töltő;
- klímaberendezés

9.ábra: A K90 rendszer értékelő központja és annak berendezései (A szerző archívumából)

A VSBRDM-2 felderítő járműbe beépített eszközök:

- AM-2 automatikus atomrobbanás-mérő;
- AVJ-1 automatikus vegyijelző;
- GVJ-1 gyorsműködésű vegyijelző;
- TMF-2 automata meteorológiai felszerelés;
- IH-31 automatikus sugárszintmérő;
- TNA-3 járműfedélzeti navigációs berendezés;
- JT speciális jelentőtábla;
- fedélzeti mikroszámítógép;
- adattároló egység;
- R-l 11 rádióállomás;
- akkumulátorok;

- kapcsolószekrény;
- generátor (a jármű motorjáról hajtva);
- AB-1 aggregátor;
- IH-81 kombinált sugárzásmérő műszer;
- vegyijelzők légellátó rendszere.

A rendszer csapatpróbáját nem hajtották végre, a koncepcióváltozás miatt. A kísérleti rendszer a katonai műszaki főiskolára került és a vegyivédelmi hallgatók kiképzésére használták.

Mentesítő eszköz

FMG-90

Az FMG-68 leváltására került kifejlesztésre az FMG-90 folyadékos mentesítő gépkocsi. Az FMG-90 Rába alvázra felépített mentesítő rendszer. A mentesítő rendszer fő összetevői:

- Szivattyú egység, amely állt egy dízelmotorból, kisnyomású és nagynyomású szivattyúból.
- Fűthető 5 m3-es, bekeverő és fűtő rendszerrel ellátott mentesítő anyag tartály.
- Csővezetékek, szelepek,
- Mentesítő anyag tároló.
- Ellenőrző és irányító egység.

Főbb működési jellemzői:

Kisnyomású kör:	munkahelyek száma 40,
	mentesítő anyag szállítási távolsága 90 m,
	mentesítő anyag térfogatárama 13 l/s,
	mentesítő anyag felfűtési ideje 1-1,5 óra.
Nagynyomású kör:	munkahelyek száma 8,
	mentesítő anyag szállítási távolsága 300 m,
	mentesítő anyag térfogatárama 220 l/s.

10. ábra: FMG-90 mentesítő gépkocsi (A szerző archívumából)

Az elkészült mintapéldány sikeres csapatpróbán ment át, majd alkamazásba vételre került, de használni nem használták.

ÖSSZEGZÉS

Az előzőekben áttekintett eszközök közül egy kivételével mind a rendszerváltás okozta koncepcióváltozás áldozatai lettek. Korábban a Varsói Szerződls országai azt vallották, hogy az ABV védelem technikai eszközeit lehetőleg minden országnak zömében magának kell gyártani, licencek vagy hazai műszaki fejlesztés alapján. Ez az elv megváltozott, mivel hozzáférhetővé váltak nyugati eszközök, és jelentős szerepet játszottak a hadsereg létszámának valamint a rendelkezésre álló forrásoknak a jelentős csökkenése. Mindenesetre ezen eszközök számos olyan szellemi értéket testesítettek meg, amely létrehozása idején nemzetközileg is jelentős volt. Így például az ionmozgékonysági kromatográf, a differenciálabszorpciós LIDAR vagy a saját fejlesztésű tömegspektrométer.

Felhasznált irodalom

[1] Halász L, Holop M., Illés B., Parragh G. Mérgező harcanyagok ellen védő rétegelt textil (158 636 /1969/ magyar szabadalom)

[2] Halász L., Pál, J., Illés B., Erdős J. Mérgező anyagok (folyadékok, gázok) ellen védő, lángálló tulajdonságú textil anyag (208 897/1993/ magyar szabadalom)

[3] Halász L., Pál J., Illés B., Erdős J.: Eljárás mosható, regenerálható, aktív szenet tartalmazó, olajálló, porózus textil előállítására (208 896/1993/ magyar szabadalom)

[4] Halász L., Prágai M.: A vegyi felderítőeszköz fejlesztés irányai a 80-as években, Haditechnika 1989 (3) 2-4

[5] Halász L., Illés B., Sáfrán L., Sáfrán Lajosné, Sebők E.: Katonai vegyifelderítő műszer a légtér mérgezőanyag szennyezettségének kimutatására (168 887/1974/ magyar szabadalom)

[6] Richter P., Halász L., Péceli I. Gazdag L. Eljárás és berendezés légköri szennyezés mérésére (T663495/1991/titkos szabadalom)

[7] Erdős J., Pintér I., Solymosi J.: Magyar ABV védelmi technikai almanach, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest (2003)

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Horváth Kristóf - Kátai-Urbán Lajos - Sebestyén Zsolt
horvathk@oah.hu; katai.lajos@uni-nke.hu, sebestyen@oah.hu;

A NUKLEÁRIS BIZTONSÁG ÉS VÉDETTSÉG HAZAI KUTATÁSI-FEJLESZTÉSI EREDMÉNYEI

Absztrakt

A nukleáris biztonság és védettség kutatási-fejlesztési eredményeinek az időszakos értékelése előfeltétele a sikeres felkészülésnek és védekezésnek. A sugárvédelmi szabályozás, eljárások és eszközök korszerűsítésének napjainkban kiemelten fontos szerepe van, mivel a meglévő jelentős számú hazai nukleáris létesítmény mellett az atomerőművi blokkok bővítését tervezzük. A szabályozási változások és az atomenergia széleskörű alkalmazása miatt szükséges a nukleáris létesítmények telephely-vizsgálati és radiológiai értékelési rendszeréhez tartozó korszerűsítési lehetőségek rendszeres feltárása. A sugárvédelmi eljárások és műszerek fejlesztése terén elért fontosabb hazai kutatási-fejlesztési és felhasználói eredmények rendszeres áttekintő érékelése elengedhetetlen a nukleáris biztonság és a nukleáris védettség sikere érdekében. A két cikkre tervezett cikksorozatunk jelen első közleményében irodalmi áttekintést adunk a sugárvédelemi eljárások és műszerek fejlesztése terén elért fontosabb hazai kutatási-fejlesztési és innovációs eredményeiről. A második cikkben elemzést teszünk közzé a hazai és nemzetközi szabályozási rendszerek korszerűsítési lehetőségeiről.

The periodic assessment of the research and development results of nuclear safety and security is a prerequisite for successful preparation and protection. The modernization of radiation protection regulations, procedures and instruments has an essential role as in addition to the significant number of existing domestic nuclear facilities, nuclear power plant expansion is being planned. Due to the regulatory changes and the extensive use of nuclear energy, it is very important to regularly review the modernization possibilities of site examination and radiological assessment of nuclear facilities. Major domestic research and development results and user records in the field of radiation protection procedures and instruments had to be regularly assessed to ensure effective nuclear safety and nuclear security. In this first release of our two planned papers we provide an overview of the literature on the most important domestic research, development and innovation results of radiation protection in the field of development procedures and instruments. In the second publication we offer an analysis about the modernization possibilities of the domestic and international legislation.

Kulcsszavak: *nukleáris biztonság, sugárvédelem, korszerűsítés, Magyarország ~ nuclear security, radiation protection, modernization, Hungary*

BEVEZETÉS

A közlemény áttekintő értékelést tartalmaz a nukleáris biztonság és védettség hazai sugárvédelmi eredményeiről. A téma aktualitását indokolja, hogy az időszakos értékelés állandó előfeltétele a sikeres felkészülésnek és védekezésnek. A sugárvédelem legfontosabb elemeit képező jogi szabályozások, valamint a sugárvédelmi eljárások és eszközrendszerek korszerűsítése értékelésének napjainkban azért van kiemelten fontos szerepe, mivel a meglévő jelentős számú hazai nukleáris létesítmény mellett napirenden van az atomerőművi blokkok bővítése.

A két cikkre tervezett cikksorozat jelen első közleményében irodalmi áttekintést adunk a sugárvédelmi eljárások és műszerek fontosabb hazai kutatási-fejlesztési és innovációs eredményeiről, a nukleáris biztonság és a nukleárisbaleset-elhárítás érdekében. A hazai és nemzetközi szabályozási rendszerek korszerűsítési lehetőségeiről a második cikk ad elemzést.

Az adott témakörben a katonai műszaki tudományos szemléletnek megfelelően feltétlenül foglalkoznunk kell a lakossági sugárvédelem mellett, az annak a biztosítása érdekében tevékenykedő, első beavatkozó állomány megfelelő védelméről is. Nevezetesen a mentő egységek, a Magyar Honvédség, a Katasztrófavédelem, a mentők, a rendészeti személyzet megfelelő sugárvédelme rendkívül fontos feladat.

A cikk megírásánál figyelembe vettük Csurgai József és társa által írt, a nukleáris létesítmények telephely-vizsgálatának és értékelésének korszerűsítéséről szóló összefoglalóját. [1]

A HATÓSÁGI SZABÁLYOZÁS JELENLEGI EGYSÉGES HAZAI RENDSZERE

Az egységes atomenergia-felügyelet megteremtése érdekében a Paksi Atomerőmű bővítéséhez alkotott törvény (2015. évi VII. törvény) [2]) az atomenergia-felügyeleti szerv (Országos Atomenergia Hivatal - OAH) hatáskörébe adta a sugárvédelmi szakterület felügyeletét is 2016. január elsejétől. A törvény az OAH hatáskörébe telepíti a radioaktív anyagok és ionizáló sugárzást létrehozó berendezések felügyeletét, a kötelezően mérendő adatok meghatározását, azok gyűjtésének, nyilvántartásának, értékelésének módját, személyi sugárvédelmi ellenőrzési kötelezettség megállapítását, a személyi dózisok nyilvántartását, védőeszközök minősítését, forgalomba hozatalát, engedélyezését, sugárvédelmi képzések, továbbképzések tematikájának, vizsgakövetelményeinek jóváhagyását, valamint dóziskorlátok megállapítását és dózismegszorítások jóváhagyását.

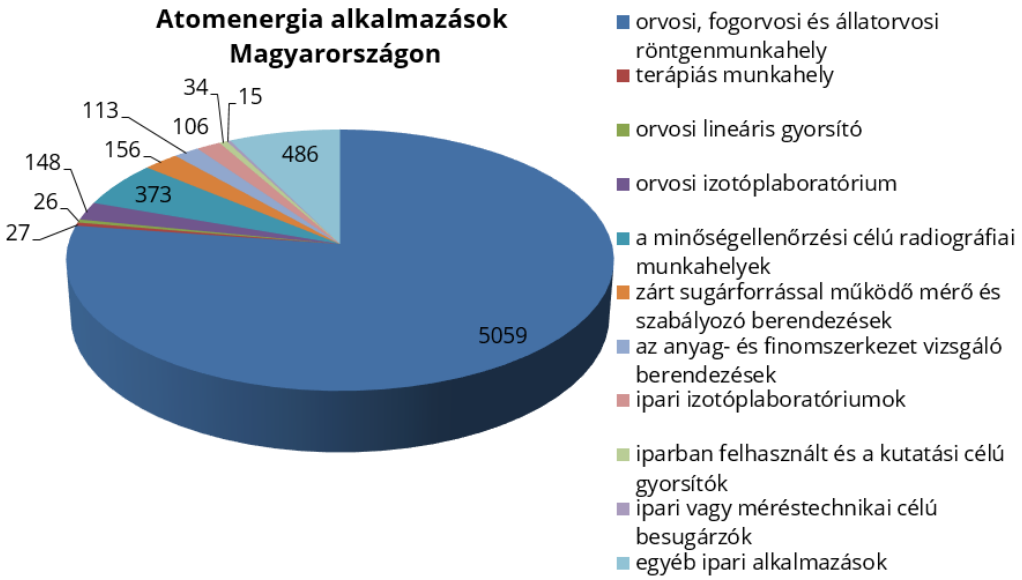
Az egységesítés célja, hogy egy hatóság alá tartozzon a nukleáris biztonság, a sugárvédelem, a kizárólag békés célú alkalmazás és a fizikai védelem felügyelete, hogy megvalósuljon egy egyszintű, országos hatáskörű, ügyfélbarát hatósági rendszer, hogy az engedélyek kérelmezése és kiadása egyszerűsödjön, az egy engedélyesre jutó eljárások száma csökkenjen, illetve hogy az atomenergia alkalmazói által nyújtandó adatszolgáltatás egységes legyen. A sugáregészségügyi kérdésekben továbbra is az egészségügyi hatóság (Országos Tisztifőorvosi Hivatal) az illetékes. A hatósági engedélyek feltételeinek vizsgálatára az atomenergia-felügyeleti szerv – szakértői közreműködés érdekében – más intézményt is igénybe vehet és a leggyakrabban igénybe vett intézetekkel, intézményekkel együttműködési megállapodást köt [3].

Magyarország az atomenergia alkalmazás területén sokszínű országnak számít, mivel a következő tizenkét szakterületen összesen 6540 felhasználó található szerte az országban:

- orvosi, fogorvosi és állatorvosi röntgenberendezést alkalmazó nyilvántartott egység – 5056,
- terápiás nyilvántartott egység – 27,
- orvosi lineáris gyorsítót alkalmazó nyilvántartott egység – 26,
- orvosi izotóplaboratóriumi egység – 148,

- minőségellenőrzési célú radiográfiai munkahelyek – 373,
- zárt sugárforrással működő mérő és szabályozó berendezések – 156,
- az anyag- és finomszerkezet vizsgáló berendezések – 113,
- az ipari izotóplaboratóriumok – 106,
- iparban felhasznált és a kutatási célú gyorsítók – 34,
- az ipari vagy méréstechnikai célú besugárzók – 15,
- egyéb ipari alkalmazások – 486.

Az atomenergia hazai alkalmazásának a számszerű megoszlása jól látható az 1. ábrán. Az 1. ábrát az OAH központi nyilvántartások 2015. évi adatai alapján szerkesztették meg a szerzők.



1. ábra. Atomenergia alkalmazások Magyarországon

Csak érdekességként említjük meg, hogy az alkalmazói csoportok elnevezése szerint az egyéb ipari alkalmazások címszó alatt – amely a máshová be nem sorolható nukleáris létesítményeket tartalmazza – olyan szerényen megbúvó, de korántsem jelentéktelen létesítményeket találunk, mint egy oktató reaktor, egy kutatórektor, két radioaktív hulladéktároló, a Kiégett Kazetták Átmeneti Tárolója, és végül, de nem utolsó sorban a Paksi Atomerőmű 4 blokkja.

NEMZETKÖZI AJÁNLÁSOK ÉS IRÁNYELVEK

A hazai szabályozásnak 2018. február 6-ig meg kell felelnie az ionizáló sugárzás okozta sugárterhelésből származó veszélyekkel szembeni védelmet szolgáló alapvető biztonsági előírások megállapításáról, valamint a 89/618/Euratom, a 90/641/Euratom, a 96/29/Euratom, a 97/43/Euratom és a 2003/122/Euratom irányelv hatályon kívül helyezéséről szóló, a Tanács 2013/59/EURATOM irányelvének. [4]

Az irányelv a korábbi BSS (96/29/Euratom) és négy további specifikus irányelv (az orvosi célú besugárzások sugárvédelmi kérdéseivel foglalkozó 97/43/Euratom, a veszélyhelyzetek esetére vonatkozó 89/618/Euratom, a külső munkavállalók sugárvédelmét szabályozó 90/641/Euratom és a nagy aktivitású zárt sugárforrások védelmét szabályozó 2003/122/Euratom) felülvizsgálatával és összeépítésével keletkezett.

Az irányelvek a Nemzetközi Sugárvédelmi Bizottság[1], a Nemzetközi Atomenergia Ügynökség[2] (továbbiakban: NAÜ) és más szervezetek újabb ajánlásait is figyelembe vették az új irányelv készítése során.

A NAÜ sugárvédelmi biztonsági alapszabályzatát [5] 2011-ben aktualizálták az új kutatási fejlesztési eredményekkel. A szabályzat többek között tartalmaz általános követelményeket a védelemre és biztonságra, illetve a tervezett-, a veszélyhelyzeti-, valamint a fennálló sugárzási helyzetekre speciális ajánlásokat. A mellékletei tartalmazzák a felszabadítási és mentességi szinteket, a zárt sugárforrások kategorizálását, a tervezett besugárzási helyzet dózis korlátait, valamint azok kiszámításához szükséges dóziskonverziós tényezőket.

NUKLEÁRIS LÉTESÍTMÉNYEKRE VONATKOZÓ SZABÁLYOZÁS

A nukleáris létesítményekre vonatkozó hazai szabályozás csúcsán az atomenergiáról szóló 1996. évi CXVI. törvény [3] áll, melynek végrehajtó rendelkezései közül a legfontosabbak a következők: a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről szóló 118/2011. (VII. 11.) Korm. rendelet [6] és mellékletei, a Nukleáris Biztonsági Szabályzatok [7]; a radioaktív hulladékok átmeneti tárolását vagy végleges elhelyezését biztosító tároló létesítmények biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről szóló 155/2014. (VI. 30.) Korm. rendelet [8], az ionizáló sugárzás elleni védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló 487/2015. (XII. 30.) Korm. rendelet [9], valamint a 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről [32].

A 118/2011.(VII. 11.) Korm. rendelet és a 155/2014. (VI. 30.) Korm. rendelet célkitűzése, hogy a nukleáris létesítmények nukleáris biztonság szempontjából fontos rendszereit, rendszerelemeit úgy kell megtervezni, hogy a nukleáris létesítmények alkalmazásával összefüggő általános nukleáris biztonság, valamint az azt megalapozó sugárvédelmi és műszaki biztonság megvalósíthatók legyenek.

Az üzemeltető személyzet és a lakosság sugárterhelése a nukleáris létesítmény üzemeltetése során mindenkor az előírt határértékek alatti, az ésszerűen elérhető legalacsonyabb szintű legyen.

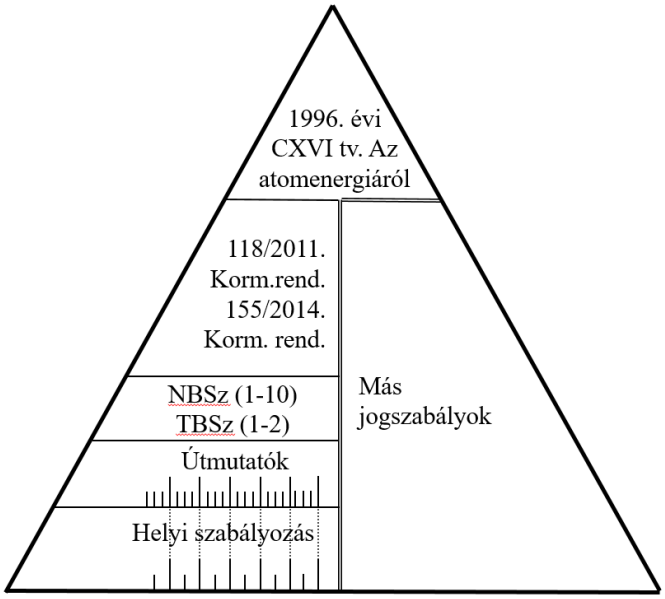
A változás végrehajtása érdekében az OAH kidolgozta a 16/2000. EüM rendelet [10] átalakításaként, valamint az EU BSS megfeleltetéseként az új sugárvédelmi rendeletet, melyet a Kormány hatályba léptetett a 487/2015. (XII.30.) Korm. rendeletként. A rendelet többek között tartalmazza a lakosság dózisbecsléséhez szükséges, kötelezően mérendő adatok meghatározását, a mérést végző szervek tevékenységének összehangolását, az adatok gyűjtését, feldolgozását, nyilvántartása és értékelését.

Az Állami Népegészségügyi és Tisztiorvosi Szolgálat Országos Tisztifőorvosi Hivatal hatáskörében maradt sugáregészségügyi követelmények továbbra is az egészségügyi szolgáltatások nyújtása során ionizáló sugárzásnak kitett személyek egészségének védelméről szóló 31/2001. (X. 3.) EüM rendeletben EüM rendeletben maradtak. Ezeken felül hatályba lépett a lakosság természetes és mesterséges eredetű sugárterhelését meghatározó környezeti sugárzási helyzet ellenőrzési rendjéről és a kötelezően mérendő mennyiségek köréről szóló 489/2015. (XII.30.) Korm. rendelet [11], valamint a hiányzó, a talált, valamint a lefoglalt nukleáris és más radioaktív anyagokkal kapcsolatos bejelentésekről és intézkedésekről, továbbá a nukleáris és más radioaktív anyagokkal kapcsolatos egyéb bejelentést követő intézkedésekről szóló 490/2015. (XII.30.) Korm. rendelet [12] a sugárvédelmi feladatok

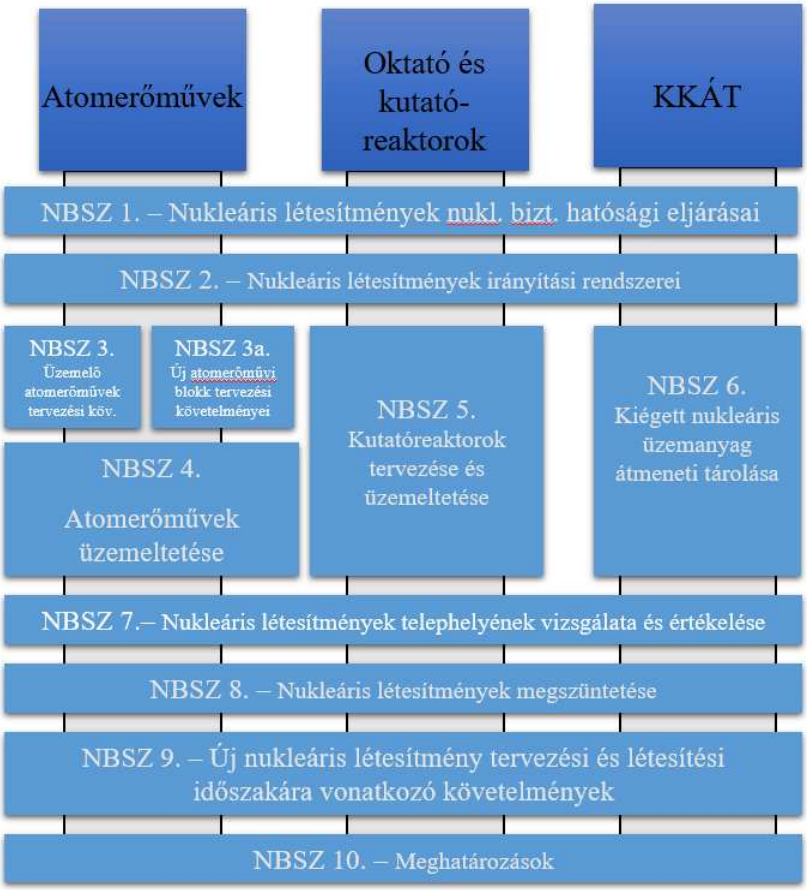
[1] International Commission on Radiological Protection, ICRP
[2] International Atomic Energy Agency, IAEA

ellátása érdekében. A hatáskörök változása miatt több jogszabályt módosítani kellett, úgymint a 112/2011 Korm. rendeletet [13] is.

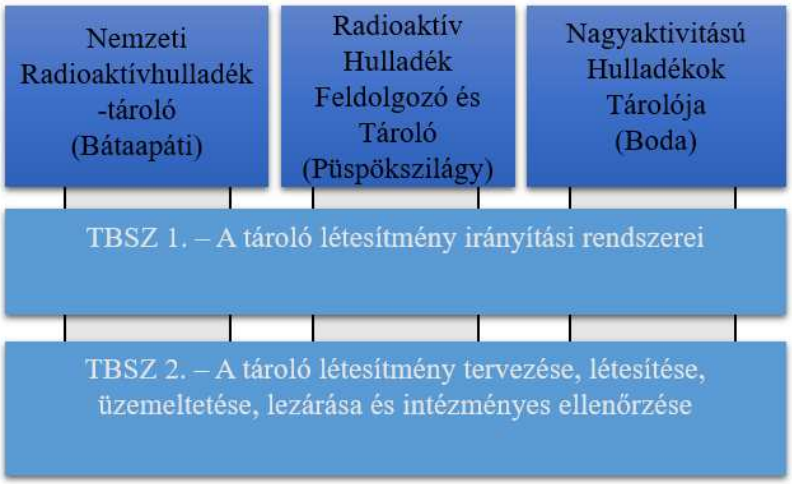
A 2. ábra a nukleáris létesítmények és radioaktív hulladéktárolók biztonságának hazai jogszabályi rendszerének felépülését szemlélteti.



2. ábra. Nukleáris létesítmények szabályozási rendszerének sematikus ábrája [1]



3. ábra. a Nukleáris Biztonsági Szabályzatok [1]



4. ábra. a Tároló Biztonsági Szabályzatok, forrás: OÁH

A nukleáris létesítményekre vonatkozó előírások hazai és nemzetközi jogi szabályozását a Feldolgozandó irodalomban adjuk meg.

A hazai jogszabályok megfelelnek az EU-s követelményeknek, ugyanakkor szükség lehet a tovább fejlesztésükre a sugárvédelem területén. Jelenleg a 487/2015 (XII.30.) Korm. rendelet tartalmazza a sugárvédelmi szabályozást minden létesítményre, alkalmazásra, berendezésre, munkahelyre. Néhány specifikus követelmény megjelenik a 118/2011 Korm. rendeletben [3], valamint a 155/2014. Korm. rendeletben [8], de szükség lehet azok fejlesztésére, hogy folyamatosan a modern fejlesztések, kutatások eredményeinek megfeleljen.

Nukleáris létesítményekre vonatkozó előírások: Az 1996. évi CXVI. törvény az atomenergiáról [3], 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól [14], 112/2011.(VII. 4.) Korm. rendelet az Országos Atomenergia Hivatal nukleáris energiával kapcsolatos európai uniós, valamint nemzetközi kötelezettségével összefüggő feladatköréről, az Országos Atomenergia Hivatal hatósági eljárásaiban közreműködő szakhatóságok kijelöléséről, a kiszabható bírság mértékéről, valamint az Országos Atomenergia Hivatal munkáját segítő tudományos tanácsról [13], 118/2011.(VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről [6], Nukleáris Biztonsági Szabályzatok [7], 246/2011.(XI. 24.) Korm. rendelet a nukleáris létesítmény és a radioaktívhulladék-tároló biztonsági övezetéről [15], 247/2011.(XI. 25.) Korm. rendelet az atomenergia alkalmazása körében eljáró független műszaki szakértőről [16], 167/2010.(V. 11.) Korm. rendelet az országos nukleárisbaleset-elhárítási rendszerről [17], 146/2014 (V.5.) Korm. rendelet a felvonókról, a mozgólépcsőkről és a mozgójárdákról [18], 215/2013. (VI. 21.) Korm. rendelet a radioaktív hulladékokkal és a kiégett üzemanyaggal kapcsolatos egyes feladatokat ellátó szerv kijelöléséről, tevékenységéről és annak pénzügyi forrásairól [19], 16/2000. (VI. 8.) EüM rendelet az atomenergiáról szóló 1996. évi CXVI. törvény egyes rendelkezéseinek végrehajtásáról [10], 15/2001. (VI. 6.) KöM rendelet az atomenergia alkalmazása során a levegőbe és vízbe történő radioaktív kibocsátásokról és azok ellenőrzéséről [20], 5/2015. (II. 27.) BM rendelet az atomenergia alkalmazásával kapcsolatos sajátos tűzvédelmi követelményekről és a hatóságok tevékenysége során azok érvényesítésének módjáról [21], 55/2012. (IX. 17.) NFM rendelet a nukleáris létesítményben foglalkoztatott munkavállalók speciális szakmai képzéséről, továbbképzéséről és az atomenergia alkalmazásával összefüggő tevékenységek folytatására jogosultak köréről [22], 108/2001. (XII. 23.) FVM-GM rendelet a felvonók biztonsági követelményeiről és megfelelőségének tanúsításáról [23].

Sugárvédelmi előírások: A TANÁCS 2013/59/EURATOM IRÁNYELVE az ionizáló sugárzás miatti sugárterhelésből származó veszélyekkel szembeni védelmet szolgáló alapvető

biztonsági előírások megállapításáról, valamint a 89/618/Euratom, a 90/641/Euratom, a 96/29/Euratom, a 97/43/Euratom és a 2003/122/Euratom irányelv hatályon kívül helyezéséről **Hiba! A hivatkozási forrás nem található.**, 487/2015. (XII. 30.) Korm. rendelet az ionizáló sugárzás elleni védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről [9], 489/2015. (XII. 30.) Korm. rendelet a lakosság természetes és mesterséges eredetű sugárterhelését meghatározó környezeti sugárzási helyzet ellenőrzési rendjéről és a kötelezően mérendő mennyiségek köréről [11], 165/2003. (X. 18.) Korm. rendelet a nukleáris és radiológiai veszélyhelyzet esetén végzett lakossági tájékoztatás rendjéről [24], 167/2010. (V. 11.) Korm. rendelet az országos nukleárisbaleset-elhárítási rendszerről [17], 4/2016. (III. 5.) NFM rendelet az Országos Atomenergia Hivatal egyes közigazgatási eljárásaiért és igazgatási jellegű szolgáltatásaiért fizetendő díjakról [25], 16/2000. (VI. 8.) EüM rendeletet az atomenergiáról szóló 1996. évi CXVI. törvény egyes rendelkezéseinek végrehajtásáról [10], 31/2001. (X. 3.) EüM rendelet az egészségügyi szolgáltatások nyújtása során ionizáló sugárzásnak kitett személyek egészségének védelméről [26], 47/2003. (VIII. 8.) ESzCsM rendelet a radioaktív hulladékok átmeneti tárolásának és végleges elhelyezésének egyes kérdéseiről, valamint az ipari tevékenységek során bedúsuló, a természetben előforduló radioaktív anyagok sugár-egészségügyi kérdéseiről [27].

Fizikai védelmi előírások: 1987. évi 8. tvr. a nukleáris anyagok fizikai védelméről szóló egyezmény kihirdetéséről [28], 2007. évi XX. törvény a nukleáris terrorcselekmények visszaszorításáról szóló nemzetközi Egyezmény kihirdetéséről [29], 2008. évi LXII. törvény a Nemzetközi Atomenergia Ügynökség (NAÜ) keretében 1979-ben elfogadott, és az 1987. évi 8. törvényerejű rendelettel kihirdetett nukleáris anyagok fizikai védelméről szóló Egyezménynek a NAÜ által szervezett diplomáciai konferencia keretében, 2005. július 8-án aláírt módosítása kihirdetéséről [30], 1996. évi CXVI. törvény az atomenergiáról [1], 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól [14], 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról [31], 112/2011. (VII. 4.) Korm. rendelet az Országos Atomenergia Hivatal nukleáris energiával kapcsolatos európai uniós, valamint nemzetközi kötelezettségével összefüggő feladatköréről, az Országos Atomenergia Hivatal hatósági eljárásaiban közreműködő szakhatóságok kijelöléséről, a kiszabható bírság mértékéről, valamint az Országos Atomenergia Hivatal munkáját segítő tudományos tanácsról [13], 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről [32], 47/2012. (X. 4.) BM rendelet az atomenergia alkalmazásával összefüggő rendőrségi feladatokról[33], 7/2007. (III.6.) IRM rendelet a nukleáris anyagok nyilvántartásának és ellenőrzésének szabályairól [34], 11/2010.(III. 4.) KHEM rendelet a radioaktív anyagok nyilvántartásának és ellenőrzésének rendjéről, valamint a kapcsolódó adatszolgáltatásról [35], A Nemzetközi Atomenergia Ügynökség nukleáris védettségre vonatkozó ajánlásai (Nuclear Security Series Publications) [36], 490/2015 (XII. 30.) Korm. rendeletet a hiányzó, a talált, valamint a lefoglalt nukleáris és más radioaktív anyagokkal kapcsolatos bejelentésekről és intézkedésekről, továbbá a nukleáris és más radioaktív anyagokkal kapcsolatos egyéb bejelentést követő intézkedésekről. [12].

Radioaktívhulladék-tárolóra vonatkozó előírások: 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól [14], 112/2011. (VII. 4.) Korm. rendelet az Országos Atomenergia Hivatal nukleáris energiával kapcsolatos európai uniós, valamint nemzetközi kötelezettségével összefüggő feladatköréről, az Országos Atomenergia Hivatal hatósági eljárásaiban közreműködő szakhatóságok kijelöléséről, a kiszabható bírság mértékéről, valamint az Országos Atomenergia Hivatal munkáját segítő tudományos tanácsról [13], 155/2014. (VI. 30.) Korm. rendelet a radioaktív hulladékok átmeneti tárolását vagy végleges elhelyezését biztosító tároló létesítmények biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről [8], melléklet: A tároló létesítmény irányítási rendszerei,

melléklet: A tároló létesítmény tervezése, létesítése, üzemeltetése, lezárása és intézményes ellenőrzései, 246/2011. (XI. 24.) Korm. rendelet a nukleáris létesítmény és a radioaktívhulladék-tároló biztonsági övezetéről [15], 247/2011.(XI. 25.) Korm. rendelet az atomenergia alkalmazása körében eljáró független műszaki szakértőről [16], 167/2010.(V. 11.) Korm. rendelet az országos nukleárisbaleset-elhárítási rendszerről [17], 146/2014 (V.5.) Korm. rendelet a felvonókról, a mozgólépcsőkről és a mozgójárdákról [18], 215/2013. (VI. 21.) Korm. rendelet a radioaktív hulladékokkal és a kiégett üzemanyaggal kapcsolatos egyes feladatokat ellátó szerv kijelöléséről, tevékenységéről és annak pénzügyi forrásairól [19], 16/2000. (VI. 8.) EüM rendelet az atomenergiáról szóló 1996. évi CXVI. törvény egyes rendelkezéseinek végrehajtásáról [10], 15/2001. (VI. 6.) KöM rendelet az atomenergia alkalmazása során a levegőbe és vízbe történő radioaktív kibocsátásokról és azok ellenőrzéséről [20], 5/2015. (II. 27.) BM rendelet az atomenergia alkalmazásával kapcsolatos sajátos tűzvédelmi követelményekről és a hatóságok tevékenysége során azok érvényesítésének módjáról [21], 108/2001. (XII. 23.) FVM-GM rendelet a felvonók biztonsági követelményeiről és megfelelőségének tanúsításáról [23], 47/2003. (VIII. 8.) ESzCsM rendelet a radioaktív hulladékok átmeneti tárolásának és végleges elhelyezésének egyes kérdéseiről, valamint az ipari tevékenységek során bedúsuló, a természetben előforduló radioaktív anyagok sugár-egészségügyi kérdéseiről [27], 213/2013. (VI. 21.) Korm. rendelet a Központi Nukleáris Pénzügyi Alap Szakbizottságról [37], 214/2013. (VI. 21.) Korm. rendelet a Központi Nukleáris Pénzügyi Alapból az ellenőrzési és információs célú önkormányzati társulásoknak nyújtott támogatások szabályairól [38].

FONTOSABB HAZAI KUTATÁSI EREDMÉNYEK

Hazánkban a nukleáris biztonság- és balesetelhárítás érdekében már az 1970-es évektől kezdve intenzív fejlesztési tevékenység indult meg a veszélyhelyzeti sugárvédelmi eljárások és műszerek fejlesztése terén a HM Haditechnikai Intézet, a Budapesti Műszaki Egyetem Vegyészmérnöki Kar, Fizikai Kémia Tanszék és a Gamma Művek együttműködésével. Solymosi József vezetésével korszerű új mérési eljárások kerültek kifejlesztésre a maghasadás radioaktív (hasadási) termékeinek kormeghatározására és az ismeretlen és/vagy összetételű, többkomponensű radioaktív anyagoktól származó elnyelt dózis folyamatos értékelésére és prognosztizálására. [39][40] Hatékony eljárást fejlesztettek ki a bétasugárzó radionuklidoktól származó felületi szennyezettség és (térfogati) radioaktív koncentráció egyszerű, gyors meghatározására. Egyedi eljárást fejlesztettek ki az intenzív gamma-háttérsugárzásban történő béta-sugárzás mérése során a jel/zaj viszony javítására energiakompenzációs módszerrel, valamint a radionuklidokkal kontaminált terep légi- és földi sugárfelderítésére.
A közös fejlesztések eredményeként jött létre több sugárvédelmi mérőműszer és rendszer, amelyeket a Gamma Műszaki Zrt. napjainkban is sorozatban gyárt és értékesít itthon és a világ számos országában.
A kezdeti időszak kormeghatározási eljárását Csurgai József vezetésével jelentősen továbbfejlesztették.[41] Iterációs módszer alkalmazásával számolták az ismeretlen összetételű hasadási termékeket tartalmazó mintáktól származó dózis prognosztizált értékét. Ezzel az értékelés pontossága jelentősen megnövekedett, és az atomrobbanási termékek mellett a továbbiakban alkalmassá vált az atomerőmű kiégett fűtőelemeinek az értékelésére is.
Csurgai József kidolgozta a Magyar Honvédségnél alkalmazott sugárhelyzet prognosztizálási és értékelési eljárások továbbfejlesztését számítógépes megvalósítással.[42] Kutatási eredményének a téziseit doktori PhD értekezésében tette közzé: Nukleárisbaleset-elhárítás és vegyi katasztrófák összefüggésrendszerének tudományos vizsgálata. [43]

Bétaszennyezettség mérése intenzív gamma-háttérben

A radioaktív felületi bétaszennyezettség, majd azt követően a béta-sugárzó izotópo(ka)t tartalmazó minta aktivitásának mérésére nagy intenzitású gamma-sugárzási háttérben mérésére fejlesztettek ki szabadalmi oltalommal védett eljárást Solymosi József és munkatársai. [44][45][46][47][48]

Kimagasló eredménynek minősíthető az alkotói kollektíva találmánya az Univerzális radioaktív sugárzásmérő műszer és eljárás, valamint rendszertechnikai elrendezés a méréshatárának kiterjesztésére. [49][50][51]

Részletesen bemutatjuk az ionizáló sugárzások (α-, β- és γ) mérésére a találmány szerinti eljárás gyakorlati megvalósítását, amely alapján a Gamma Műszaki Zrt., Budapest sorozatban gyártja a széles méréshatárú, "Gammacont" elnevezésű univerzális sugárzásmérő műszert.

A GM-csövek méréshatárának kiterjesztésére régóta használt módszer több GM-cső használata, illetve az impulzus-üzemű alkalmazás. Ha az anódfeszültséget 10-20 μs-os időtartamig – ami a holtidőhöz képest rövid idő – megnöveljük úgy, hogy az a plató-tartományba essen, akkor a látszólagos holtidő erre a 10-20 μs-os értékre csökken.

A GAMMA Rt. által kifejlesztett - GAMMACONT - műszerben ezek továbbfejlesztett kombinációját valósítottuk meg. Több GM-cső helyett egyetlen 10 anódos típust használunk kapcsolt anódokkal, illetve új impulzusüzemű algoritmussal. A legérzékenyebb méréstartományban mind a tíz anódra jut nagyfeszültség. A nagyobb tartományban csak egy anód marad bekapcsolva. A nem használt anódokra 200 V feszültség jut. A beérkező impulzus hatására az áramkör 400 V-ról - 200 V-ra csökkenti az anódfeszültséget kb. t = 1 ms időtartamra. Ez alatt a GM-cső gázterében a tértöltés az alacsony anódfeszültség miatt további sokszorozás nélkül megszűnik.

Az IH-95 sugárszint- és szennyezettség- mérő műszer sugárvédelmi célú mérésekre alkalmas hordozható kivitelű dózismérő, és felületi radioaktív-szennyezettségmérő.

A műszer dózismérés és dózisteljesítmény mérés üzemmódban a fotonsugárzás levegőben elnyelt dózisát illetve dózisteljesítményét méri és jelzi ki. A beállított riasztási szint elérésekor mind dózismérés mind dózisteljesítmény mérés esetén hangjelzéssel riaszt.

Szennyezettségmérőként a műszer alfa és béta felületi szennyezettséget, illetve béta folyadék térfogati aktivitáskoncentrációt mér.

Az IH-95 szabványos RS-232 soros kimeneten a mérések eredményeit továbbítani tudja IBM AT kompatibilis számítógépnek további feldolgozásra.

A műszer főbb műszaki (metrológiai) jellemzői:

<u>Dózismérő:</u>

méréstartomány: 10 nGy ... 1 Gy
50 nGy/h ... 500 mGy/h

energiatartomány: a fotonsugárzás 60 keV ... 1,5 MeV tartománya

mért mennyiség: levegőben elnyelt dózis D [Gy] és
levegőben elnyelt dózisteljesítmény $\dot{D}$ [Gy/h]

<u>Szennyezettségmérő:</u>

méréstartomány: 0,2 ... 500 $kBq \cdot cm^{-2}$

energiatartomány: >50 keV béta- és >4 MeV alfa sugárzókra

mért mennyiség: felületi béta-szennyezettség ($Bq \cdot cm^{-2}$)
felületi alfa-szennyezettség ($Bq \cdot cm^{-2}$)
béta aktivitáskoncentráció ($Bq \cdot l^{-1}$)

Az akkumulátoros műszer egyesíti a hordozható dozimetriai és a szennyezettségmérő műszerek funkcióit. A készülék nyakba akasztható hordtáskájában gamma dózis és dózisteljesítmény mérésére szolgál. A táskában a beépített dozimetriai szűrők az érzékenység energiafüggését linearizálják a 60 KeV - 1,5 MeV tartományban.

Hordtáskájából kivéve a műszer automatikusan szennyezettség-mérővé változik. A mérések előtt célszerű a helyszínen háttérsugárzást mérni, amely alapján a műszer háttérlevonást végez. A beállítható üzemmódok a következők:

- összegzett α - β - γ felületi szennyezettség folyamatos keresés,
- felületi β szennyezettség mérés - beállítható sugárminőséggel (90Sr, 204Tl, 14C),
- felületi α indikálás,
- térfogati β koncentráció mérés - beállítható sugárminőséggel (90Sr, 204Tl, 14C),
- 2 perces háttér mérés.

A műszer detektora az SZBT-10 típusú, orosz gyártmányú GM-cső. A készülék 11 μGy/h ± 20 % dózisteljesítmény értéktől felfelé 10 elektródáról 1-re vált, amellyel együtt a mérés elve és a beütésszám-feldolgozás algoritmusa is változik. 11 μGy/h alatti dózisteljesítménynél 180 impulzus beérkezésének idejéből számolja a kijelzett értéket 30 nGy/impulzus állandó hatásfokkal. 11 μGy/h felett 2 másodperces mérési ciklusban egy anódot használva, a nagyfeszültséget 1 ms-onként ki-be kapcsolja, a bekapcsolás után a holtidő korrekciót figyelembe véve az első bejövő impulzusok beérkezési idejének átlagából számítja és jelzi ki a méréseredményt.

Ezzel a kombinált mérési eljárással sikerült a természetes háttérsugárzás mérésére készült nagyérzékenységű magsugárzás detektor detektálási hatásfokát kiterjeszteni a magasabb méréshatár irányában egészen a katasztrófa szintig. Ily módon egyetlen detektor 8-9 nagyságrendet fog át szinte lineárisan.

Külön említést érdemel, hogy a kapcsoló üzemű tápfeszültség alkalmazásával sikerült megvalósítani a GM-cső gerjedés elleni védelmét. Azaz a cső intenzív sugárzási térben nem megy át önkisülési üzemmódba és megtartja üzemképességét, - míg az általunk alkalmazott eljárás hiányában - a GM-cső ilyen esetben köztudottan tönkremenne.

Terepszakaszok sugárszintjének földi felderítése

Az ismeretlen összetételű és/vagy többkomponensű, főként hasadási termékekkel kontaminált terepszakaszok sugárszintjének földi felderítésére Solymosi József és munkatársai egyszerű mérési eljárást fejlesztettek ki, amelyre szabadalmi oltalmat szereztek. [52]

A sugárszint definíciója szerint megegyezik a talaj felszínétől egy méteres magasságban és nyílt elhelyezésben mért dózisteljesítménnyel.

$$P = P\ (1m;\ nyílt\ elhelyezés)$$

Azonban a gyakorlatban soha nem teljesül ez a két feltétel - sem a gyalogos, sem a gépjárművel történő sugárfelderítés alkalmával. Valójában esetben sem biztosítható, hogy a sugárzásmérő műszer a sugárfelderítés ideje alatt a talaj felszínétől egy méteres magasságban és nyílt elhelyezésben legyen. Ezért szükséges egy kalibrációs faktor, a Kgy gyengítési tényező használata.

Gyengítési tényező alatt a talaj felszínétől egy méteres magasságban és nyílt elhelyezésben mért dózisteljesítmény, valamint a sugárzásmérő műszer rendeltetésszerű elhelyezésében mért érték hányadosát értjük. A gyengítési tényező, mint kalibrációs faktor meghatározása ezzel a két méréssel történik.

$$Kgy = P\ (1m;\ nyílt\ elhelyezés)/\ P(Xm;\ adott\ elhelyezés)$$

Tehát a sugárszint értékét a sugárzásmérő műszer rendeltetésszerű elhelyezésében mért dózisteljesítmény és a gyengítési tényező szorzata adja.

A gyengítési tényező értéke erősen függ a mérőműszer elhelyezése mellet a mérendő gammasugárzás energiájától is. Ez utóbbi változó értékű lehet a felderítés során.

Kgy = f (Egamma)

De a hordozójármű saját kontaminációja ugyancsak megváltozhat, amely a kalibrációs feltételektől eltérő háttérként meghamisíthatja a sugárszint mérési adatokat.

A sugárzásmérő szonda - az elterjedten alkalmazott belső elhelyezéstől eltérően - a felderítő gépjárműn kívül kerül elhelyezésre úgy, hogy a szonda és a gépjármű között elhelyezünk a gammasugárzás teljes elnyelődését biztosító, úgynevezett végtelen vastag árnyékoló lemezt. Ezzel kettős előnyös hatást érünk el. Egyfelől kiszűrjük a gépkocsi kontaminációjából eredő saját gamma hátteret. Másfelől pedig a gyengítési tényező állandó értékű lesz, és nem függ a gammasugárzás változó energiájától, sem a mérőműszer elhelyezéstől a gépkocsiban.

Tehát a sugárfelderítés során a gyengítési tényezőnek mindvégig a kalibrált, állandó értékével lehet számolni: Kgy = konstans.

Az ismeretlen összetételű és/vagy többkomponensű, főként hasadási termékekkel kontaminált terepszakaszok sugárszintjének földi felderítésére szolgáló mérőrendszerek megvalósítási lehetőségeit és feltételeit vizsgálta Pintér István: A járműfedélzeti sugárszintmérés elvei és gyakorlati megvalósításuk harctevékenység illetve nukleáris baleset-elhárítás során című doktori (PhD) értekezésében.[53]

A Gamma Műszaki Zrt. sorozatban gyártja az 5. ábrán bemutatott járműfedélzeti ABV felderítő rendszert.

5. ábra. Járműfedélzeti ABV felderítő rendszer [57]

Légi ABV felderítő rendszerek fejlesztése

A légi sugárfelderítés katonai alkalmazásának elsődleges követelménye a gyorsaság és a hajózó állomány távolságvédelme. Hazai feltalálók szabadalma oldotta meg ezt a feladatot:

Eljárás és berendezés ismeretlen összetételű és/vagy több komponensű, főként hasadási termékekkel kontaminált terepszakaszok sugárszintjének légi felderítésére. [54]

Zelenák János és társai a munkájuk során vizsgálták az elveszett vagy az ellopott sugárforrások felkutatása, illetve szennyezett terepszakaszok felderítése során a légi felderítés alkalmazhatóságát. A módszer és az erre kifejlesztett eszköz, a sugárszennyezett terepszakasz teljes körű feltérképezése, illetve pontszerű sugárforrás pozíciójának meghatározása érdekében egy hármas feladatrendszert valósít meg:

1. A terepszennyezés felderítése: nagy kiterjedésű szennyezés feltérképezése során az egyes területek sugárszintjét a repülési magasság, a légköri- és talajviszonyok figyelembevételével számítással meghatározza, amelynek alapjai az alábbiakban látható:

$$P_1 = k_1 \cdot P_h e^{k_2 h}$$

ahol

P_1 = sugárszint, Gy/h,

P_h = h magasságon mért dózisteljesítmény, Gy/h,

h = mérési magasság, m,

K_1 = terepviszony elnyelési faktor (1,7 – 2),

K_2 =légkör elnyelési faktor (0,007 - 0,012).

A magassági gyengítési tényezőknek a fenti összefüggéssel való közelítése figyelembe veszi különböző terep- és légköri elnyelési viszonyokat és gyakorlatban végrehajtott, nagyszámú méréssel alá lett támasztva [55][56]. Ezen értékek összhangban vannak a NATO STANAG 2112 által ajánlott gyengítési tényező (AGRCF) értékeivel, valamint a régebbi, már nehezen fellelhető szovjet irodalomban található összefüggésekkel, de ami a legfontosabb, terepviszony és légkör elnyelési faktoroktól függetlenül, 100 m-es repülési magasság alatt 10-25 %-os relatív hibán belül közelíti a terepen, gyalogosan mért sugárszint értékeket.

2. Pontszerű radioaktív források behatárolása: a háttérsugárzástól szignifikánsan eltérő pontok indikálásával meghatározza a források földrajzi koordinátáit. Nagy aktivitású forrás esetén dózisteljesítmény konverzió is alkalmazható a mérések végrehajtására, az alábbi összefüggéssel [55]:

$$P_1 = k_3 \cdot P_h h^{k_4}$$

ahol:

P_1 = a forrástól 1 méterre mért dózisteljesítmény, Gy/h,

P_h = h magasságon mért dózisteljesítmény, Gy/h,

h = mérési magasság, m,

K_3 = terepviszony elnyelési faktor (1 –1,18),

K_4 =légkör elnyelési faktor (2 –2,4).

Kis aktivitású források esetén nagy hatásfokú üreges szcintillációs detektorral végzett beütésszámlálással lehet nagy pontossággal meghatározni egy forrás pozícióját, az adott módszer az irodalomban jól le van írva [56]. Igaz, kis aktivitások esetén, kis magasságokon (40-60 m) végzett repülésekkel a detektálható aktivitások az alsó korlátja mintegy 500 kBq – 1 MBq.

3. Radioaktív izotópok azonosítása. Energia-szelektív mérésekkel támpontot nyújtani a radioaktív szennyezettség összetételének becsléséhez. Itt azonban meg kell jegyeznünk, hogy a repülési magasságon történő méréseknél egyrészt a levegőréteg gyengítése, másrészt az intenzív Compton-szórás jelentős mértékben csökkent ezt a képességet.

A Gamma Műszaki Zrt. ipari kivitelben gyártja a RABV (6. ábra bal oldala) sugárfelderítő rendszert UAV-ra, valamint a LABV Légi ABV-felderítő rendszert (6. ábra jobb oldala), mint harci helikopterre telepített változatot.

6. ábra. LABV Légi ABV felderítő rendszer [57]

A légi sugárfelderítő rendszer korszerűsített változata alkalmas az elveszett vagy ellopott radioaktív sugárforrások felkutatására is, pontosság tekintetében pedig egyenértékű a földi felderítéssel.

A modern légi sugárfelderítés új eszköz- és eljárásrendjének előnyei az alábbiakban foglalhatók össze:

- a konténerbe épített rendszer környezeti hatásokkal szembeni állékonysága megfelelő;
- a konténer gyorsan, könnyen szerelhető a helikopterre;
- a rendszer pontszerű és kiterjedt sugárforrások felderítésére egyaránt alkalmas;
- a négycsatornás spektrometria támpontot nyújt az izotópazonosításhoz;
- A felderítések során az idő-, hely- és magasság koordináták hiánytalanul rögzítésre kerülnek,
- a repülés útvonala digitális térképen pontosan jelenik meg;
- a felvételek rendben archiválódnak, visszajátszhatók, kiértékelhetők;
- a mérési eredmények reálisak, pontosságuk a földi rendszerekével egyenértékű;
- Az on-line adattovábbítás digitális adatrádió segítségével történik.

A mérési eljárás és az adatok kiértékelése térinformatikai platformon történik, aminek a feltételei az alábbiak szerint teljesülnek:

- a GPS magasságmérés korrekciója a DDM-50 digitális domborzati modell és a barometrikus magasságmérő adatai segítségével történik;
- digitális térkép használata: az adatfeldolgozó szoftver teljes körűen kezeli a DTA-50-es térképészeti adatbázist;
- a felderítési adatok memóriakártyára íródnak;
- a mérési eredmények megjelenítése NATO szabvány szerinti térképi jelekkel, jelzésekkel történik.

A légi sugárfelderítés fenti új eszköz- és eljárásrendjének a rendszerbe állítása mérföldköves előrelépés a vegyivédelmi csapatok képességeiben.

Sugárvédelmi kutatások áttekintése

Az eddigiekben itt bemutatott sugárzásmérési eljárások és eszközök összességének az elméleti és gyakorlati ismereteit, valamint a megvalósított alkotások alapját képező szabadalmakat együttesen tartalmazó egyetemi tankönyvben foglalták össze: Erdős József, Pintér István, Solymosi József: Magyar ABV védelmi technikai almanach. [57]

Csurgai és társai az ABV (NBC) anyagok terjedését vizsgálták szimuláció segítségével. [59]

Csécs és társai az ABV (NBC) anyagok terjedését vizsgálták az akkor legszélesebb körben alkalmazott, korszerű FLUENT numerikus áramlástani szimulációs kód segítségével, hogy megállapíthassák, milyen mértékben alkalmas a légáramlással együttmozgó anyagok terjedésének leírására zárt terekben. [60]

Kiss Enikő és társai olyan eljárás kidolgozásán dolgoznak, ami a sugárérzékenység kimutatására alkalmas lehet. Ezt az eljárást alkalmazni lehetne a sugárkezelésre váró betegek körében is. Eredményeik nagy haszonnal járhatnak, így érdemes figyelemmel kísérni azokat. [61]

Vincze Árpád és társai egy esetlegesen a Paksi Atomerőműben történő, radioaktív vizet szállító cső lyukadásának környezeti hatásait vizsgálták. [62]

Rónaky József és társai egy cikk-sorozat keretében a nukleáris létesítmények katonai terror-fenyegetettségének értékelését vizsgálták, mely során áttekintették a nemzetközi és hazai szabályozást és gyakorlatot, majd ezek alapján kidolgozták a Paksi Atomerőmű katonai terror-fenyegetettségének értékelési eljárását. [63][64] Vizsgálták a 2. számú akna balesetét és a dekontaminálás ellenőrzését. [65][66]

Petőfi Gábor és társai kutatásuk során megvizsgálták a nukleárisbaleset-elhárítási követelmények fejlődését. A későbbiekben ez alapján tettek javaslatot a jogszabályok fejlesztésére. [67]

Rónaky József és társa 2007-ben elsőként tett közzé részletes elemzést a hazai sugárvédelmi, biztosítéki, nukleáris biztonsági, és nukleáris veszélyhelyzeti felkészülési jogkörök egyesítéséről. [68] A Katonai Műszaki Tudományok doktori PhD értekezésében már akkor tudományosan megalapozott tézisként deklarálta a hatósági jogkörök egyesítése jogi szabályozásának potenciális lehetőset. [69]

Sebestyén Zsolt a leszerelés és a környezeti remediációs programok globális végrehajtásának a fejlődése témakörökkel foglalkozó nemzetközi konferencián beszámolt a magyarországi szabályozási rendszer változásairól, a radioaktívhulladék-tárolók és a sugárvédelmi felügyeleti feladatok változásáról. [70]

Lucas Grégory és társai arról számoltak be, hogy miként kívánják kutatni a kontaminált talaj radioaktivitásának mérési módszereit, légi távérzékelési rendszerek alkalmazásával. Megvizsgálták, hogyan lehetne integrálni a nukleáris felismerő rendszerekbe alternatív technológiákat (hiperspekrális, termális, LiDAR), illetve melyek lennének a hozzáadott értékek. [71][72][73][74]

A cikk bemutatja a környezet kármentési terv automatikus előkészítésére és a nehéz gépezetek pontos utasításához szükséges irányítási adatokhoz végzett kutatást egy ipari katasztrófát követően végzett tisztítási munkák során. A bemeneti vizsgálati adatok a kolontári vörös iszap katasztrófánál, a hiperspektrális légi felmérési adatok feldolgozásából származtatott szennyezés kiterjedésének shape fájlja volt.

2010 október 4-én Magyarország története során az egyik legnagyobb környezeti katasztrófa következett be, amikor egy mérgező hulladék tároló medencéjének sérülése következtében 600.000 - 700.000 m^3 vörösiszap és víz jutott ki a környezetbe. 10 ember meghalt és 120 ember sérült meg. A vörösiszap 4 km^2-nyi területet árasztott el.

Az ötlet, ami motiválta a kutatómunkát, a kolontári szennyezett területen végzett tisztítási munkát követően fogalmazódott meg. Míg a szennyezett terület körvonalát a digitális térképek mutatták és a környezetszennyezés vastagsága rendelkezésre állt, addig az ásatási munkák a hagyományos módon zajlottak, helyzetmeghatározás és navigációs technológia nélkül. Tehát a pontos és részletes információk már a helyreállítási folyamat korai szakaszában rendelkezésre álltak, ugyanakkor azok kihasználása nem volt hatékony.

Tágabb összefüggésben, a kutatási munkánk olyan módszerek és eszközök fejlesztését célozta meg, amelyek a geográfiai információk kihasználásának/támogatásának folytonosságán keresztül egy pontos helyreállítási folyamatot biztosítanak. A katasztrófa értékelési szakasz során gyűjtött GI-t a tervezési fázisban kellene alkalmazni és használni; ez

gondoskodhatna a tisztítási fázis terveiről és navigációs adatairól. Emellett a következőket is célszerű lenne kutatni: technológiák integrálása (távérzékelés (detektálás), GIS (tervezés), helymeghatározás és navigáció (tisztítás)).

A kutatás eredménye, hogy az optimális irány megállapításával munkát, időt és pénzt spórolhatunk meg a kármentesítés során.

A légi távérzékelési rendszerek (hiperspekrális, termális, LiDAR) felhasználása alkalmas lehet a talaj radioaktivitásának feltérképezésére, egyben a remediáció alakulásának a szakaszos nyomon követésére több, a kontaminált terület fölött, egymást követően eltérő időben végrehajtott pásztázó repüléssel.

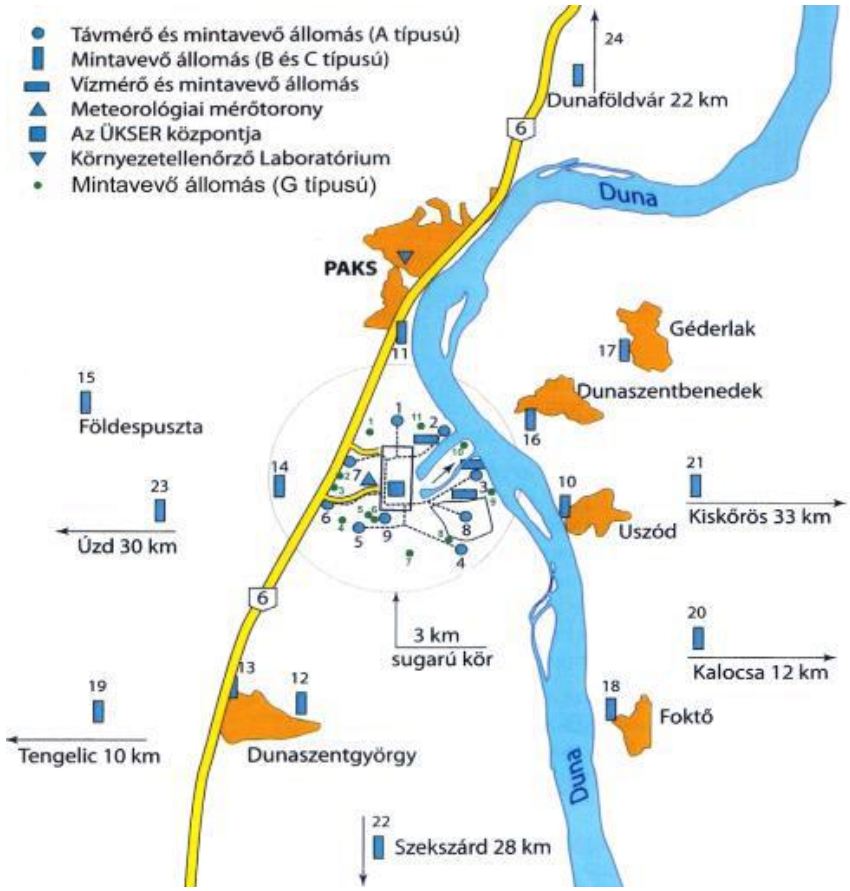
A fenti légi távérzékelési rendszerek, mint alternatív technológiák, a jövőben alkalmasak lehetnek a nukleáris létesítmények leszerelését követően a környezeti remediáció felmérésére gyors és átfogó módon, továbbá a változások időszakos nyomon követésére.

Bujtás Tibor és társai a Paksi Atomerőmű Környezetellenőrző Laboratóriuma mintavételi adatbázisának korszerűsítésének eredményeiről számoltak be.[75]

Az erőmű környezeti sugárvédelmi ellenőrzésének feladata és célja hogy közvetlen mérésekkel bizonyítsa, az erőmű normál üzemben radioaktív izotópokkal, illetve sugárzásukkal kevésbé terheli a környezetet, mint az elfogadhatónak megállapított érték. További feladata, hogy – elsősorban az üzemi területen végzett méréseivel – hozzájáruljon a környezetet veszélyeztető technológiai rendellenességek feltárásához, kiküszöbölésük után pedig ellenőrizze a környezetveszélyeztetés megszűnését. Végül, egy esetleges üzemzavar környezeti következményeinek megítéléséhez, a lakosságot érintő beavatkozások megalapozásához a környezet sugárzási állapotáról gyorsan, megbízható adatokat szolgáltasson.

A radioaktív anyagok kibocsátásának, valamint a környezet radioaktív terhelésének ellenőrzése céljából a Paksi Atomerőmű (PAE) egy széleskörűen kiépített üzemi kibocsátás- és környezeti sugárvédelmi ellenőrző rendszert (ÜKSER) üzemeltet. A rendszert egyrészt távmérő hálózatok, másrészt laboratóriumi mintavételes vizsgálatok alkotják.

A telepített kibocsátás és környezeti sugárvédelmi ellenőrző rendszer (KKSER) egy szűkebb részét a környezeti A és B típusú levegőmonitoring távmérő állomások hálózata, a G típusú dózisteljesítményt mérő állomások hálózata, a V típusú vízmintavételeket ellátó állomások hálózata továbbá a meteorológiai mérőtorony – röviden környezetellenőrző hálózat – képezi (7. ábra).[76]



7. ábra. A mintavevő és a távmérő állomások elhelyezkedése a Paksi Atomerőmű körül [76]

A környezetellenőrző hálózat érzékelői kereken 100 különböző sugárzási és meteorológiai paraméterről szolgáltatnak folyamatosan, 10 perces mérési időciklusokban információt. A távmérő állomások aktív és passzív mintavevő egységekkel is fel vannak szerelve, melyek folyamatos mintavételt végeznek a különböző környezeti közegekből laboratóriumi vizsgálatok céljára.

ÖSSZEGZÉS

Közleményünkben részletes irodalmi értékelő áttekintést adtunk a sugárvédelmi eljárások és műszerek fontosabb hazai kutatási-fejlesztési és innovációs eredményeiről, különösen a nukleárisbaleset-elhárítás érdekében.

Az adott témakörben a katonai műszaki tudományos szemléletnek megfelelően feltétlenül foglalkoznunk kell a lakossági sugárvédelem mellett, az annak a biztosítása érdekében tevékenykedő, első beavatkozó állomány megfelelő védelméről is. Nevezetesen a mentő egységek, a Magyar Honvédség, a Katasztrófavédelem, a mentők, a rendészeti személyzet megfelelő sugárvédelme rendkívül fontos feladat. Ezekre a feladatokra kiválóan alkalmasnak bizonyultak az itt bemutatott hazai fejlesztésű eszköz- és eljárási rendszerek.

A következőkben felsorolt korszerű új mérési eljárások kerültek kifejlesztésre:

- a maghasadás radioaktív (hasadási) termékeinek kormeghatározására,
- a bétasugárzó radionuklidokkal kontaminált felületi szennyezettség és (térfogati) radioaktív koncentráció egyszerű, gyors meghatározására,
- az intenzív gamma-háttérsugárzásban történő béta-sugárzás mérése során a jel/zaj viszony javítására energiakompenzációs módszerrel,

- univerzális radioaktív sugárzásmérő műszer GM-csövek méréshatárának kiterjesztésére, ahol a 10 anódos GM-csövet használva kapcsolt anódokkal, és impulzusüzemű algoritmussal egyetlen detektor 8-9 nagyságrendet fog át szinte lineárisan,
- terepszakaszok sugárszintjének földi felderítése,
- légi ABV felderítő rendszerek.

A hazai feltalálók alkotásait szabadalmi oltalomban részesítették. Tudományos közlemények és PhD értekezések is születtek belőlük a katonai műszaki tudományok tudományágban.

Az eljárásokat jelentősen továbbfejlesztették, növelték a mérési pontosságot, és intelligens mérőrendszereket fejlesztettek ki, amelyeknél a mérési adatok kiértékelése térinformatikai platformon történik.

A sugárvédelmi mérőműszereket és rendszereket a Gamma Műszaki Zrt. napjainkban is sorozatban gyártja, és kiterjedten értékesíti itthon és a világ számos országában.

A Paksi Atomerőmű környezetellenőrzési eljárásainak és eszközeinek a fejlesztése a lakosság sugárvédelmének egyre megbízhatóbb megvalósítását szolgálják.

Összegezetten kimondhatjuk, hogy a hazai sugárvédelem eljárás- és eszközrendszere világszínvonalon működik. Ezt tanúsítják a rendszeres NAÜ és a Nukleáris Üzemeltetők Világszövetsége[3] által végrehajtott nemzetközi ellenőrzések is.

Új távlatokat nyit meg a légi távérzékelési rendszerek (hiperspekrális, termális, LiDAR) felhasználása a talaj radioaktivitásának feltérképezésére, egyben a remediáció alakulásának a szakaszos nyomon követésére több, a kontaminált terület fölött, egymást követően eltérő időben végrehajtott pásztázó repüléssel. Ezek a légi távérzékelési rendszerek, mint alternatív technológiák, a jövőben alkalmasak lehetnek a nukleáris létesítmények leszerelését követően a környezeti remediáció felmérésére gyors és átfogó módon, továbbá a változások időszakos nyomon követésére.

További kutatások-fejlesztések szükségesek a legújabb lehetőségek feltárására – mind a műszaki megoldások, mind pedig a jogi szabályozás ésszerű korszerűsítése terén egyaránt.

Felhasznált irodalom

[1] Csurgai J., Sebestyén Zs.; Nukleáris létesítmények telephely-vizsgálatának és radiológiai értékelésének módszertana korszerűsítési lehetőségének kutatása-fejlesztése; Hadmérnök; XI. Évfolyam 3. szám; pp 44-56.; 2016. szeptember

[2] 2015. évi VII. törvény a Paksi Atomerőmű kapacitásának fenntartásával kapcsolatos beruházásról, valamint az ezzel kapcsolatos egyes törvények módosításáról

[3] Az 1996. évi CXVI. törvény az atomenergiáról

[4] A Tanács 2013/59/EURATOM irányelve az ionizáló sugárzás okozta sugárterhelésből származó veszélyekkel szembeni védelmet szolgáló alapvető biztonsági előírások megállapításáról, valamint a 89/618/Euratom, a 90/641/Euratom, a 96/29/Euratom, a 97/43/Euratom és a 2003/122/Euratom irányelv hatályon kívül helyezéséről

[5] International Atomic Energy Agency, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards; General Safety Requirements Part 3; No. GSR Part 3, IAEA, Vienna (2014).

[6] 118/2011.(VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről

[3] World Association of Nuclear Operators, WANO

[7] Nukleáris Biztonsági Szabályzatok
1. melléklet: Nukleáris létesítmények nukleáris biztonsági hatósági eljárásai
2. melléklet: Nukleáris létesítmények irányítási rendszerei
3. melléklet: Üzemelő atomerőművek tervezési követelményei
3a. melléklet: Új atomerőművi blokkok tervezési követelményei
4. melléklet: Atomerőművek üzemeltetése
5. melléklet: Kutatóreaktorok tervezése és üzemeltetése
6. melléklet: Kiégett nukleáris üzemanyag átmeneti tárolása
7. melléklet: Nukleáris létesítmények telephelyének vizsgálata és értékelése
8. melléklet: Nukleáris létesítmények megszüntetése
9. melléklet: Új nukleáris létesítmény tervezési és létesítési időszakára vonatkozó követelmények
10. melléklet: Nukleáris Biztonsági Szabályzatok meghatározásai

[8] 155/2014. (VI. 30.) Korm. rendelet a radioaktív hulladékok átmeneti tárolását vagy végleges elhelyezését biztosító tároló létesítmények biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről

[9] 487/2015. (XII. 30.) Korm. rendelet az ionizáló sugárzás elleni védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

[10] 16/2000. (VI. 8.) EüM rendelet az atomenergiáról szóló 1996. évi CXVI. törvény egyes rendelkezéseinek végrehajtásáról

[11] 489/2015. (XII.30.) Korm. rendelet a lakosság természetes és mesterséges eredetű sugárterhelését meghatározó környezeti sugárzási helyzet ellenőrzési rendjéről és a kötelezően mérendő mennyiségek köréről

[12] 490/2015. (XII.30.) Korm. rendelet a hiányzó, a talált, valamint a lefoglalt nukleáris és más radioaktív anyagokkal kapcsolatos bejelentésekről és intézkedésekről, továbbá a nukleáris és más radioaktív anyagokkal kapcsolatos egyéb bejelentést követő intézkedésekről

[13] 112/2011.(VII. 4.) Korm. rendelet az Országos Atomenergia Hivatal nukleáris energiával kapcsolatos európai uniós, valamint nemzetközi kötelezettségével összefüggő feladatköréről, az Országos Atomenergia Hivatal hatósági eljárásaiban közreműködő szakhatóságok kijelöléséről, a kiszabható bírság mértékéről, valamint az Országos Atomenergia Hivatal munkáját segítő tudományos tanácsról

[14] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

[15] 246/2011.(XI. 24.) Korm. rendelet a nukleáris létesítmény és a radioaktívhulladék-tároló biztonsági övezetéről

[16] 247/2011.(XI. 25.) Korm. rendelet az atomenergia alkalmazása körében eljáró független műszaki szakértőről

[17] 167/2010.(V. 11.) Korm. rendelet az országos nukleárisbaleset-elhárítási rendszerről

[18] 146/2014 (V.5.) Korm. rendelet a felvonókról, a mozgólépcsőkről és a mozgójárdákról

[19] 215/2013. (VI. 21.) Korm. rendelet a radioaktív hulladékokkal és a kiégett üzemanyaggal kapcsolatos egyes feladatokat ellátó szerv kijelöléséről, tevékenységéről és annak pénzügyi forrásairól

[20] 15/2001. (VI. 6.) KöM rendelet az atomenergia alkalmazása során a levegőbe és vízbe történő radioaktív kibocsátásokról és azok ellenőrzéséről

[21] 5/2015. (II. 27.) BM rendelet az atomenergia alkalmazásával kapcsolatos sajátos tűzvédelmi követelményekről és a hatóságok tevékenysége során azok érvényesítésének módjáról

[22] 55/2012. (IX. 17.) NFM rendelet a nukleáris létesítményben foglalkoztatott munkavállalók speciális szakmai képzéséről, továbbképzéséről és az atomenergia alkalmazásával összefüggő tevékenységek folytatására jogosultak köréről

[23] 108/2001. (XII. 23.) FVM-GM rendelet a felvonók biztonsági követelményeiről és megfelelőségének tanúsításáról

[24] 165/2003. (X. 18.) Korm. rendelet a nukleáris és radiológiai veszélyhelyzet esetén végzett lakossági tájékoztatás rendjéről

[25] 4/2016. (III. 5.) NFM rendelet az Országos Atomenergia Hivatal egyes közigazgatási eljárásaiért és igazgatási jellegű szolgáltatásaiért fizetendő díjakról

[26] 31/2001. (X. 3.) EüM rendelet az egészségügyi szolgáltatások nyújtása során ionizáló sugárzásnak kitett személyek egészségének védelméről

[27] 47/2003. (VIII. 8.) ESzCsM rendelet a radioaktív hulladékok átmeneti tárolásának és végleges elhelyezésének egyes kérdéseiről, valamint az ipari tevékenységek során bedúsuló, a természetben előforduló radioaktív anyagok sugár-egészségügyi kérdéseiről

[28] 1987. évi 8. tvr. a nukleáris anyagok fizikai védelméről szóló egyezmény kihirdetéséről

[29] 2007. évi XX. törvény a nukleáris terrorcselekmények visszaszorításáról szóló nemzetközi Egyezmény kihirdetéséről

[30] 2008. évi LXII. törvény a Nemzetközi Atomenergia Ügynökség (NAÜ) keretében 1979-ben elfogadott, és az 1987. évi 8. törvényerejű rendelettel kihirdetett nukleáris anyagok fizikai védelméről szóló Egyezménynek a NAÜ által szervezett diplomáciai konferencia keretében, 2005. július 8-án aláírt módosítása kihirdetéséről

[31] 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról

[32] 190/2011.(IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

[33] 47/2012.(X. 4.) BM rendelet az atomenergia alkalmazásával összefüggő rendőrségi feladatokról

[34] 7/2007(III.6.) IRM rendelet a nukleáris anyagok nyilvántartásának és ellenőrzésének szabályairól

[35] 11/2010.(III. 4.) KHEM rendelet a radioaktív anyagok nyilvántartásának és ellenőrzésének rendjéről, valamint a kapcsolódó adatszolgáltatásról

[36] A Nemzetközi Atomenergia Ügynökség nukleáris védettségre vonatkozó ajánlásai (Nuclear Security Series Publications)

[37] 213/2013. (VI. 21.) Korm. rendelet a Központi Nukleáris Pénzügyi Alap Szakbizottságról

[38] 214/2013. (VI. 21.) Korm. rendelet a Központi Nukleáris Pénzügyi Alapból az ellenőrzési és információs célú önkormányzati társulásoknak nyújtott támogatások szabályairól

[39] Solymosi J, Tömör J, Gaál L: Eljárás és berendezés atomrobbantások radioaktív termékei által az élő szervezetre gyakorolt sugárveszély mértékének a termékek életkora alapján történő értékelésére Lajstromszám: 177 623.

[40] J Solymosi, P Zagyvai, L Gy Nagy: Dosimetric measurement of the disintegration rate of fission products Journal of Radioanalytical and Nuclear Chemistry - Articles 162:(1) pp. 187-198. (1992)

[41] J Csurgai, Á Vincze, J Solymosi, P Zagyvai; Application of an iterative method for dose prognosis of fission products with unknown composition; ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 2:(1) pp. 59-64. (2003)

[42] Csurgai J.: A Magyar Honvédségben alkalmazott sugárhelyzet prognosztizálási és értékelési eljárások továbbfejlesztése számítógépes megvalósítással; HADITECHNIKA 34:(1) pp. 6-12. (2000)

[43] Csurgai J.: Nukleárisbaleset-elhárítás és vegyi katasztrófák összefüggésrendszerének tudományos vizsgálata: doktori (PhD) értekezés, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest 2003. http://ludita.uni-nke.hu/repozitorium/handle/11410/9508 (2015.09.10.)

[44] Solymosi J, Baumler E, Gresits I, Gujgiczer Á, Németh F, Nagy L Gy, Horváth L, Sarkadi A: Eljárás és kapcsolódási elrendezés radioaktív felületi szennyeződés mérésére. Lajstromszám: 201 162.

[45] Solymosi J, Bäumler E, Nagy L Gy, Gresits I, Gujgiczer Á, Sarkadi A, Kőrösi S, Dorogi L, Vodicska M: Eljárás és berendezés béta-sugárzó izotópo(ka)t tartalmazó minta aktivitásának mérésére nagy intenzitású gamma-sugárzási háttérben Magyar Szabadalom 200 001 (1990)

[46] Solymosi J, Zagyvai P, Nagy L Gy: Determination of the radioactive bulk and surface concentration by beta detection I. Journal of Radioanalical and Nuclear Chemistry 209:(1) pp. 3-14. (1996)

[47] Solymosi J, Zagyvai P, Nagy L Gy: Determination of the radioactive bulk and surface concentration by beta detection II. Journal of Radioanalical and Nuclear Chemistry 209:(1) pp. 15-26. (1996)

[48] Solymosi J, Zagyvai P, Nagy L Gy: Determination of the radioactive bulk and surface concentration by beta detection III. Journal of Radioanalical and Nuclear Chemistry 209:(1) pp. 27-39. (1996)

[49] Baumler E., Erdős K., Pintér I., Sarkadi A., Gujgiczer Á., Solymosi J., Németh F., Nagy L., Plachtovics Gy., Illés Zs., Szabó E.: Univerzális radioaktív sugárzásmérő műszer és eljárás, valamint rendszertechnikai elrendezés a méréshatárának kiterjesztésére Lajstromszám: 224 502.

[50] Solymosi J, Baumler E, Sarkadi A, Gujgiczer Á, Pintér I, Vincze Á: Wide range universal radiation measuring instrument. Academic and Applied Research in Military Science 1:(1) pp. 133-144. (2002) http://zmne.hu/aarms/docs/Volume1/Issue1/pdf/10soly.pdf (2016. 08. 03.)

[51] Baumler E., Sarkadi A., Erdős K., Solymosi J., Gujgiczer Á., Illés Zs., Simoncsis L., Plachtovics Gy.: Magsugárzás-detektorok méréshatárának kiterjesztése MAGYAR KÉMIAI FOLYÓIRAT 103:(9) pp. 462-469. (1997)

[52] Solymosi J., Nagy L., Zagyvai P. , Gresits I., Gujgiczer Á. , Vajda N. , Dorogi L., Vodicska M., Takács M.: Eljárás és berendezés ismeretlen összetételű és/vagy

többkomponensű, főként hasadási termékekkel kontaminált terepszakaszok sugárszintjének földi felderítésére
Magyar Szabadalom Lajstromszám: 198 798

[53] Pintér I: A járműfedélzeti sugárszintmérés elvei és gyakorlati megvalósításuk harctevékenység illetve nukleáris baleset-elhárítás során, Doktori (PhD) értekezés, ZMNE 2002. Link: http://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9866/Teljes%20sz%C3%B6veg!?sequence=1&isAllowed=y (letöltve: 2015.09.10.)

[54] Solymosi J, Bäumler E, Nagy L Gy, Zagyvai P, Gresits I, Gujgiczer Á, Dorogi L, Takács M, Vajda N, Vodicska M: Eljárás és berendezés ismeretlen összetételű és/vagy több komponensű, főként hasadási termékekkel kontaminált terepszakaszok sugárszintjének légi felderítésére Magyar Szabadalom Lajstromszám: 201 161 (1990)

[55] Solymosi József: Korszerű sugárvédelmi mérőrendszerek I.-II. – Haditechnika 1994/2, 1994/3. sz.

[56] Zelenák J., Csurgai J., Halász L., Solymosi J., Vincze Á.; A légi sugárfelderítés képességei alkalmazhatóságának vizsgálata elveszett vagy ellopott sugárforrások felkutatása, illetve szennyezett terepszakaszok felderítése során; HADMÉRNÖK 4:(1) pp. 46-62. (2009) http://hadmernok.hu/2009_1_zelenak.pdf 2016. 08. 03.

[57] Erdős J., Pintér I., Solymosi J.: Magyar ABV védelmi technikai almanach Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest 2003. 285 p.

[58] Gamma Műszaki Zrt., Termékek, Sugárzásmérő műszerek; http://www.gammatech.hu/?mnuGrp=mnuProducts&module=products&lang=hun&group=sugarzasmero&menupath=sugarzasmero-&csoport=Sug%C3%A1rz%C3%A1sm%C3%A9r%C5%91%20m%C5%B1szerek 2016. 08. 03.

[59] Csurgai J, Zelenák J, Lajos T, Goricsán I, Halász L, Vincze Á, Solymosi J; Numerical simulation of transmission of NBC materials; ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 5:(3) pp. 417-434. (2006)

[60] Á Csécs, J Csurgai, J M Suda, G Kristóf, I Pintér, J Zelenák; ABV (NBC) anyagok épületen belül történő terjedésének numerikus szimulációja és modellkísérleteBOLYAI SZEMLE 13:(3) pp. 1416-1443. (2004)

[61] Kiss E., Sáfrány G., Solymosi J.; A sugárérzékenység vizsgálatának katasztrófavédelmi jelentősége; HADMÉRNÖK VIII. (4.): pp. 104-112. (2013)

[62] Á. Vincze, T. Ranga, G. Nagy, O. Zsille, J. Solymosi: Environmental impact assessment of radioactive water pipe leakage at NPP Paks PERIODICA POLYTECHNICA-ELECTRICAL ENGINEERING 53:(2) pp. 87-91. (2009)

[63] Rónaky J, Macsuga G, Volent G, Csurgai J, Cziva O, Horváth K, Petőfi G, Vincze Á, Zelenák J, Solymosi J: A nukleáris létesítmények katonai terror-fenyegetettségének értékelése I.: A nemzetközi és hazai szabályozás, valamint a gyakorlat áttekintése, Hadmérnök II:(1) pp. 77-85. (2007) Link: http://www.hadmernok.hu/archivum/2007/1/2007_1_ronaky.pdf (letöltve: 2015.09.09.)

[64] Rónaky J, Petőfi G, Volent G, Macsuga G, Horváth K, Csurgai J, Cziva O, Molnár L, Tóth J, Vincze Á, Zelenák J, Solymosi J: A nukleáris létesítmények katonai terror-fenyegetettségének értékelése II.: A Paksi Atomerőmű katonai terror-

fenyegetettségének értékelési eljárása, Hadmérnök II :(2) pp. 32-49. (2007) http://www.hadmernok.hu/archivum/2007/2/2007_2_ronaky.pdf (2015.09.09.)

[65] K Horváth, J Rónaky, J Solymosi; Determination of the root cause of the serious incident at Paks NPP on 10 April 2003; ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 4:(3) pp. 481-496. (2005)

[66] Tibor B., Á. Nényei, J. Solymosi; Raditation protection aspects of the accident recovery ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 5:(4) pp. 557-568. (2006)

[67] Petőfi G., Rónaky J., Solymosi J.: A nukleárisbaleset-elhárítási követelmények fejlődése HADMÉRNÖK II:(1) pp. 58-64. (2007)

[68] Rónaky József, Horváth Kristóf, Szabó Szilárd, Solymosi József; Nukleáris non-proliferáció HADMÉRNÖK 1:(3) pp. 4-16. (2006)

[69] Rónaky J., Solymosi J.; Elemzés a hazai sugárvédelmi, biztosítéki, nukleáris biztonsági, és nukleáris veszélyhelyzeti felkészülési jogkörök egyesítéséről; HADMÉRNÖK II:(1) pp. 86-123. (2007)

[70] Zs. Sebestyén; ID143 Modification of the Hungarian regulatory system related to the oversight transfer; Poster; International Conference on Advancing the Global Implementation of Decommissioning and Environmental Remediation Programmes; Madrid, Spain; 23–27 May 2016; URL.: http://www-ub.iaea.org/MTCD/Meetings/PDFplus/2016/cn238/cn238FinalProgramme.pdf 201610.14.

[71] Lucas Grégory, Halász L., Solymosi J.: Exploring the capacities of airborne technology for the disaster assessment, HADMÉRNÖK 8: (3) pp. 74-91. (2013)

[72] Grégory Lucas, Solymosi J., Lénart Cs.: Using hyperspectral imaging in nuclear radiation aerial reconnaissance?, REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK (1997-TŐL) 25: (2) pp. 644-656. (2013)
[67]Lucas Grégory, Lénárt Csaba, Solymosi József: Development and testing of geo-processing models for the automatic generation of remediation plan and navigation data to use in industrial disaster remediation, INTERNATIONAL ARCHIVES OF PHOTOGRAMMETRY AND REMOTE SENSING (2002-) XL-3: (W3) pp. 195-201. (2015)

[73] Lucas Grégory, Solymosi J.: Preliminary study on the detection of radioactivity with airborne remote sensing systems, HADMÉRNÖK 10: (3) pp. 137-155. (2015)

[74] Lucas Grégory, Solymosi József, Lénárt Csaba: Development and testing of geo-processing models for the automatic generation of remediation plan and navigation data to use in industrial disaster remediation, US OPEN GEOGRAPHIC INFORMATION SYSTEM JOURNAL 1: pp. 1-13. pp. 1-13. (2016)

[75] Bujtás T., Manga L., Nagy G., Solymosi J.: A paksi atomerőmű környezetellenőrző laboratóriuma mintavételi adatbázisának korszerűsítése, HADMÉRNÖK X.: (1.) pp. 161-173.

[76] Bardon J., Daróczi L., Kapás P., Lencsés A., Manga L., Végh G.: Nukleáris Környezetvédelem 2013, pp. 40-42. in: Dr. Bujtás Tibor (szerk.): MVM Paksi Atomerőmű Zrt, Biztonsági Igazgatóság, Sugár- és Környezetvédelmi Főosztály: Sugárvédelmi Tevékenység a Paksi Atomerőműben 2013-ban, (belső kiadvány)

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Lajos KÁTAI-URBÁN

katai.lajos@uni-nke.hu

ASSESSMENT OF THE AUTHORITY EXPERIENCES RELATED TO THE SUPERVISION OF DANGEROUS GOODS TRANSPORTATION

Absztrakt

The development of the Hungarian system of industrial safety has more than 15-year's history. The aim of this article to overview the measures related to the development of the legislative area for industrial safety in the field of dangerous goods transportation and draw the potential experiences from this progress.

Az iparbiztonsági szabályozásnak a katasztrófavédelem rendszerében történő fejlődése több mint 15 évre tekint vissza Magyarországon. Jelen cikk célja áttekintést adni az iparbiztonsági jogterület veszélyes szállítmányok felügyeletével kapcsolatos fejlődési intézkedéseiről és levonni a fejlődésben rejlő hatósági és szakmai tapasztalatokat.

Keywords: *industrial safety; transport accidents; transportation of dangerous goods; disaster management ~ iparbiztonság, szállítási balesetek, veszélyes áru szállítás, katasztrófavédelem*

INTRODUCTION

Hungary's geographical location is very favourable and has an important role in the transportation to and from the eastern and southern countries. As a result of this, transit shipments are also significant in addition to the domestic transportation, therefore transport infrastructure has a very important role in our country.

Transportation of dangerous goods is happening mostly on road but is getting more and more popular on railways, inland waterways and by air as well. International rules and regulations by the European Union of the different transportation methods have been integrated into the Hungarian legislation. EU regulations based on the international convention about the transportation of dangerous goods has been implemented to the Hungarian law system around the millennium. [1] Disaster management authority has gained significant enforcement experiences on inspecting the transportation of dangerous goods.

The authors have made a brief historical review and technical analysis on the supervision of the transportation of dangerous shipments in their previous articles, especially on the changes in law and the strengthening of the legal institution. In this article the experiences of the implementing measures on the supervision of dangerous goods will be analysed.

ANALYSIS OF THE LAW ENFORCEMENT EXPERIENCES ON SUPERVISION OF DANGEROUS SHIPMENTS 2001-2011

Disaster management is involved in the designation process of the routes of transportation and the inspection of vehicles on these routes since 18th June, 2001. The number of route designations is between 600-800 decisions per year which decisions arrived to the bodies in standby of disaster management. The number of announcements have increased along with the intensity of control. Although good standing was not unified among the entities. The system was hardly working due to the lack of central database and electronic (via internet) announcements.

Regional bodies of the National Directorate General for Disaster Management, Ministry of Interior (NDGDM, MoI), the National Transport Authority, the law enforcement and the customs administration have done the inspections together and also separately between 2001 and 2011. The bodies in concern do the inspections on transportation of dangerous goods based on the so-called Guide for Complex Control and Fine since 2010. [2]

The number of controls on transportation of dangerous goods on road doubled between 2002 and 2005. Income from the fines also increased significantly between 2007 and 2009 along with the number of inspections. The average number of inspections was 1000 per year. The performance of the regional bodies entitled for inspections has been checked both by quantity and quality (efficiency).

The performance depended on the commitment of the regional body's management, on the personal and technical conditions and also on the endangerment of the territory due to the dangerous shipments. All regional bodies completed the minimal number of inspections that had been determined in advance. The below diagram shows the quantity of inspections of dangerous shipments on road between 2002 and 2011.

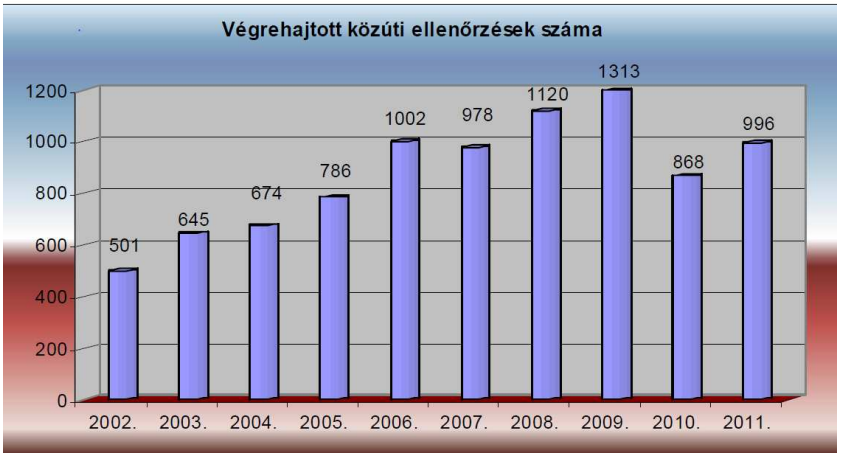


Figure 1. Quantity of inspections of dangerous shipments on road between 2002 and 2011, source: NDGDM 2012

The number of inspected vehicles has continuously increased. The average quantity of inspections was around 2000 vehicle/year. The years of 2008 and 2009 were outstanding. Inspection of unmarked vehicles served the goal of the detection of irregularities which was around 10,000 a year.

Efficiency of the inspections has been influenced by the place and time of the inspections along with the volume of traffic. It happened with many regional bodies that during the inspections there were no or only a few vehicles carrying dangerous goods because there are not many places suitable for conducting the inspections and delivery companies try to avoid them as soon as they get information about the inspections. These cases can only be solved by increasing the number of inspections and changing the places frequently. The differences between the effectiveness of different directorates are also significant, there are big discrepancies between the numbers of detected irregularities. [3]

Quantity of inspected ADR vehicles can be seen at the below diagram.

Figure 2. Quantity of inspected ADR vehicles, source: NDGDM 2012

Average number of inspections during the analysed period was 2000 ADR vehicle/year. Outstanding performance in the usage of fine revenue was in 2008-2009.

Based on the experiences the highest number of irregularities were detected among the smaller domestic transport companies and among the foreign companies coming from the European Economic Area's member states. There were several irregularities according to the

ADR 1.1.3.6 paragraph among the suppliers delivering goods under specified limits that make an exemption.

There were significant differences between directorates regarding the detection of irregularities and efficiency of inspections. By reviewing the statistics of the directorates, findings show a big discrepancy (1.5–27%). [3]

Quantity of detected irregularities during inspections can be described by the changes of relative number of failures. This yearly indicator has continuously decreased in the analysed period. The reason behind it is mainly the improvement of good conduct due to the supervision and inspections.

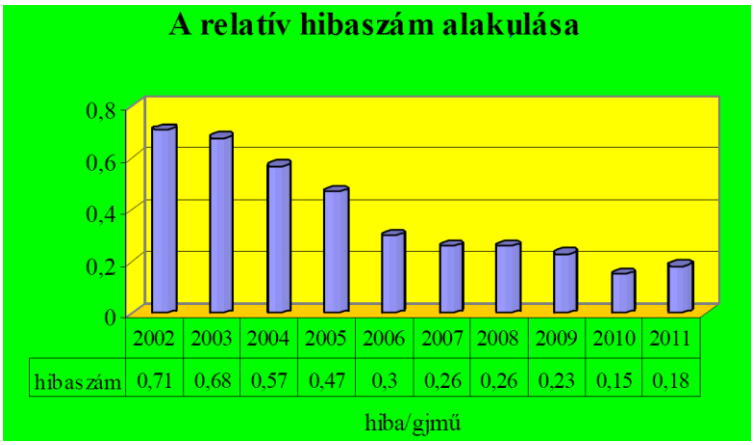


Figure 3. Changes of relative number of failures, source: NDGDM 2012

The most common irregularities are related to the inappropriate management of waybills, the fire extinguishers and the securement of cargo. Lack of written instructions, inappropriate labelling of vehicles and packages were outstanding but lack of protective equipment, warning devices or their validity has been expired or their disfunction were also significant. Unfortunately it is still common that multiple irregularities can be detected with the same vehicle.

Cooperative bodies in the inspections were the police, the transport authority, the tax and customs and the fire service.

Inspections affecting several counties at the same time - including alternative routes - were conducted in a higher quantity each year. Regional bodies of the National Transport Authority, the law enforcement, motorway police, customs administration and governmental fire service also participated in the controls.

During the inspections of transportation on road the partner organizations checked the compliance with the rules that fall under their own tasks and responsibilities while the directorates of disaster management controlled the transportation according to the ADR. The experiences of the complex inspections show that these kind of cross-regional controls are useful and justified even without involving the partner organizations.

Site inspections have been conducted 60-600 times where the directorates also checked the vehicles. Site inspections were mainly conducted only by the directorates of disaster managements, although some of the partner organizations also attended.

Organisations whose industrial sites were inspected strive to be law-abiding and at the same time, cost-effective as much as possible. In many cases, dangerous goods safety advisor contracts were signed before the inspections. Public safety plans were also under scrutiny during inspections. It was general experience that the majority of irregularities could be avoided with site inspections, so they were to be made more frequent. Another reason for site

inspections is that some establishments try to store their dangerous materials at industrial facilities with unsettled issues or at smaller sites probably in an effort to avoid being in the scope of regulations on dangerous establishments.

The greatest series of inspections within the examined period was the so-called "Green Commando" series between 2005 and 2006. The country-wide series of inspections were organised by the Ministries of Interior and of Environment and Water, with the involvement of other affected ministries, and coordinated by NDGDM. The aim of the inspections, which were held in all counties, was to prevent environmentally harmful events and accidents involving dangerous materials.

After 2010, illegal refilling and selling of LPG cylinders were added to the range of inspections. These special tasks were carried out by the authorities as part of exceptional ADR inspections in cooperation with domestic distributors.

At checks of road transport of dangerous goods, professionals conducted awareness raising as a legal instrument for authorities. Fines were set in about 200 instances annually in the case of major or multiple infringements. Altogether, the fines amounted to HUF 100-300 million each year. A third of the cases were taken to the second instance, while on average, 5% of them were discussed at administrative judicial proceedings.

Until 2011, directorates carried out 10-30 inspections a year on road accidents where vehicles transporting dangerous goods were involved. Based on the inspection findings, it can be concluded that in most cases violation of traffic rules or inattention led to the road accidents. Furthermore, it was found that occasionally poor handling of goods (e.g. cargo is not secured properly, etc.) can also be blamed. However, as regards rail incidents, they were caused by leakages almost without exception and some of them even escalated to major incidents.

Before 2011, NDGDM MoI did not conduct inspections of dangerous goods transport by inland waterway, rail and air. Nevertheless, they were involved in professional tasks, which are described below.

NDGDM MoI paid special attention to the safety of establishments that fall out of the scope of the legislation. Enforcing RID provisions is the responsibility of the National Transport Authority. Earlier, the Railway Chemical Response Unit of the Hungarian State Railways used to be in charge of this task. Between 2010 and 2011, NDGDM MoI carried out a Pilot Project to ensure that marshalling yards comply with the requirements to create Emergency Response Plans.

Between 2006 and 2007 NDGDM MoI took part in the project called "Monitoring Dangerous Goods Transport on the Danube", where experts on dangerous goods transport determined the disaster management services to be applied in the system of River Information Services (RIS) on the Danube.

REVIEW OF LEGAL EXPERIENCES RELATED TO THE SUPERVISION OF DANGEROUS SHIPMENTS 2012-2015

The government recognised the society's need for public safety and, as a result, created the legislative background that allowed the disaster management authority to conduct inspections on rail and water transport of dangerous goods – in addition to road transport – starting from 1 January 2012.

The newly emerging tasks and powers in 2012 related to the new transport sub-branches required extending the earlier structure of industrial safety and also developing the system of industrial safety organisations and procedures. [4]

The Director-General issued a new instruction at the end of 2011 that contains authority procedures in the field of dangerous goods transport and many others, thus regulating the unitary application of the methodology and the procedures. Most of the regional directorates have been applying them successfully ever since.

Centralising the fire departments and creating the disaster management branches directly managing them made it possible to increase the number of disaster management staff to be engaged in checks of transport of dangerous goods – primarily road transport.

A three-day series of inspections of road, rail and inland waterway transport, the so-called "DISASTER" is carried out from time to time, coordinated by NDGDM MoI but involving three other partner authorities (National Tax and Customs Administration, Hungarian Police Headquarters and National Transport Authority). [5]

As regards road transport, typically the most problems spotted were with the documents, goods handling and labelling as well as the equipment. In the case of rail transport, the most problems were found with the notifications, but incorrect labelling and leakages were also common. Similarly, water transport inspections revealed irregularities mainly with the documents and the equipment.

For the sake of more successful inspections of inland waterway transport, the Mohács Branch of the Baranya County Disaster Management Directorate established a vessel inspection team in 2012, whose members continuously check vessels transporting dangerous goods. Their centre is located in the premises of the Water Border Crossing Point in Mohács.

In the field of dangerous goods transport, there is still a significant disparity between the directorates in the identification of shortcomings and in the effectiveness of the inspections.

Personnel conditions for inspections are constantly changing as a result of workforce fluctuations at the regional organs, so courses and trainings have to be organised.

Legislation changes in the authority powers coming into effect on 4 June 2013 put local organs in charge of inspections, which previously had been done exclusively by regional organs. From 2013, review procedures at the second instance are performed by regional organs instead of the central organ, NDGDM MoI. Based on the legislation coming into effect at the end of 2014, local organs of disaster management became authorities of the first instance in the field of dangerous goods transport by road, as well. It is also possible for disaster management organs to conduct checks on one another's jurisdiction.

When studying the period between 2002 and 2014, it becomes clear that both the number of dangerous good transport inspections on the road and the number of inspected vehicles are gradually growing. The extent of the growth has been considerable since the introduction of the second disaster management act, which is shown in the figures below.

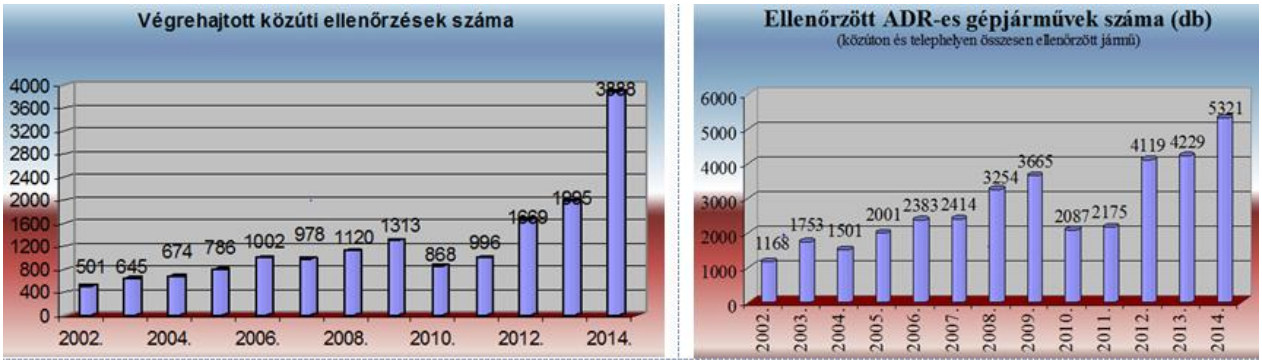


Figure 5. Number of ADR inspections and inspected vehicles [5]

After 2012, inspections that were not performed independently still involved experts from the following partner authorities: police (51%), transport authority (26%) and the National Tax and Customs Administration (16%). In 2014, experts from the National Food Chain Safety Office took part in most joint site inspections. [5]

The following table shows quantitative changes in the inspections of dangerous goods transport by road compared to 2002, 2006, 2009 and 2011, which can be considered base years.

Table 1. Figures of road inspections, source: NDGDM MoI, 2015 [5]

Inspections of Dangerous Goods Transport	**2002**	**2006**	**2009**	**2011**	**2012**	**2013**	**2014**
ADR road transport inspections							
Number of inspections	501	1002	1313	996	1669	1625	3888
Number of inspected vehicles	n/a	n/a	10970	13964	35000	35428	31780
Number of ADR vehicles	1168	2383	3665	2175	4242	4229	5321
Number of defective vehicles	581	362	370	165	317	405	384
Relative number of errors	0.71	0.3	0.23	0.18	0.15	0.13	0.11
Number of site inspections	65	166	322	588	612	654	1114
Number of penalty decisions	not authorised	not authorised	353	233	237	499	645
Number of second-instance decisions	not authorised	not authorised	137	70	100	144	163
Total amount of penalties (million HUF)	not authorised	not authorised	212.45	98	148.55	188.650	215.240
Number of court proceedings	not authorised	not authorised	17	6	13	23	44
Number of inspected accidents	n/a	8	13	27	36	17	32
The inspecting authority (in the first instance)	Regional body	Regional body	Regional body	Regional body	Regional body	Regional body	Local body

Based on the table, it can be stated that the figures related to authority inspections steadily increased. The year of 2011 represents the average performance of inspections under the effect of the first disaster management act. After the second disaster management act came into force, a substantial growth can be seen in the figures, which is most probably due to the authority activity's drop in the public administration level. Local organs replaced regional ones as authorities of the first instance in the integrated organisation. Another reason is the country-wide series of inspections called "Disaster", which embraces all means of transportation.

Relatively less data is available about the quality of the inspections (effectiveness). Occasionally, there are substantial differences between the numbers of irregularities found by the regional and the local organs, which can be explained with differences in staff preparedness. For more effective checks, driving up the quality of the trainings is necessary.

The following table depicts the effectiveness of the inspections in the past three years in the field of dangerous goods transport by rail.

Table 2. Figures of rail inspections, source: NDGDM MoI, 2015

Inspections of Dangerous Goods Transport	2012	2013	2014
RID rail transport inspections			
Number of inspections	705	987	1291
Number of inspected vehicles	15600	20670	23468
Number of RID vehicles	6760	7935	13375
Number of defective vehicles	181	448	341
Number of site inspections	61	110	228
Number of authority decisions	126	135	139
Number of second-instance decisions	36	17	20
Total amount of penalties (million HUF)	13.35	31.23	30.01
Number of court proceedings	2	4	0
Number of accidents	32	16	13

Among the irregularities that were spotted, incorrect documentation ranks first, followed by the lack of labelling and improper use. Some other breaches were typical to the means of transport and a small number of them fell into a “miscellaneous” category. [5]

The table below shows the effectiveness of the inspections in the last three years in the field of dangerous goods transport by inland waterway.

Table 3. Figures of inland waterway inspections, source: NDGDM MoI [5]

Inspections of Dangerous Goods Transport	2012	2013	2014
ADN inland waterway transport inspections			
Number of inspections	315	498	725
Number of inspected vehicles	1200	2388	2488
Number of ADN vehicles	365	435	985
Number of defective vehicles	56	27	26
Number of site inspections	5	14	28
Number of authority decisions	51	37	32
Number of second-instance decisions	6	9	2
Total amount of penalties (million HUF)	17.15	12.81	6.42
Number of court proceedings	0	0	0
Number of accidents	1	1	0

Similarly, the volume of inspections grew in the field of dangerous goods transport by inland waterway.

It is true for both means of transport that disaster management authority is steadily strengthening its activities, which is reflected in better coordination and effectiveness of supervision.

The figure below displays figures related to the incidents between 2012 and 2015 and their inspections.

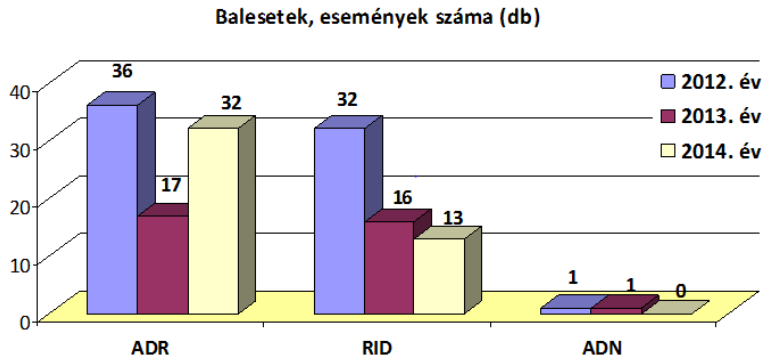


Figure 6. Number of inspected accidents and incidents, source: NDGDM MoI, 2015 [5]

As regards the number of incidents where vehicles transporting dangerous goods were involved, the figures between 2012 and 2015 show a tendency to decrease in all the three means of transport. However, road transport shows some slight variation. [5]

Authority Data Collection System (HADAR) launched on 1 January 2013 took over the tasks of Dangerous Goods Transport Information System (VÁSZIR). HADAR basically relies on the registry elements developed in VÁSZIR. The software Statinfo is still available for the inspectors on the scene.

The modification to the disaster management act that came into force in February 2014 allowed the government to issue decrees on the storage of dangerous materials and goods on site. The draft decree has been drawn up, but its referral to the government has been delayed for an indefinite time after a public administration consultation. The decree will include regulations on how to register, package and label dangerous goods. In addition, it also covers availability of back-up equipment, storage of different types of dangerous goods together as well as the rules of authority inspections.

Since 2012, disaster management has been authorised by law to check dangerous goods transport by air, but it is only since Hungary adopted ICAO Technical Instructions on 1 January 2015 (containing detailed rules on dangerous goods transport by air) that breaches can be sanctioned. Based on this new legislation, primarily six directorates are involved in the inspections (Capital Disaster Management Directorate, County Directorates in Pest, Hajdú, Zala, Baranya and Győr-Moson-Sopron counties). The other directorates may be involved in the so-called “aerial truck” inspections, back-up airports, unauthorised transports, etc. [5]

Manuals on the inspection of dangerous goods transport are prepared by working groups whose members are experts and inspectorate generals from regional bodies. The manual for road transport is already available for inspectors, while the ones for rail and inland waterway will be ready by the end of the year.

CONCLUSIONS AND RECOMMENDATIONS

The presence of disaster management authority in the inspection of dangerous goods transport still poses a highly important task, which greatly facilitates safe transport, and thereby, public safety. Inspection findings and public feedback justify the need for disaster management to continue to act as an independent authority in the checks of dangerous goods transport.

It is apparent that inspections on the road and fining carried out by the disaster management authority underwent smooth progress between 2001 and 2012 and became a renowned field. In 2010, supervisory activities on dangerous establishments and transport, whose high quality was also recognised by the EU, became the foundations of the new set of tasks and instruments of industrial safety.

Due to the legislative preparatory works and institutional development between 2010 and 2012, a more dynamic and strengthened industrial safety authority has been functioning within disaster management since 1 January 2012. Since then, supervision of dangerous consignments has belonged to the field of industrial safety with extended powers and its activities cover all means of transport since the beginning of 2015.

The inspection and fining system in all means of transport relies on the experiences gained in the legislative preparatory works and institutional development related to road transport between 2001 and 2012.

Apparently, the implementation institutions function effectively and the personnel and technical conditions are mostly available. The Institution of Disaster Management (of the National University of Public Service) and the Disaster Management Training Centre are key players in the training of professionals. A balanced relationship exists with the partner authorities, interest associations and safety advisory associations. In 2012 the Industrial Safety Advisory Board was established (at NDGDM MoI), which together with the relevant department at the Institution of Disaster Management (at NUPS) perform and support professional and scientific work.

Currently in Hungary, local organs of disaster management perform inspections of dangerous goods transport in the whole jurisdiction of the regional organ. Checks may be expected in road traffic (road transport), on the railways, at freight stations, at border inspection posts, at railway facilities (rail transport), on national and international waterways, at ports, at berths (waterway transport) and at other related premises. When transported by air, dangerous goods listed in the legislation can be checked whether they are promptly prepared for the flight. Moreover, local and regional bodies of disaster management are also entitled to act as an independent authority when checking dangerous goods that arrived by air but nor forwarded directly by air.

Based on the assessment of road accidents, it can be concluded that the major cause of accidents are basically traffic violations or inattention, but occasionally infringements in goods handling also occur. Rail incidents reveal that their primary cause is leaking in loading and unloading fittings as well as the unsatisfactory technical conditions of tank wagons and the lack of their proper maintenance.

The volume of disaster management inspections significantly increased in the examined period of 15 years, with the quantitative indicators notably rising once the unitary organisation for disaster management was established in 2012. We have to continue to pay special attention to creating the professional conditions for the authorities to achieve unitary application of law and more effective inspections.

Concerning the prevention of transport accidents, the response to them and the recovery of damages, the following professional recommendations can be made to further develop disaster management activities.

Differentiated road tolls, a special fare for ADR consignments (posing a significant risk to public safety) – as a collateral to cover the costs of preventing, responding to and recovering from transport accidents.

Keeping track of dangerous consignments posing a significant risk to public safety based on notification requirements. A compulsory liability insurance system is worth developing. Inspection of ADR consignments has to cover foreign consignments and irregular transportation activities to a greater extent.

ADR inspections can be made more effective by centralising authority activities under the auspices of disaster management, although it requires high-level trainings and technical equipment along with an increased number of staff.

To improve technical conditions of storage, it is suggested that goods are stored in warehouses built and equipped specifically for this purpose instead of buildings and areas unfit for this use and under irregular circumstances.

The current method for the designation of dangerous goods routes cannot be considered a modern procedure any more. Instead, in EU countries the Highway Codes are a popular way to control traffic. It is important to note the need for risk assessments of public roads, freight stations and dangerous goods ports, similarly to the practice in western countries.

The use of a tracking device to monitor the movement of dangerous goods has not gained enough ground yet in the field of authority inspections, this technology is mainly applied to ensure the security of the cargo.

Creating an online interface where dangerous goods transport can be notified is also recommended. Air consignments would be the first to undergo this change, followed by the other means of transport.

The overall conclusion is that, in accordance with the requirements of the EU, international organisations and the Hungarian government, the supervision of dangerous shipments in Hungary ensures the protection of human life and health, the environment and material property, thus contributing to public safety in Hungary as set out in the Basic Law.

References

[1] Kátai-Urbán L.: Establishment and Operation of the System for Industrial Safety within the Hungarian Disaster Management. ECOTERRA: JOURNAL OF ENVIRONMENTAL RESEARCH AND PROTECTION (ISSN: 1584-7071) 11: (2) pp. 27-45. (2014)

[2] NKH Komplex Ellenőrzési és Bírságolási Útmutató (National Transport Authority Guide for Complex Control and Fine): URL.: http://www.katasztrofavedelem.hu/index2.php?pageid=adr_kebu

[3] BM OKF Veszélyes áru – éves beszámoló jelentések. (NDGDM MoI Annual Reports on Dangerous Goods) Budapest, 2003-2011. URL.: http://www.katasztrofavedelem.hu/index2.php?pageid=adr_beszamolo_index

[4] Bognár Balázs, Kátai-Urbán Lajos, Kossa György, Kozma Sándor, Szakál Béla, Vass Gyula: Kátai-Urbán Lajos (szerk.) IPARBIZTONSÁGTAN I.: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. (INDUSTRIAL SAFETY I. Handbook on the Tasks of Operators and Authorities) Budapest: Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 564 p. (ISBN:978-615-5344-12-1)

[5] BM OKF Összefoglaló a veszélyes áru szállítás ellenőrzésének 2014. évi tapasztalatairól (2014 Summary of the experiences on inspections of dangerous goods transport), Budapest, 2015

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Balog Károly
balog.karoly07@gmail.com

DIGITÁLIS PMR RENDSZEREK ÖSSZEHASONLÍTÁSA II.

Absztrakt

Cikkemben a hagyományos analóg rendszereket fokozatosan leváltó elterjedtebb TDMA[1] típusú digitális PMR[2] szabványok, rendszerező, összehasonlító elemzésének eredményeit foglalom össze. Ismertetem a feldolgozott szabványokból, egyéb technikai leírásokból megismerhető, általános, és azoktól eltérő egyedi megoldásokat, eljárásokat, melyekből következtetéseket vonok le a felderítésük és azonosításuk lehetséges ismérveire, technikai paramétereik megállapításán keresztül. Az ismérvek megállapításának célja az alacsony szintű analóg és digitális beszédtípusú PMR adások felderítésére, azonosítására a beszédinformáció kinyerésére univerzálisan alkalmazható eszköz paramétereinek, a vételi képességek tulajdonságainak kidolgozása.

This article summarizes the results of the comparative analysis of the more common TDMA type digital PMR systems, which gradually replace the presented analog systems. I describe the commonly used and unique solutions and procedures from the processed standards, technical descriptions and from which conclusion are set out in the radio detection and identification of possible criteria, through technical parameters. The goal of develop parameters is the low-level analog and digital, voice type PMR transmission detection, identification, speech information extraction for the determination of parameters of the radio reception capabilities, in the universally applicable device.

Kulcsszavak: *PMR (Professional/Private Mobile Radio), DMR (Digital Mobile Radio), dPMR (Digital PMR), LLVI (Low Level Voice Intercept), COMINT (Communications Intelligence) ~ professzionális / magán mobil rádió, digitális mobil rádió, digitális professzionális mobil rádió, alacsonyszintű beszédtípusú kommunikációs jelek felderítése, kommunikációs felderítés*

[1] TDMA: Time Division Multiple Access – Időosztásos többszörös hozzáférési (rádiócsatorna megosztási) eljárás
[2] PMR: Professional / Private Mobile Radio - professzionális / magán mobil rádió: A felhasználók által saját maguknak nyújtott zártkörű rádióalkalmazások gyűjtőneve

BEVEZETÉS

A két cikkből álló sorozat első részében [1], a hagyományos, analóg PMR rendszereket fokozatosan leváltó – frekvenciaengedélyhez kötött és nem kötött formában egyaránt alkalmazható – világviszonylatban elterjedtebb digitális PMR szabványok közül, az FDMA3 típusú keskenysávú szabványok rendszerező, összehasonlító elemzésének eredményeit foglaltam össze. A második részben a TDMA típusú szabványok vizsgálatát végzem el a fenti módszerek segítségével, illetve a terjedelmi korlátok miatt a P25 FDMA része is itt kerül ismertetésre. Így az I. és II. rész együttesen ad áttekintést a fontosabb digitális PMR szabványokról.

Ismertetem a feldolgozott szabványokból, specifikációkból, egyéb technikai leírásokból megismerhető általános, és azoktól eltérő egyedi megoldásokat, eljárásokat, melyekből következtetéseket vonok le a felderítésük és azonosításuk lehetséges ismérveire, technikai paramétereik megállapításán keresztül. Az ismérvek megállapításának célja az analóg és digitális beszédtípusú PMR adások jeleinek felderítésére, azonosítására a beszédinformáció kinyerésére univerzálisan alkalmazható eszköz paramétereinek, vételi képességeinek tulajdonságainak kidolgozása. Ez főleg a nemzetbiztonsági, de a katonai felderítés számára is jelentőséggel bír, mivel ezek a rendszerek és az egyedi készülékek képesek kikerülni a hagyományos távközlési infrastruktúrákat, így ebben az esetben felderítésük, ellenőrzésük kizárólag rádiós úton, a kommunikációs felderítés eszközrendszerével lehetséges.

A DIGITÁLIS PMR SZABVÁNYOK JELENLEGI ELTERJEDTSÉGE

A jelen cikk első részének készítésekor 2014 elején, már működtek digitális PMR rendszerek Magyarországon, azonban az azóta eltelt időben hatványozottan felgyorsult az ilyen rendszerek hazai, de nemzetközi elterjedése is. Ez az akkori és a jelenlegi hazai vételkísérleteim tapasztalatai, valamint a nemzetközi szakirodalom tanulmányozása alapján egyértelműen megállapítható, és kijelenthető. Gyakorlatilag ez azt jelenti, hogy a régi elavult amortizálódott rendszerek leváltásakor csakúgy, mint új rendszerek tervezésekor már egyértelműen szinte kizárólag a digitális rendszerek kerülnek az előtérbe, és kivitelezésre a gyakorlatban is, azaz beindult és működik a digitális migráció. A működő rendszerek között egyaránt megtalálhatóak a keskenysávú FDMA és a TDMA típusú rendszerek, de kezd jól körvonalazódni ezek hazai elterjedtsége is az adott konkrét szabványokra vonatkoztatva.

A jelen cikk tárgyát képező TDMA típusú rendszerek tekintetében gyakorlatilag 4 féle szabvány létezik, az európai TETRA[4], az amerikai P25[5], a szintén európai DMR[6] és a kínai PDT[7], ahogyan ez a cikk első részében lévő táblázatban is látható [1]. A szabványok tekintetében azóta csak az elterjedtségükben történt változás. Vegyük sorra az egyes szabványokat. A TETRA és a P25 főleg a rendvédelmi szektorban egyeduralkodók Európában és Amerikában, de a civil TETRA rendszerek is egyre nagyobb elterjedtséget mutatnak a világban. A kínai PDT rendszernek szintén inkább rendvédelmi vonatkozásai vannak, Európában pedig egyáltalán nincs is piaca. A PDT emellett olyannyira kötődik a rendvédelemhez, hogy először Police Digital Trunking-nek nevezték, utalva a fő kínai

[3] FDMA: Frequency Division Multiple Access – frekvenciaosztásos többszörös hozzáférési (rádiócsatorna megosztási) technika

[4] TETRA: Terrestrial Trunked Radio – európai 4 időréses trönkölt rádiószabvány

[5] P25: Project 25 – az APCO (Association of Public Safety Communications Officials International) kezdeményezésére a TIA (Telecommunications Industry Association) által kidolgozott nyílt rádiószabvány, melyet a TETRA-hoz hasonló célokkal hoztak létre amerikában, de Kanadában és Ausztráliában is használt.

[6] DMR: Digital Mobile Radio – Európia két időréses digitális rádiószabvány.

[7] PDT: Professional Digital Trunking – professzionális digitális, a DMR-hez hasonló 2 időréses trönkölt rendszer

felhasználás jellegére. A rendszert ugyanis a kínai közbiztonsági minisztérium kezdeményezésére kezdték el kifejleszteni hazai (kínai) tudományos bázison. [2]

A nem trönkölt típusú rendszerek tekintetében egyedül az európai DMR szabványú rendszerek mutatnak jelentősebb elterjedtséget itthon, bár a DMR-nek is van trönkölt változata. A DMR típusú rendszereknek már számos alkalmazása valósult meg Magyarországon, erőművek, taxi társaságok, futárszolgálatok, autógyárak és egyéb ipari üzleti alkalmazások tekintetében. A DMR azonban már nem csak az üzleti életben, de az amatőr rádiózásban is legalább annyira népszerű, nem csak Európában, de az amerikai kontinensen is. Az elmúlt években 4 magyarországi átjátszó is kiépítésre került, melyekkel már szinte teljes országos lefedettség valósult meg napjainkra. Az átjátszók egy kiterjedt nemzetközi hálózat részeként a világ számos DMR átjátszóján keresztül kommunikációt biztosíthatnak az azok vételkörzetében tartózkodó regisztrált felhasználókkal. A TDMA szabványú nem trönkölt rendszerek tekintetében, tehát a DMR gyakorlatilag egyeduralkodó itthon.

TDMA rendszerek tekintetében az érdeklődésem legfőképpen a DMR szabványra irányul, mivel a vizsgálataim célját tekintve, az illegális, vagy engedélyhez nem kötött használatra az ilyen rendszerek alkalmasak, hiszen a trönkölt rendszerek használatához fix telepítésű infrastruktúra szükséges. Az ilyen szempontú vizsgálat okán a P25 nevű amerikai szabvány bizonyos típusainak is lehet még jelentősége az eszközök nagy száma, és ezek esetleges illegális terjedése miatt. Ez utóbbi okán azonban a PDT rendszerű készülékekkel is foglalkozni kell annak ellenére, hogy a rendszer még csak Kínában mutat jelentősebb elterjedtséget. Mivel azonban a Hytera és más nagy kínai gyártók a kínai kormány kulcsfontosságú partnerei a rendszer fejlesztésében, ezért a cégek súlya miatt egyéb, főleg ár érzékeny afrikai és ázsiai piacokon is működnek már PDT rendszerek, pl. Guatemalában, Thaiföldön, Kambodzsában, Indonéziában és Vietnámban is [2]. A Hytera cég információja szerint [2] azonban érdeklődés volt már Európából, latin-Amerikából és a közel keletről is tesztrendszerek tekintetében, azaz a szabvány jelentősége egyre nő, nem csak Kínában, de nemzetközi szinten is.

Az európai TETRA tekintetében is jelentős elterjedtségről beszélhetünk itthon, de világviszonylatban is, hiszen a rendvédelmi szervek hazai kommunikációját kizárólag az országos EDR rendszer biztosítja. Amellett, hogy a nem rendvédelmi alkalmazások terén is egyre nagyobb igény mutatkozik a TETRA rendszerű EDR hazai igénybevételére. Mivel azonban ez a rendszer is trönkölt megoldást alkalmaz alapvetően, továbbá olyan szintű kiiktathatatlan azonosítási, titkosítási és biztonsági eljárásokat implementáltak a rendszerbe, ami nagymértékben biztonságossá teszi az alkalmazását, ezért ennek vizsgálatával nem foglalkozom.

Nézzük meg először a PDT és a P25 rendszerekkel kapcsolatos aktuális információkat, majd pedig részletesen a DMR-el kapcsolatos ismereteket.

A PDT RENDSZER

A PDT rendszer alapvetően a kínai piacra készült szabvány, amelyik erős párhuzamosságokat mutat az európai DMR-el, azonban a kínai piac helyi specifikus igényeit is ki tudja szolgálni. Így együtt tud működni a jelenleg is meglévő MPT 1327 típusú analóg trönkölt rendszerrel (350 millió felhasználó) és annak GIS rendszerével is, majd fokozatosan biztosítja a PDT bevezetését a digitális átállás keretében. A kínai nagyvárosokban alapvetően TETRA rendszerek működnek, azonban a nagy területi lefedettséget országos szinten megoldó MPT analóg hálózatok cseréje költséghatékonyan csak a TETRA-nál olcsóbb technológia kiváltásával lehetséges a kínai kormány szerint [3].

A PDT tekintetében a beszédkódolás (vocoder) kulcskérdés, mivel annak eljárása meglehetősen nyelv specifikus. Azonban nemcsak ezért, hanem a DVSI[8] beszédkódolók nemzetközi monopóliumának megtörése és licenszdíjának megspórolása okán sem akartak amerikai szabványú beszédkódolót alkalmazni a rendszerben [4]. Így az orosz és kínai nyelv specifikus NVOC beszédkódoló fejlesztését a kínai Tsinghua Egyetemen végezték el [2]. A beszédkódolás mellett pedig az alkalmazott biztonsági is titkosítási technológia is a nemzeti szükségleteikkel van összhangban, azaz hazai fejlesztésű algoritmust alkalmaznak, továbbá a helymeghatározás tekintetében is a saját kínai Beidou[9] rendszerrel történő együttműködést preferálják.

Összességében a fentiek miatt a rendszer olcsóbb, mint a TETRA és DMR típusú rendszerek. Az Actec cég információja szerint egy PDT rendszerű terminál mintegy 1/7-árú egy TETRA terminál árához képest [4]. A PDT rendszer 2010. április 20-i bejelentése után három évvel a Kínai Közbiztonsági Minisztérium 2013. március 20-án hivatalosan is kiadott 4 ipari műszaki szabványt, amelyik tartalmazza a PDT rendszer általános technikai specifikációját a GA/T1056-2013 számon, a rádiócsatorna fizikai és adatkapcsolati rétegének leírását a GA/T1057-2013 számon, a rádiócsatorna hívásvezérlő rétegének technikai leírását a GA/T1058-2013 számon valamint a rendszer biztonsági műszaki előírásait a GA/T1059-2013számon [5]. A szabványokról angol nyelvű leírást nem találtam az interneten, egyedül az Amazon kínai vállalatának on-line kínálatában akadtam egy azonos című kínai nyelvű nyomtatott szabványleírásra, amelyik 25 jüanba kerül az oldalon. Angol nyelven egyelőre a Springer India kiadásában jelent meg egy hiánypótló könyv a Wireless Communications, Networking and Applications 2016-os kiadása, de ebben is csupán két cikk található a PDT-vel kapcsolatban. Az egyikből [6] megtudjuk, hogy a PDT a 2010-es bemutatása óta a folyamatos kutatás-fejlesztésnek köszönhetően 2015-re a termékek nagy volumenű kereskedelmi bevezetése és gyártása elkezdődött, és Kínában már számos helyen alkalmazzák a régi MPT trönkölt rendszerek kiváltására. A szerzők szerint a PDT az érett időszakába lépett. A fenti kiadvány másik cikke [7] a PDT rendszer csatorna hozzáférésének fejlesztését írja le a TETRA szabványhoz hasonlítva annak képességeit.

Szintén az Actec cég honlapján [8] további információkat kapunk arról, hogy a rendszer széleskörű bevezetése megkezdődött Kínában, amit 2013 szeptemberig már mintegy 45 hazai cég támogatott beszállítóként és kivitelezőként. A PDT rendszer mindemellett a gyártók és beszállítók nagy száma (kritikus tömege) miatt már Oroszország, Thaiföld, Pakisztán és Nepál kommunikációs hálózataiban is működik projekt jelleggel. Az orosz felhasználás természetesen érthető a közösen kifejlesztett nyelv specifikus beszédkódoló kapcsán, valamint az ország hasonló területi és gazdasági adottságai, politikai beállítottsága miatt. Egy másik gyártó (Volinco) angol nyelvű honlapján [9] található dokumentumból azonban további hasznos részletek derülnek ki a szabvánnyal kapcsolatban. Ebben egyértelműen leírják, hogy bár a szabvány neve trönkölt rendszerre utal, azonban a DMR Tier 1-2-3 szintjeihez hasonlóan a trönkölt üzemmód mellett itt is lehetséges a közvetlen direkt valamint az átjátszón keresztüli kommunikáció is. Ennek fényében a később legálisan vagy illegálisan terjedő várhatóan igen olcsón beszerezhető készülékek direkt módú kommunikációja szintén érdekes lehet a témám szempontjából.

Mivel egyelőre nem érhető el angol nyelvű változat az eredeti szabványból így a rendszerrel kapcsolatos konkrét műszaki tartalmak hiányában csak azt lehet feltételezni, hogy annak címzési és készülékazonosítási megoldási, eljárásai nagymértékben hasonlítanak egymásra, mivel a PDT megalkotásakor a DMR volt a kiindulási alap. Ezt támasztják alá azok az információk is, hogy a gyártók által készített PDT készülékek a legtöbb esetben a DMR

[8] DVSI: Digital Voice Systems Inc. –alacsony bitrátájú beszédkódolókat gyártó amerikai cég

[9] Beidou: (magyaros átírással: Pejtou) a kínai megfelelője a jól ismert amerikai GPS, valamint az orosz GLONASSZ és az európai Galileo műholdrendszereknek.

szabvány szerint is képesek működni. A Hytera cég DMR termékvonalához készült szoftververziójának 7.0 kiadásába bekerült az átjátszóállomások új képességei közé a PDT-hez készült NVOC beszédkódoló támogatása is [10]. De számos más kínai gyártó DMR rádiójában az AMBE vokóder mellé az NVOC támogatása is bekerült [11].

A PDT rendszer olcsósága miatt az arra érzékeny piacokon jelentős sikereket érhet el a jövőben, ami elősegítheti az egyébként önmagában sem kicsi kínai piac mellett a rendszer globálisabb elterjedését is.

A P25 RENDSZER

A Project 25 rövidebb nevén P25, az APCO[10] kezdeményezésére a TIA[11] által kidolgozott és 1995-ben közzétett nyílt rádiószabvány (TIA-102), melyet a TETRA-hoz hasonlóan – rendvédelmi és kormányzati kommunikációs – célokkal hoztak létre Amerikában, de Kanadában és Ausztráliában is használt. A P25 természetesen a magánszféra és a rádióamatőrök által is széleskörűen alkalmazott kommunikációs szabvány világszerte, adott esetben titkosított, de titkosítás nélküli formában is.

A P25-nek két „fázisa” létezik: az egyik a Phase 1. (1995: analog, 2003: digitális), amelyik 12,5 kHz-es FDMA átvitellel és a digitális változat C4FM modulációval működik. A másik a Phase 2. (2009-2012), amelyik szintén 12,5 kHz-es csatornán, azonban két-időréses TDMA átvitellel és H-CPM[12] állandó burkolójú nemlineáris modulációval valamint H-DQPSK[13] non-koherens modulációval működik. A H-CPM-et a felhasználói készülékeknél alkalmazzák, míg a H-DQPSK modulációval a fix telepítésű berendezések (átjátszók, bázisállomások) sugároznak a felhasználók felé. [12]

A digitális P25 Phase 1 szabványánál DVSI szabványú teljes sebességű (full rate) IMBE[14] beszédkódolót alkalmaznak, azonban a Phase 2 már félsebességű (half-rate) AMBE[15] beszédkódolót használ, csak úgy, mint a DMR szabvány. Az IMBE kódoló a 20 ms-os szabványos beszédkeretekből 88 bit kódolt adatot állít elő (4400 bit/s) amit 2800 bit/s-os hibakorlátozó kódolással (FEC) egészít ki. Az így kapott 7200 bit/s a beszédkódoló kimenő bitsebessége, amihez legvégül a 2400 bit/s-os jelzésátviteli és hívásvezérlő információ adódik hozzá. Így összességében megkapjuk a Phase 1 9600 bit/s-os csatorna kapacitását. A Phase 2 esetében kisebbek a sebességek: az AMBE kódoló 2450 bit/s-os natív audió jeléhez 1150 bit/s-os hibakorlátozó kódolás (FEC[16]) adódik, ez eredményezi a beszédkódoló 3600 bit/s-os kimenő jelét, amihez szintén 2400 bit/s-os jelzésátviteli információ adódik. Így összességében 6000 bit/s-os csatornakapacitást kapunk (1 időrés esetén). [13, p. 23.]

A rendszerben alkalmazott hibavédő és hibakorlátozó kódolások hasonlóak, mint a többi PMR szabványnál vagy egyéb mobil kommunikációs rendszernél. Így a védelemre Hamming, Golay, Reed-Solomon, stb. kódokat alkalmaznak bitszétkenéssel kombinálva, az átvitt rádiófrekvenciás-jelek fédingek okozta hibái ellen.

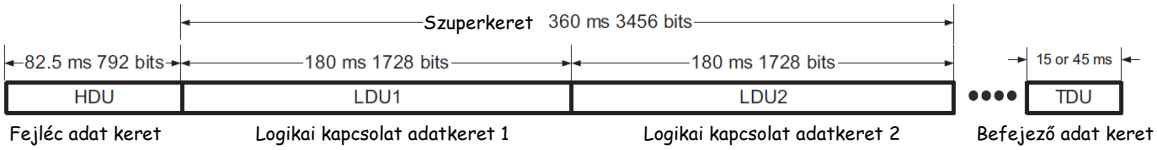
A szabványleírás szerint a Phase 2 módú rádiók kizárólag trönkölt rendszerű üzemmódban működnek, azonban visszafelé kompatibilisek a Phase 1 típusúakkal. Ez azért van így, mert a Phase 2 esetében a vezérlőcsatorna minden esetben a Phase 1 FDMA szabványa szerint működik. A Phase 2 rendszer a Phase 1 jelzésrendszerének és az Air Interfészének alapjaira épül, kiegészítve azt a TDMA működésmód képességével. Megállapítható, hogy a Phase 1 a

[10] APCO: Association of Public Safety Communications Officials International
[11] TIA: Telecommunications Industry Association
[12] H-CPM: Harmonized Continuous Phase Modulation –állandó burkolójú nemlineáris moduláció
[13] H-DQPSK: Harmonized Differential Quadrature Phase Shift Keyed modulation
[14] IMBE: Improved Multi-Band Excitation – Továbbfejlesztett többsávos beszédkódoló
[15] AMBE: Advanced Multi-Band Excitation – Fejlett többsávos beszédkódoló
[16] FEC: Forward Error Correction – hibakorlátozó kódolás, ami a kisebb bithibákat képes javítani növelve ezzel a hatótávolságot és az átvitel minőségét

témám szempontjából a lényegesebb, mivel közvetlen, vagy átjátszón keresztüli működésre kizárólag ez képes. Így a következőkben a Phase 1 ismertetésére szorítkozom annak ellenére, hogy ez egy FDMA szabvány. A Phase 2 szabványú rádiók is tudják ezt az üzemmódot, a fent leírtak miatt, és így akár közvetlen összeköttetésre is képesek, annak ellenére, hogy a fő funkciójuk a trönkölt üzemű működés.

A P25 phase 1 keretszervezése, logikai csatornái, címzési módjai

A P25 rendszer esetében is keretszervezéssel biztosítják a hang és adat információk rendezett és átviteli hibák ellen is védett adását és vételét. A beszédkódoló által előállított 20 ms-os beszédnek 88 bitnyi információ felel meg, melyet 56 bites paritásvédelemmel kiegészítve egy beszédkeret 144 bit-re adódik. Ezekből 9-9 db kerül átvitelre mindkét LDU1 és LDU2 [17] mezőben. A két egyenként 180 ms-os LDU mező együtt alkot egy 360 ms-os szuperkeretet. Ezek folyamatos átvitele addig ismétlődik, egy bevezető keret HDU18 átvitele után, amíg a beszéd tart. Az információátvitel végét egy befejező adatkeret TDU 19 kisugárzásával jelzik. Adatátvitel esetén az LDU1-2 adatkeretek helyett változó hosszúságú csomagkapcsolt PDU[20] adatkereteket használnak

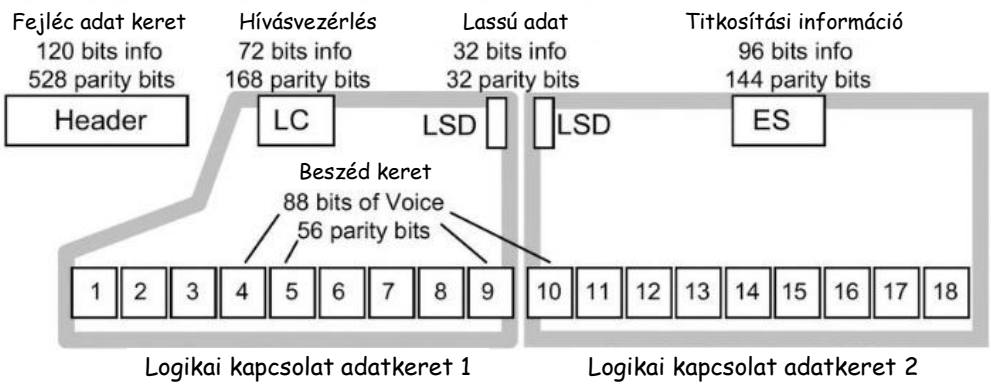


1. ábra: A P25 keret felépítése [12, p. 49. a szerző által szerkesztett]

Ha kiszámoljuk, látható hogy a 144*9=1296 bit nem tölti ki az LDU 1 és 2 adatkeretek 1728 bitjét. Ez azért van, mert a maradék bitidőben egyéb társított információkat visznek át a hívásvezérlési információk (LC[21]), titkosítási információk (ES[22]) és lassú-adat (LSD[23]) átvitele céljából, ahogyan ez a 2. ábrán látható.

Ezeket nevezhetjük logikai csatornáknak is, melyek bitjeit az egyes beszédkeretek közötti szünetekben viszik át a következő képen. Az LC: az LDU1 2-8. beszédkeretek közötti 6x40=240 bit segítségével kerül átvitelre. Az LSD: egyik fele az LDU1 8-9. még második fele az LDU2 17-18. beszédkeret közötti 2x32 (összesen 64) biten kerül átvitelre. Az ES: azaz a titkosítással kapcsolatos információk egyrészt minden egyes fejléc adatkeretben HDU, továbbá az LDU2 11-17. beszédkeretek közötti 6x40=240 bit segítségével is átvitelre kerül.

[17] LDU1 és LDU2: Logical Link Data Unit – logikai kapcsolat adatkeretek /ezek a beszédkeretek/
[18] HDU: Header Data Unit – fejléc adatkeret
[19] TDU: Terminator Data Unit – befejező adatkeret
[20] PDU: Packet Data Unit – csomagkapcsolt adatkeret
[21] LC: Link Control – hívásvezérlő logikai csatorna
[22] ES: Encryption Syncronisation – titkosítási információk
[23] LSD: Low Speed Data – lassú adatátviteli csatorna

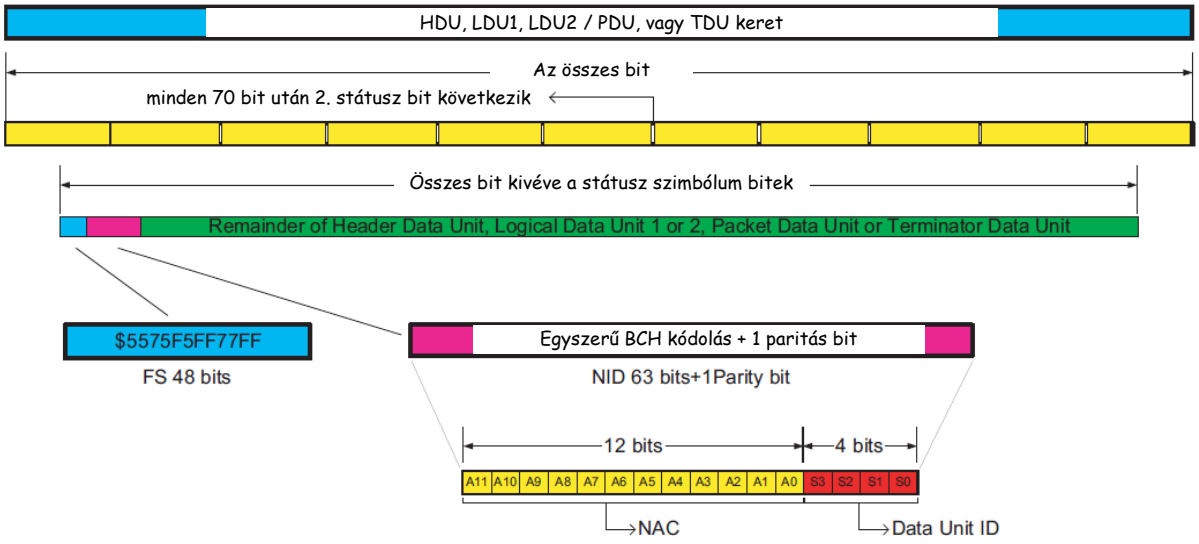


2. ábra: A P25 keret felépítése [14, p. 8. a szerző által szerkesztve]

A P25 szabvány kód rendszere

Keretszinkronizálás és hálózatazonosítás

Mindegyik 1. ábrán látható adatkeret (a HDU, az LDU1, LDU2/ vagy PDU továbbá a TDU) egy speciális 48 bites ún. keret-szinkronizációs FS[24] szekvenciával továbbá a 64 bites (16 bit hasznos) NID[25] hálózatazonosító kóddal kezdődik, mind beszéd mind adatátvitel esetében (3. ábra). Azaz legrosszabb esetben is 180 ms-onként ismétlődik, ami biztosítja az ún. late entry azaz a késői belépés lehetőségét a kommunikációba. Az FS ismert bitsorozata biztosítja az egyes adatkeretek elejének megtalálását. A szoftveres és hardveres digitális PMR dekóderek is erre szinkronizálnak rá. Az FS nem programozható a felhasználó által.



3. ábra: Keretek szinkronizálása, és a hálózat azonosítása valamint a csomag típus beállítása [12, p.50.]

Hálózat és szolgáltatásazonosítással kapcsolatos kódok

A *Státusz szimbólum* minden 70 bit utáni 2 bit, (3. ábra sárga sor) a csatorna aktivitását jelzi az ismétlő felé 00 vagy 10 jelzéssel. Míg az ismétlő a 01 státuszjelzéssel foglaltságot, az 11-el pedig idle átvitelt jelez /szabad jelzés/ a felhasználók felé a bejövő időkeretek tekintetében. A 00 ismeretlen állapotot jelent, illetve ezt alkalmazzák Direkt kommunikáció esetén is. Az 10 állapotot pedig szintén használt ismétlő ismeretlen státuszának jelzésére is.

[24] FS: Frame Synchronization – keretszinkronizáló bitsorozat
[25] NID: Network Identifier – hálózatazonosító

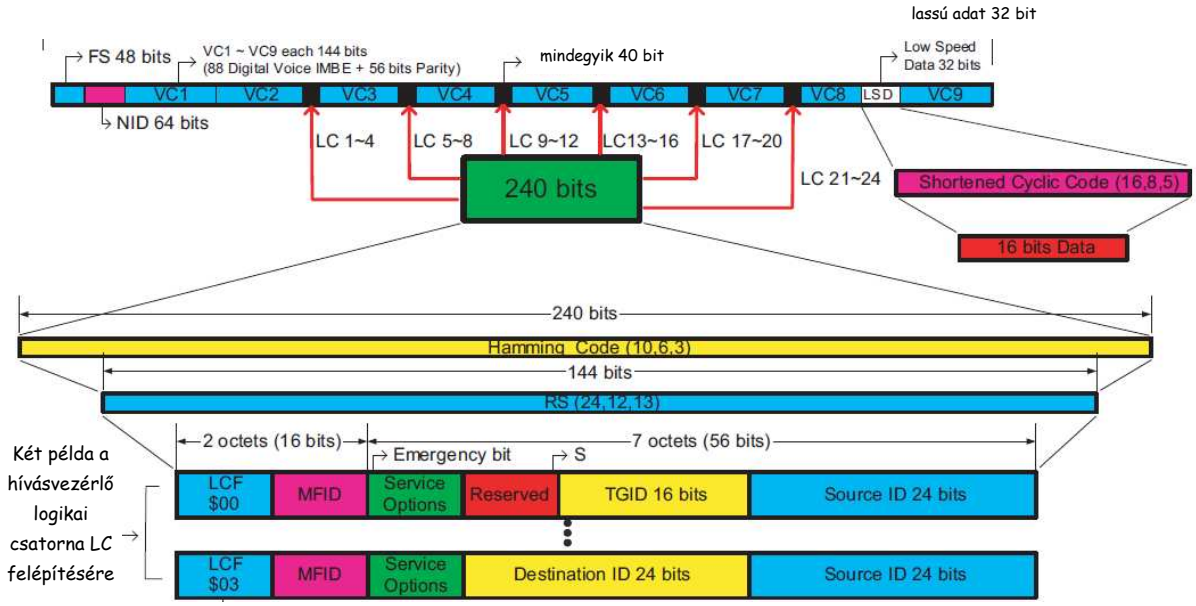
A P25 esetében *a hálózat azonosítására* az un. NID[26] kódok (64 bit) szolgálnak, amelyeket minden P25 adatkeret tartalmaz. Ez egy 12 bites NAC[27] és egy 4 bites Data Unit ID kódból áll. Ezek együttese egy egyszerű BCH kódolás és paritás képzés után nyeri el végső 64 bites alakját. (3. ábra)

A *Data Unit ID* 4 biten definiálja az adatkeret típusát, pl. fejléc HDU vagy logikai kapcsolat adatkeret LDU1 / LDU2 vagy befejező adatkeret TDU adatcsomag, stb. Ezek a bitek nem hozzáférhetők, ill. programozhatók a felhasználó által.

A *NAC kód* 12 biten (4096 kóddal) a felhasználó által programozhatóan az átjátszóhoz vagy másik rádióhoz történő hozzáférést vezérli, a DMR-nél alkalmazott CC- színkódhoz vagy az analóg rendszereknél alkalmazott CTCSS és DCS kódokhoz hasonlóan. Azaz minimalizálja az azonos területen működő, de eltérő hálózatok közötti interferenciákat. *Emiatt azonban egy felderítésre alkalmazott eszköznél a NAC kód segít azonosítani a felderített adások hovatartozását.* Mind az egyedi készülékeken (F7E) mind az átjátszókon (F7F) beállítható a NAC speciális értéke, amelyiknél bármely NAC azonosítóval ellátott hálózat jeleit veszik, illetve továbbítják (átjátszók) a berendezések szelektálás nélkül. *Ez egyrészt ismeretlen adók monitorozását teszi lehetővé rádiók esetében, másrészt pl. amatőr /nyilvános használatú/ átjátszók esetén tetszőleges bejövő adások továbbítását biztosítják.*

Hívócsoport és készülékazonosítással valamint gyártóval kapcsolatos kódok

Az LDU1 tartalmazza a hívásvezérlő csatornát LC, melynek 240 bitjéből a 72 hasznos bit két lehetséges változatát szemlélteti a következő 4. ábra. A legfelső sor összesen 1680 bit, amihez még hozzáadódik 48 bitnyi státusz szimbólum, így kapjuk meg az adatkeret 1728 bites teljes hosszát.



4. ábra: Az LDU1-ben átvitt hívásvezérlő (LC) és lassú-adat (LSD) logikai csatornák átvitele [12, p.53. szerző által szerkesztett]

Az LC 72 hasznos bitje többféle formátumot vehet fel, a fenti ábrán ezek közül kétféle látható. Az LCF[28] 8 bitje közül az első bit az MFID utáni bitek titkosítását (1), illetve nyílt átvitelét (0) jelzi. Az LFC utolsó 6 bitje az un. LCO[29] ami meghatározza az LC felépítését, azaz a típusát. Ez 0-63-ig vehet fel értéket. Ezek közül a számunkra két legfontosabb típust részletezi a 4. ábra.

[26] NID: Network IDentifier – Hálózat azonosító kód
[27] NAC: Network Access Code –Hálózat /ismétlő/ hozzáférési kód
[28] LCF: Link Control Format – hívásvezérlő csatorna formátumát meghatározó mező, az LC első 8 bitje
[29] LCO: Link Control Opcode – hívásvezérlő formátum kódja

A felső egy csoporthívás, míg az alsó egy direkt hívás vezérlésére szolgáló felépítést mutat. Ezek az alábbi a hívó és hívott fél egyedi azonosítására alkalmas kódokat tartalmazzák.

A *hívócsoportok* (a felhasználók adott szempont szerinti beszédcsoportjának) logikai *azonosítására* (címzésére) szolgálnak a 16 bites TGID[30] kódok. Ez 0000-FFFF (hex.) 65536 egyedi címet vehet fel. Speciális értékei: 0001 csak egy beszédcsoport létezik, 0000 beszédcsoporton kívüli felhasználó vagy egyedi hívást kezdeményez, illetve FFFF esetén mindenki számára elérhető csoport. A TGID-t nem csak az LC tartalmazza, de minden egyes fejléc adatkeretben HDU-ban is átvitelre kerül. Így már ennek dekódolásából eldönthető, hogy nekünk szól-e az üzenet.

Az *egyedi készülékek azonosítására* szolgál a 24 bites (16.777.216 különböző) Unit ID[31] kód, mely mind csoport, mind egyedi hívás esetén azonosítja a hívó és a hívott felet egyaránt. Két típusa van a Source ID a hívást kezdeményező címe, míg a Destination ID a hívott fél (a vevő) egyedi címe. Az ID kódokat a felhasználók szabadon programozhatják a készülékbe.

További azonosító a rendszerben a 8 bites MFID[32], amelyik a *készülékgyártót azonosítja* (ilyen szintén van a DMR-nél), így az esetleg gyártónként kismértékben eltérő rádió képességeket, egyedi alkalmazásokat, illetve jelzésátviteli specialitásokat lehet általa figyelembe venni a kommunikáció során. Ha ennek értéke nem a szabványos 00 vagy 01 (hexa) érték, akkor az adott rádió jelét nem biztos, hogy venni vagy továbbítani tudja egy másik kóddal rendelkező átjátszó, vagy rádiókészülék. Az MFID szintén átvitelre kerül minden egyes fejléc adatkeretben HDU-ban is.

Lassú adattal és vészjelzéssel kapcsolatos kódok

Az LDU1 VC8 és VC9 beszédkeretek között kerül átvitelre a lassú-adat logikai csatorna LSD első fele 32 biten. Ennek 16 bites hasznos része a szabványban részletesen nem definiált olyan alacsony sebességet igénylő adatátvitelt tartalmazhat, mint a GPS helyzetinformációk, infrastruktúra státusz információk stb. Az adatokat rövid ciklikus kóddal védik a hibáktól. Az LSD második fele az LDU2 VC17 és VC18 beszédkeretek között a fentiekhez hasonlóan kerülnek átvitelre.

A vészjelzéssel kapcsolatos un. emergency indicator bit, a 4. ábrán látható csoporthívást bemutató LC-csatorna szolgáltatás opciók (zöld színű) mezőjének első bitje jelenti. Ha ez 0, akkor normál, ha 1 akkor vészhívásról van szó.

Titkosítással kapcsolatos kódok

Az összességében 96 bitnyi titkosítással kapcsolatos információk az LDU2-ben kerülnek átvitelre, melyek 144 bites paritással (Reed-Solomon+Hamming) vannak kiegészítve. A titkosítási információk minden egyes HDU fejléc adatkeretben is átvitelre kerülnek, az MFID és a TGID kódjaival együtt, azonban itt jóval erősebb hibavédelemmel vannak ellátva. A hasznos bitek tartalma mindkét átvitel esetében a következő.

A 8 bites ALGID[33] kódok az alkalmazott titkosító *kódolási algoritmust* azonosítják: pl. 80 (hex.) titkosítatlan, 84 (hex.) AES titkosítást jelent.

A 16 bites KID[34] az alkalmazott egyedi *titkosító kulcsot* azonosítja, amelyet a titkosító modulba kell betölteni. Titkosítatlan esetben ez 0000 (hexa) értékű.

A 72 bites MI[35] egy szinkronizáló bitsorozat a titkosító kulcsgenerátor szinkronizálásához, amelyet 1, 2, 3, 4 típusú kódolási algoritmusok (ALGID) esetén alkalmaznak. Titkosítatlan üzenetnél az értéke 0.

---

[30] TGID: Talk Groups Identification Code – Beszédcsoport azonosító kód
[31] Unit ID: készülékazonosító egyedi kód, ami egyaránt lehet az adó vagy a vevő kódja is
[32] MFID: Manufacturers Identification Codes – Berendezésgyártó azonosító kód
[33] ALGID: Algorithm ID – Azaz algoritmus kód, az üzenet kódolására használt titkosítás eljárást definiálja
[34] KID: Key ID – Azaz kulcs azonosító, a titkosító kulcsot azonosítja

Titkosított üzenet esetén a fenti kódokkal tudjuk az adó és a vevő titkosító modulját azonos állapotba hozni, hogy a titkosított információt vissza tudja fejteni.

A P25 azonosítására alkalmas kódok összefoglalása

Az FS keretszinkronizációs kód ismert bitszekvenciája segít a (keretszinkronizálás mellett) vett jel szabványának beazonosításában, melyet többféle szabványhoz tartozó ismert keretszinkronizáló bitsorozattal is össze tudunk hasonlítani. Ennek megállapítása után a hálózat (átjátszó) azonosítására a 12 bites hálózat hozzáférési NAC kód vizsgálata alapján van lehetőség, melyet a felhasználó szabadon programozhat. A hálózaton belüli hívócsoport azonosításra az LC hívásvezérlő csatornán belüli 16 bites beszédcsoport azonosító TGID kód, míg az egyedi készülékek azonosítására a 24 bites hívó és hívott fél Source és Destination ID azonosító kódjai szolgálnak. Ezek szintén szabadon programozhatók. Az LSD logikai csatornából kinyerhetők a GPS helyzetinformációk, ha alkalmaznak ilyet az átvitelnél.

A DMR RENDSZER

A DMR rendszer az ETSI[36] által 2005-ben kidolgozott szabványokon alapul. A DMR egy digitális 12,5 kHz-es 2 időréses TDMA alapú rendszer, melyet a TS 102 361 szabványcsoport [15] definiál, melynek három szintjét különbözteti meg az ETSI:

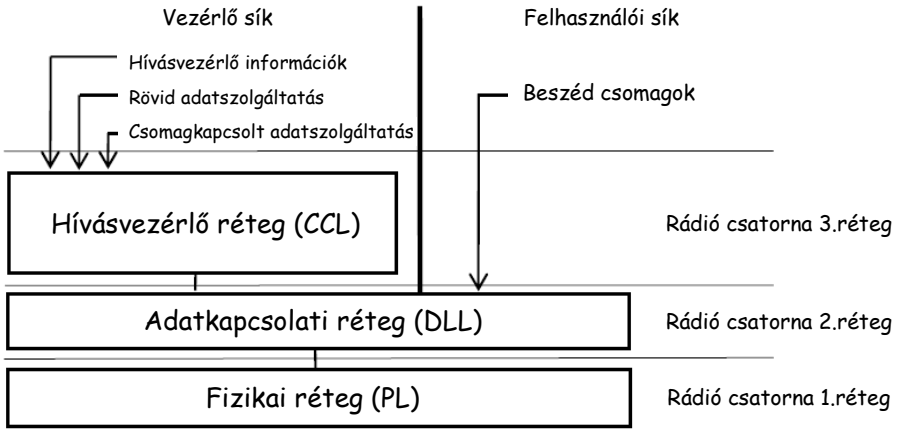
- Tier 1: Alacsony költségű, *engedélymentes* sávú, peer to peer (közvetlen kapcsolatú), infrastruktúra nélküli digitális szabvány,
- Tier 2: Professzionális felhasználású peer to peer és repeater módú (átjátszó alkalmazásával) szabvány az *engedélyköteles* sávokban történő használatra,
- Tier 3: Trönkölt rendszerű szabvány az *engedélyköteles* sávokban történő használatra.

A DMR szabványok egy jól skálázható rendszert alkotnak, és számtalan olyan plusz szolgáltatást nyújtanak, amire analóg társaik nem képesek kifinomult hívásvezérlési funkciók, rövid szöveges és adat üzenetek küldése, csomagkapcsolt IP-alapú adatátviteli lehetőségének biztosítása, teljes duplex beszédátvitel vagy beszéd és adat típusú információk egyidejű továbbítása a rádiócsatornán, hogy csak a fontosabbakat említsem. A fentiek közül nem minden funkciót és szabványban definiált megoldást valósítanak meg az egyes szabványkategóriák, ezek skálázva vannak az egyes szintekbe beépítve illetve az egyes készülékgyártók implementációi is eltéréseket mutatnak.

A DMR szabvány általános protokoll felépítése

A DMR szabványcsalád protokoll felépítése teljesen hasonló a dPMR felépítéséhez. Ezeknél 3 szintű rétegben, rétegenként eltérő funkciókat valósítanak meg, az alábbi, 5. ábrának megfelelően. A protokoll felépítés eltér az OSI 7 rétegű modelltől, amennyiben itt csak 3 réteget használnak.

[35] MI: Message Indicator – szinkronizáló bitsorozat a titkosító kulcsgenerátorhoz, 1-2-3-4 típusú ALGID esetén
[36] ETSI: European Telecommunications Standards Institute – Európai Távközlési Szabványosítási Intézet



5. ábra: A DMR protokoll /ISO/OSI/ felépítése [16, p. 18.szerző által szerkesztett]

A rádiócsatornán (Air Interface) a fizikai rétegen (PL[37]), az adatkapcsolati rétegen (DLL[38]) és a hívásvezérlő rétegen (CCL[39]) keresztül a *vétel szempontjából megvalósított* rádiófunkciók a következők: [16]

A *fizikai rétegen keresztül (1. réteg)* valósul meg: az RF jel vétele, a 4FSK demodulálás, a frekvencia és szimbólumszinkronizálás, a bit-, és szimbólum helyreállítás.

Az *adatkapcsolati rétegben (2. réteg)* alapvetően logikai kapcsolatokat kezelnek, ez a réteg „rejti el" a fizikai réteget a hívásvezérlő réteg elől. Itt kerülnek végrehajtásra a következők:

- a csatorna dekódolása hibajavítása, azaz a FEC40, CRC41 kódolások alapján az átviteli hibák javítása a bitsorrend-visszarendezés42 (az adásnál történt bitszétkenés inverz folyamataként);
- a szuperkeretek és keretek szinkronizálása visszaállítása, burst és paraméter visszaállítás;
- a kapcsolat (forrás és cél) címének megállapítása (a hívásvezérlő rétegen keresztül);
- felületet biztosít a beszédalkalmazások (beszédkódoló adatok) számára a fizikai réteg irányából; adathordozó szolgáltatásokat biztosít, és végül a jelzésrendszer és/vagy felhasználói adatok cseréjét biztosítja a hívásvezérlő réteggel.

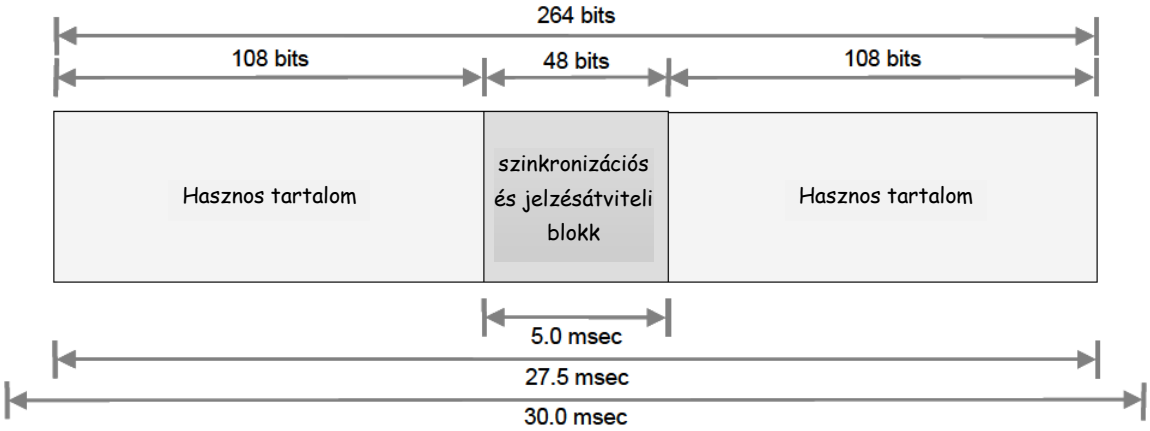
A *hívásvezérlő rétegben (3. réteg)* történik:

- a bázisállomás vagy átjátszó aktiválása-deaktiválása;
- a hívásvezérlés (hívások létrehozása, fenntartása, lezárása);
- az egyéni vagy csoporthívások, kezelése;
- a cél címzése (DMR ID vagy valamilyen átjáró /átjátszó);
- a beépített szolgáltatások támogatása: pl. vészjelzés, késői hívásbelépés43 stb. kezelése;
- az adathívások vezérlése.

[37] PL: Physical Layer – Fizikai réteg
[38] DLL: Data Link Layer – Adatkapcsolati réteg
[39] CCL: Call Control Layer – Hívásvezérlő réteg
[40] FEC: Forward Error Correction – hibakorlátozó kódolás inverz művelete a hiba ellenőrzési és javítási eljárása
[41] CRC: Cyclic Redundancy Check – hibadetektáló kódolás inverz folyamata, a CRC ellenőrzése
[42] de-interleaving – a bitszétkenés inverz folyamata, ahol helyreállítjuk a bitek eredeti sorrendjét (ennek az a célja, hogy az átvitel során fellépő csoportos hibák, a visszarendezés után ne egymás mellé essenek, így a csoportos hibákat különálló bithibákká alakítjuk, aminek a korrigálása sokkal egyszerűbb és hatékonyabb)
[43] Late entry call: /a DMR szolgáltatása/ amikor egy már kisugárzott adást nem az elejétől veszünk, hanem közben lépünk be a kommunikáció vételébe.

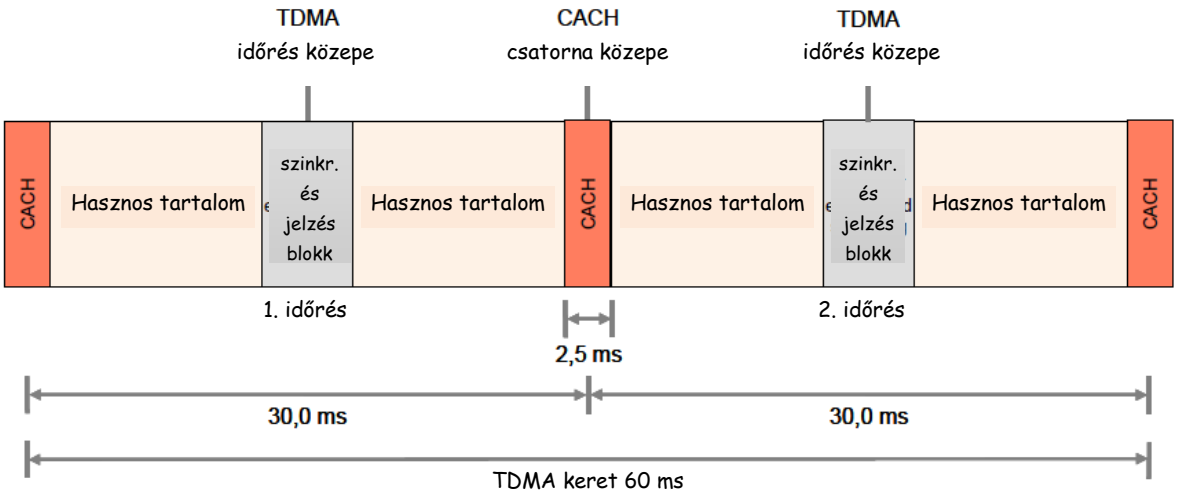
A DMR szabvány logikai csatornái keretszervezése

A DMR rendszer alapvető egysége a TDMA időrés (6. ábra) ami 27,5 ms (védősávval együtt 30 ms) hosszú összesen 264 bitet tartalmazó struktúra. Egy időrés 3x20ms (60 ms) tömörített beszédinformációnak megfelelő, 3x72 bit beszédkódoló kimenő keret hibajavítással (FEC) ellátott információs bitjeit viszi át. Ezek kitöltik a 2x108=216 bit hasznos időrés tartalmat (payload). A maradék 48 bit a keret közepén elhelyezkedő szinkronizációs és jelzésátviteli blokk. Ennek speciális tartalma a szinkronizációs bitsorozat (Sync pattern) melynek kiemelkedő jelentősége van a vétel szempontjából mind hardveres, mind szoftveres vevőimplementáció esetén. A vétel során segít a címzettnek az adás detektálásában és az adóra történő időbeli szinkronizációban, a kommunikáció- tartalmának (beszéd/ adat/ vezérlő/ visszirányú-csatorna információk) és irányának (felmenő/lejövő) megállapításában.



6. ábra: A DMR időrés felépítése [16, szerző által szerkesztett]

Két időrés (1, 2) alkot egy 60 ms-os TDMA keretet (7. ábra), melynek időrései között 2,5 ms-os védő „sávok" vannak. Ezeket egy külön jelzésátviteli logikai csatorna a CACH[44] átvitelére használják, de csak az átjátszók által küldött keretek szüneteiben (lásd később a 10. ábránál). A 24 bites CACH csatornát a felmenő csatorna (keretek) TDMA keretszám aktuális értékének és foglaltságának jelzésére, illetve kissebességű jelzésátvitelre az un. lassú összeköttetésvezérlő csatorna átvitelére alkalmazzák az átjátszók/ismétlők esetében.



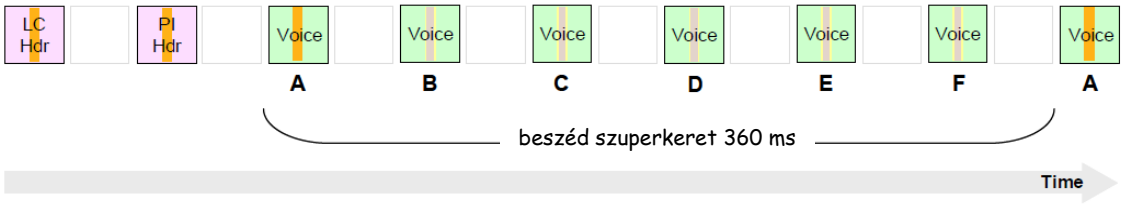
7. ábra: A DMR keret felépítése [16, szerző által szerkesztett]

[44] CACH: Common Announcement Channel – Közös szóró vagy hirdetmény csatorna

A tömörített beszédinformációt valamint a jelzésinformációkat kódolás és hibavédelemmel történő kiegészítés után egységes időrés-keret-szuperkeret formátumba szervezik a kisugárzás előtt. Az egyes csomagok fejlécekkel vannak ellátva amelyek a hívásvezérlő és a címzési információkat tartalmazzák. A csomagok többi része pedig a tömörített (vocoded) beszédinformációt tartalmazzák. Ez hasonló struktúra mint amit az internet protokoll (IP) adatcsomagok esetében alkalmaznak. A hasznos csomagok (payload frame) éppen ezért az IP csomagok egyszerű és alternatív formái a DMR rádiók esetében. A fejlécek információi periódikusan kisugárzásra kerülnek, ami megbízhatóbbá teszi a jelzésátvitelt, emellett pedig lehetővé teszi a vételbe később bekapcsolódó rádiók számára a kommunikációba történő utólagos részvételt/behallgatást (late entry).

A beszéd szuperkeretek, a beszéd inicializálása és befejezése

A beszéd keretek 360 ms-os szuperkereteket alkotnak, (8. ábra) melyek összesen 6 keretet tartalmaznak, ezeket A-F-ig betűvel jelölik. A hagyományos (nem trönkölt) rendszerekben a beszédkisugárzás kezdetét, mindig bevezető keret(ekkel) kezdjük. Ezek közül az LC[45] (Voice LC Header) fejléc mindig kisugárzásra kerül, amelyik jelzi a beszéd kezdetét és címzésinformációt is hordoz.



8. ábra: Beszédátvitel inicializálása az LC és PI fejlécekkel [16]

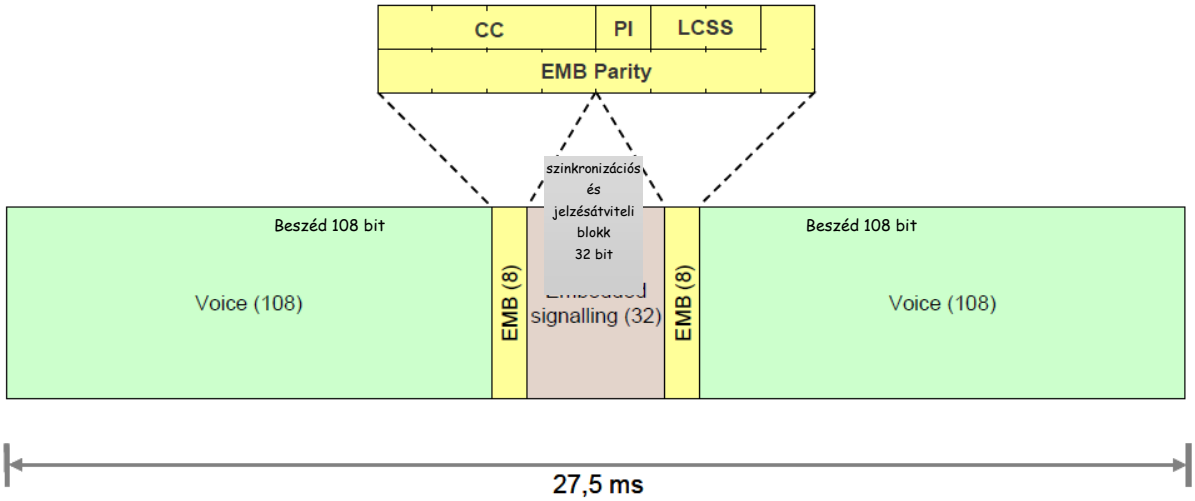
Az LC bevezető keret tartalmazza a kommunikáció felépítéséhez szükséges alapvető információkat, melyeket az átvitel során más helyeken is megismételnek, pl. a CACH csatorna CSBK[46] jelzésblokkjában, a beszédcsomagok fejlécében, stb. Ez magába foglalja a beszéd és egyéb társított jelzésinformációkat, pl. a szín kódot (CC[47]) ami az átjátszót vagy a hálózatot azonosítja, a beszédcsoport azonosítót (group ID), az egyedi készülékazonosítót (forrás és cél ID-t – source/destination ID), az üzenet típusát (call type) stb.

A PI[48] (ami mindig az LC után következik) csak abban az esetben kerül kisugárzásra, ha az üzenet titkosított. Ez un. Privacy Indicator Information tartalmú burst, a hiánya jelzi, hogy nyílt, míg kisugárzása, hogy kódolt tartalmú az üzenet.

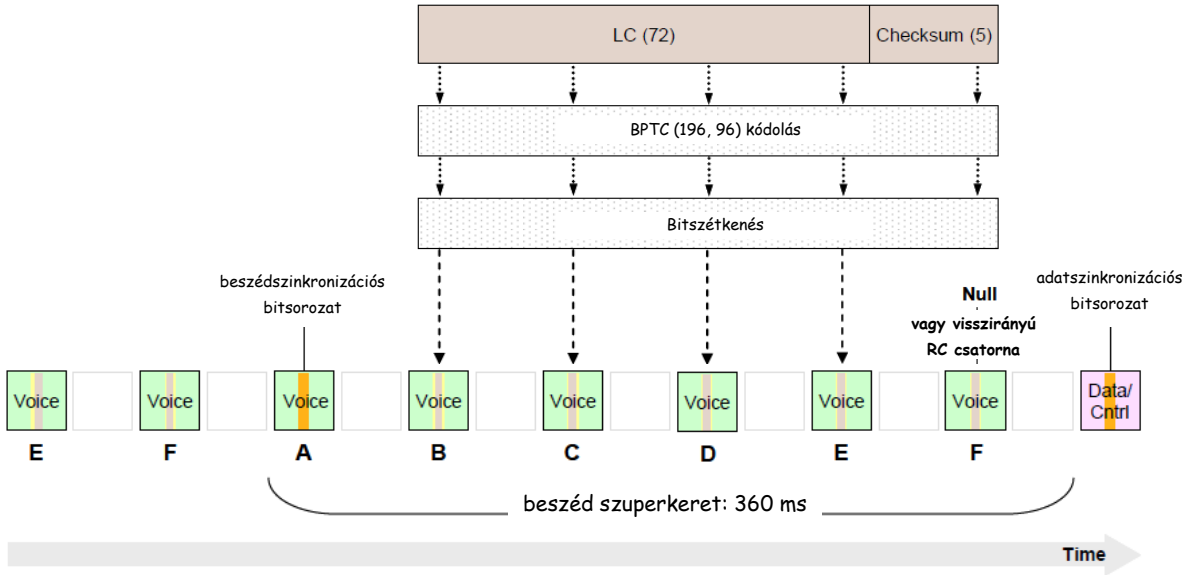
Ha csak később kapcsolódunk be egy beszélgetésbe, abban az esetben is tudjuk venni az üzeneteket, un. *late entry azaz késői belépés* lehetőségével, mivel a szupekeretek minden „A” jelű kerete közepén beszédszinkronizációs (Voice Sync) 48 bites bitsorozat kerül kisugárzásra (a 9. ábrán látható zöld részek között), míg az B-F keretekben az időrések közepén a 32 bites (szinkronizációs és jelzésátviteli blokkban) 4 időrésben elosztva összesen 128 biten, beépített adat (Embedded signalling) formájában kerül átvitelre az LC összeköttetésvezérlő csatorna 72 hasznos bitje hibavédelemmel kiegészítve, ahogyan ez a 10. ábrán látható. A 2x8=16 bites EMB[49] mező tartalmazza a 4 bites CC színkódot, az 1 bites PI[50] indikátort, a 2 bites LCSS[51]

[45] LC: Link Control - Összeköttetés vezérlés
[46] CSBK: Control Signalling Block – vezérlőjel átviteli blokk
[47] CC: Colour Code – színkód, az azonos földrajzi területen üzemelő egymástól független hálózatokat azonosítja
[48] PI: Privacy Indicator – az összeköttetés védelmére vonatkozó információ
[49] EMB: EMBedded signalling field -
[50] PI: Pre-emption and power control Indicator – foglaltsági és teljesítményszabályozási jelző bit (itt más a jelentése mint a PI bevezető keretnél, lásd a 47. lábjegyzetnél fentebb)

jelzi, hogy az időrés tartalmaz-e kezdődő /befejeződő /folyamatban-lévő LC vagy CSBK jelzésátvitelt. A maradék 9 bit az előzőek paritását képezi. A 32 bites Embedded Signalling lehet LC átvitel, RC átvitel, vagy null üzenet. Az LCSS ennek információtartalmára vonatkozik.



9. ábra: Beszédkeret beépített jelzésátviteli blokkal /szuperkeret B-F keretekben/ [16, szerző által szerkesztett]



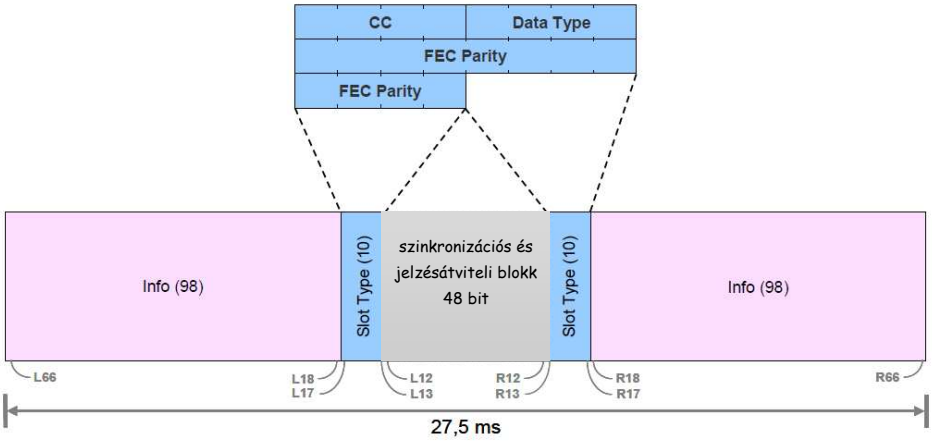
10. ábra: LC átvitele a B-F keretekben és a beszédátvitel befejezésének jelzése [16, szerző által szerkesztett]

A beszédinformáció annyi egymás utáni szuperkeretben kerül átvitelre, amennyi szükséges a teljes információtartalom átviteléhez, majd a legutolsó szuperkeret végén egy befejező adatkeret (Voice LC Terminator) kerül átvitelre, adat szinkronizációs bithátter tartalommal. Az adatkeret jelzi a vevőnek a beszélgetés befejezését, ahogyan ez a 10. ábrán látható.

[51] LCSS: Link Control Start/Stop – az összeköttetés vezérlő csatorna (LC) időbeli állapotát jelző bitek

A bevezető és befejező keretek felépítése tartalma

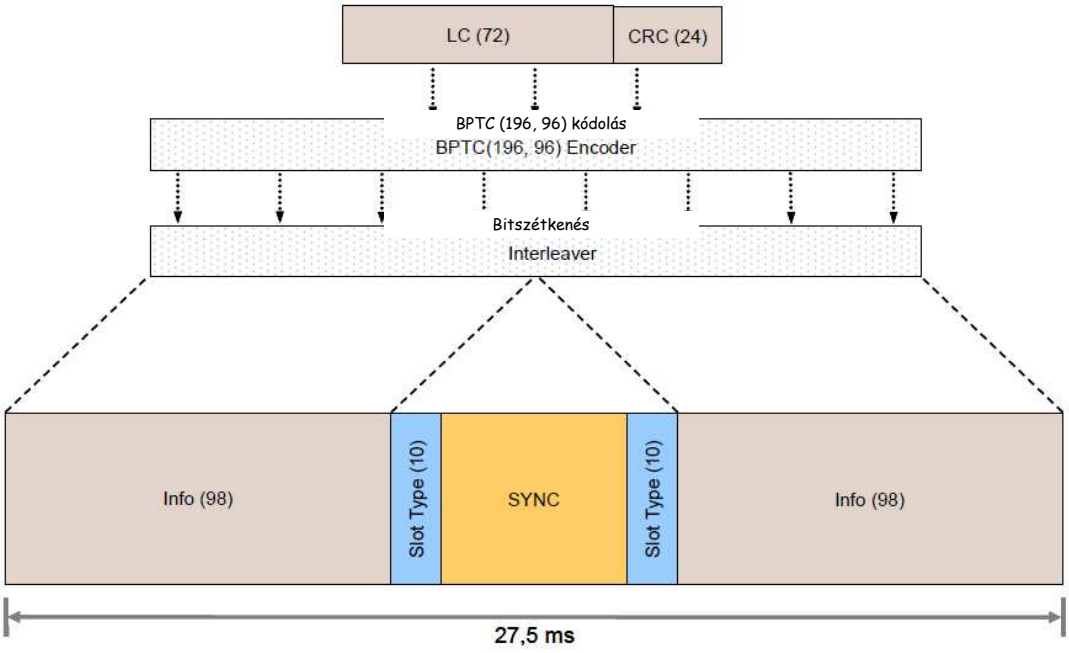
A kommunikáció elejét jelző *bevezető és* a végét jelentő *befejező keretek* a normál beszédkeretek felépítésétől kissé eltérő un. jelzés és adatkeret formátumban kerülnek átvitelre. Ezek a beszédkeretek 2x108 bites hasznos tartalma helyett, csak 2x98=196 bitnyi hasznos információt hordoznak, azonban az időrés közepén lévő szinkronizációs és jelzésátviteli blokkot két oldalról keretező 2x10 bites keret típus (slot type) mezővel egészítik ki, így az időrés 264 bites összes bitszáma nem változik. Ennek általános formátuma látható a 11. ábrán.



11. ábra: Általános adatburst felépítése [16, szerző által szerkesztett]

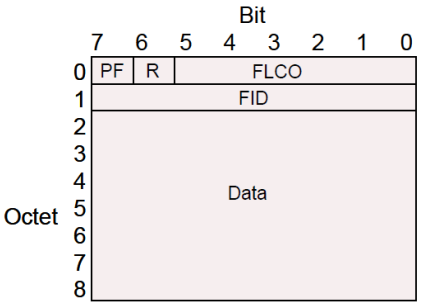
Az összesen 2x10=20 bites Slot Type mező definiálja az időrés összesen 196 bitnyi hasznos információtartalmát. Ezen belül is a 4 bites adat típus (Data Type) mező határozza meg a burst konkrét típusát pl. 0001: bevezető keret (Voice LC Header), 0000: védelemjelző keret (PI header), 0010: befejező keret (Terminator with LC), 0011: CSBK, stb.

Bevezető és befejező keret esetén a 2*98=196 bites információs bitek tartalmazzák a 72 hasznos bitet tartalmazó LC biteket, melyek 24 bit CRC kód és BPTC kódolás valamint bitszétkenés után kitöltik a 196 bitet, ahogyan ez a 12. ábrán látható.



12. ábra: Bevezető és befejező adatburst felépítése kódolása [16, szerző által szerkesztett]

A 72 hasznos bitet tartalmazó LC felépítése a következő 13. ábrán láthatóak szerint alakul



Information element	Length	Remark
Message dependent elements		
Protect Flag (PF)	1	
Reserved	1	This bit shall be set to 02
Feature elements		
Full Link Control Opcode (FLCO)	6	
Feature set ID (FID)	8	Shall be set to 000000002
Service Options	8	
Target address	24	
Source address	24	

13. ábra: Bevezető és befejező adatburst felépítése [17]

A 72 bites LC csatorna 9 oktetből (8 bites blokkokból) áll. [18]

A nulladik oktet sorában a PF[52] a védelem jelző bit, az R[53]: későbbi használatra fenntartott bit (0 értékű), a 6 bites FLCO[54]: teljes összeköttetés vezérlő műveleti kód, ami a rádiócsatorna funkciókat azonosítja adott FID[55] esetén.

Az első oktet 8 bites FID: funkciókészlet (szolgáltatáskészlet) azonosítója jelzi, hogy ETSI szerinti szabványos LC csatornáról van szó ekkor SFID[56], vagy gyártó specifikus un. MFID[57] tartalmú az adat (Data) mező tartalma.

A 2-8. oktet az adat mező (Data), ami felhasználó specifikus információkat tartalmaz: a 2. oktet a 8 bites szolgáltatás opció kód, a 3-8 oktet (48 bit) pedig a hívás típusától függő 24 bites címzési azonosítókból tartalmaz kettőt. *Csoport hívás esetén* a hívócsoport azonosítására szolgáló csoport azonosítót (Group address) és az adást kisugárzó rádió azonosítóját a (Source address) értékét tartalmazza. *Egyedi hívás esetén* pedig a célrádió címét (Target Address) valamint a forrás (Source address) értékét tartalmazza. [18]

A DMR címzési módjai, hálózati és szolgáltatásazonosítással kapcsolatos kódok

A DMR esetében alapvetően kétféle címzési módot definiál a szabvány: az egyik a *csoportcímzés*, amivel a hívócsoportokat azonosítják a benne lévő készülékek számára, megkülönböztetve a más csoportoknak szóló üzeneteket (pont-többpont kommunikáció). A másik az *egyedi címzés*, ami egyedi rádiókészülékeket azonosít, amivel egyéni hívásokat (pont-pont kommunikáció) kezdeményezhetünk egy csoporton belül, de adott esetben csoporton kívül is. További hálózatazonosításra szolgáló kód a 4 bites CC vagy színkód, amit az azonos vagy átfedő földrajzi területen működő, de eltérő hálózatok (átjátszók, vagy direkt kommunikáció esetén hívócsoportok) megkülönböztetésére használnak. Hasonló a funkciója, mint az analóg rendszereknél alkalmazott szelektív hívókódoknak (CTCSS[58], DCS[59]). A CC speciális értéke az 1111 bináris kód, amit direkt módú összeköttetésnél alkalmaznak.

A DMR szabványban a rádió egyedi azonosítója ID-je és a csoport ID is 24 bites azonosító, ami 1 és 16.776.415 közé eső szám lehet, ahogyan ez a szabvány ETSI 102-361-1 címzési eljárásokat bemutató táblázatában látható [16, p.117.]. Ezek értékét hexadecimális formában tartalmazza a táblázat. Az általános gyakorlat szerint a rádiók egy flottában folytonos ID tartományt képeznek, de ezt a felhasználó szabadon programozhatja.

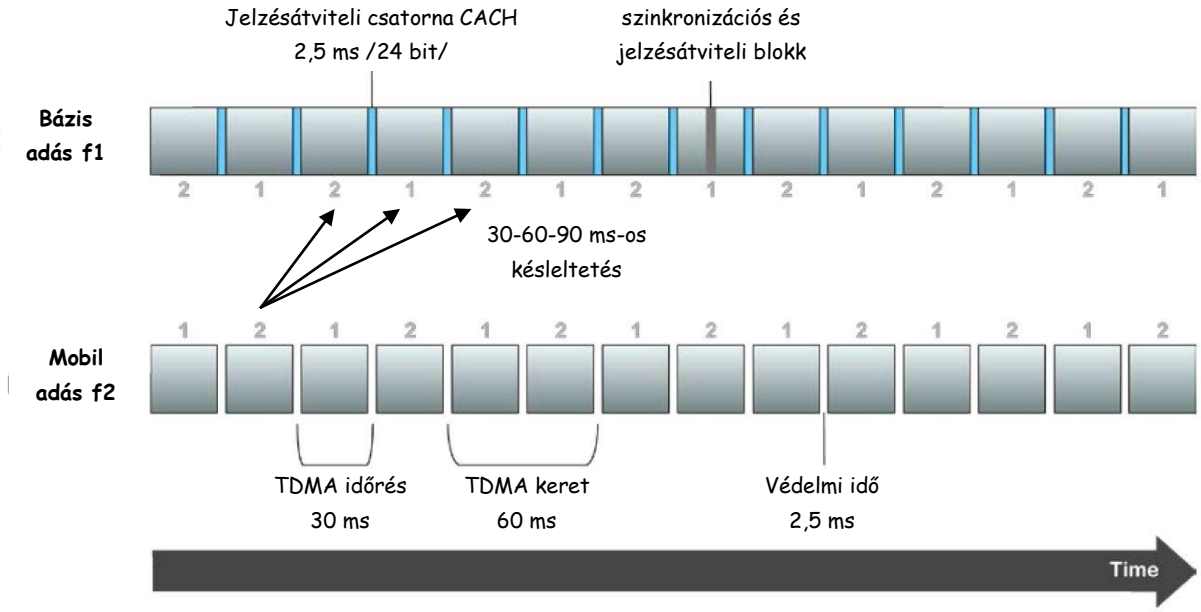
---

[52] PF: Protect Flag – védelem jelző bit
[53] R: Reserved – fenntartott bit /későbbi használatra/
[54] FLCO: Full Link Control Opcode – teljes összeköttetés vezérlő műveleti kód
[55] FID: Feature Set ID – funkciókészlet azonosító
[56] SFID: Standardized feature set ID – szabványos funkciókészletű LC csatorna
[57] MFID: Manufacturer's Specific Feature set ID – gyártóspecifikus funkciókészletű LC csatorna
[58] CTCSS: Continuous Tone Coded Squelch System – folyamatos alacsony frekvenciával kódolt zajzár
[59] DCS: Digital Coded Squelch – digitálisan kódolt zajzár

Két és egyfrekvenciás működési mód időzítése csatorna használata

Az összeköttetés frekvenciahasználata különféle szabvány által biztosított módozatokban lehetséges. Így megvalósítható a Tier2. szerinti átjátszón keresztüli egy és kétfrekvenciás működésmód, továbbá a Tier2 és a Tier1 szerinti közvetlen vagy direkt módú összeköttetések is (trönkölt rendszereket nem vizsgálok). Ezek leírását ismertetem beszédátvitel esetében a következőkben, mivel ezek ismerete a felderítés és azonosítás szempontjából lényeges.

A 14. ábra egy *átjátszón keresztüli kétfrekvenciás* átvitelt ábrázol, ahol az adásra és a vételre eltérő frekvenciát alkalmaznak. A két időrés kihasználása többféle konfigurációban lehetséges, ekkor 30 vagy 60 ms-os késleltetés van az átvitelben. Az első esetben eltolt, míg a másodiknál igazított csatorna (keret) szervezésről beszélünk. Azonban létezik *egyfrekvenciás* átjátszási működési mód is, ekkor un. kétirányú csatornáról beszélünk (bi-direction channel). Ebben az esetben, az első időrésben a bázis-mobil, míg a másodikban a mobil-bázis irányú (vagy fordítva) kommunikáció zajlik megfelelő késleltetéssel. A második időrés azonban visszirányú jelzéscsatornaként RC[60] is alkalmazható.



14. ábra: Kétfrekvenciás DMR adásmód keretszervezése [19, szerző által szerkesztett]

Azonban a témám szempontjából fontosabb *közvetlen módú* (átjátszó nélküli) *egyfrekvenciás* kommunikáció esetén csak az egyik időrés használható különálló beszédátvitel céljára, így itt nem érvényesül a TDMA spektrális hatékonysága. Közvetlen vagy direkt módú kommunikáció esetében a rádiók azonos frekvencián un. aszinkron módban kommunikálnak egymással, mivel nincs infrastruktúra (bázisállomás, vagy átjátszóállomás), ami időbeli szinkronizálást biztosítana a számukra az időrések tekintetében [16, 20].

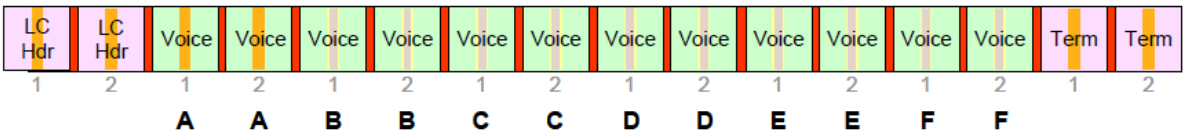
Emiatt, az ilyen rendszerek esetében szükséges valamilyen módon megoldani az ütközések elkerülésének problémáját. Analóg rádiók esetében elképzelhető, hogy mindkét azonos frekvencián egy időben sugárzott adás vehető, még ha torzítottan is, digitális adásoknál azonban a BER leromlása miatt egyik adás sem lesz sikeres. Ezen felül az adást egyszerre elindító digitális rádiók egyike sem lehet biztos abban, hogy az adásuk elérte a célcsoportot. Ennek esélye annál nagyobb, minél több rádió működhet a csoportban. Ötnél több rádió esetében már jelentősen megnő az adásütközések esélye. Emiatt a közvetlen módú

[60] RC: Reverse Channel – visszirányú jelzéscsatorna

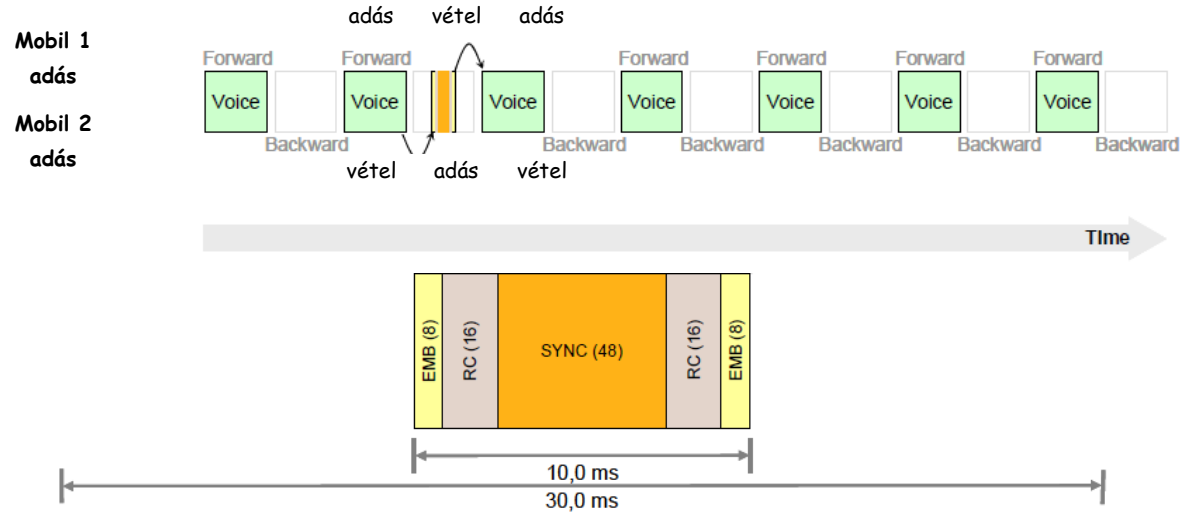
kommunikáció esetére olyan monitoring algoritmust kellett kidolgozni, ami figyeli a rádiócsatorna aktuális foglaltságát és segít elkerülni az adásütközéseket. A Motorola cég 2016 februári amerikai szabványbejegyzése ennek megoldására vonatkozik [21].

Ekkor az adást elkezdő rádió aszinkron időzítésű kisugárzásához szinkronizálódnak a hatókörzetében azonos csoportban lévő készülékek. Ha egy mobil adásra készül, előtte belehallgat a környezetébe a saját color code, vagy csoport ID azonosítóval ellátott adásokat keresve. Ha adást talál, akkor elkezdi dekódolni azt, hogy megtudja a forrás ID-jét azaz az adást sugárzó rádió azonosítóját. A rádió ID az adás elejét jelző LC (Link Control) burstben, vagy a beépített LC burstben, a beszédcsomagok fejlécében (voice header), vagy a CACH-ba beépített CSBK jelzésblokkban, illetve egyéb további adatcsomagokban is megtalálható (lásd ezeket fentebb).

A Tier 1 típusú (engedély nélkül alkalmazható készülékeknél) a másik időrésben összekötetés esetén az elsővel megegyező tartalmú adatok vannak duplikálva ez az úgynevezett folytonos kisugárzású mód (15. ábra). Míg Tier 2 kategória esetén a második időrés csak jelzésátvitelre használható direkt módban. Ez a 96 bites közvetlen módú visszirányú jelzésátviteli csatorna (Direct mode RC - Reverse Channel) 16. ábra, ami természetesen nem csak a közvetlen de az átjátszón keresztüli üzemmód esetében is alkalmazható Az EMB mező tartalma megegyezik a 9. ábránál részletezett EMB tartalommal. Az ETSI DMR Tier 2. szabvány írja le a lehetőségeket. Ezzel különféle professzionális szolgáltatások vitelezhetőek ki, mint a prioritásos hívások, a rádiók távvezérlése, vészhívások bonyolítása stb.



15. ábra: Közvetlen módú egyfrekvenciás folytonos adásmód keretszervezése Tier 1. esetén [16]



16. ábra: Közvetlen módú egyfrekvenciás adásmód keretszervezése és a visszirányú jelzéscsatorna (RC) felépítése Tier 2. esetén [16, p. 36, szerző által szerkesztett]

A keretszinkronizáció (Sync) folyamata és jelentősége a vétel és felderítés szempontjából

A kommunikáció során a bevezető és befejező keretek, az „A” jelű időrések továbbá a fentebb látható visszirányú jelzéscsatorna egyaránt tartalmazza a 48 bites, időrések közepén elhelyezkedő szinkronizációs bitsorozatot. Ezek segítik a vétel során a keretszinkronizálás folyamatának lebonyolítását, az időrések megtalálását, mivel annak közepén helyezkednek el. Átjátszón keresztüli üzemmód esetében mindig az átjátszó (BS – Base Station) időzítéséhez szinkronizálódnak a mobil vagy kézi rádiókészülékek (MS – Mobile Station) a rendszerben. Közvetlen/direkt módú kommunikáció esetén az adást kezdeményező MS lesz az időzítési referencia, az ellenállomások hozzá igazodnak.

Ha sikerült elérni az időbeli, azaz a bitszerinti szinkronizálást, vagyis a csatornára szinkronizáltuk a vevőt és annak időzítését, megindulhat az információtartalom visszanyerése. A vétel során a speciális tartalmú szabványban definiált szinkronizációs bitsorozatok segítenek megállapítani a vevő részére az alább felsorolt eseményeket/tényeket.

- azonosítják az időrések hasznos tartalmát (payload) a következő módokon:
    - elkülönítik a beszéd és adat vagy vezérlő jel tartalmú időréseket valamint a visszirányú csatorna (RC-Reverse Channel) tartalmat egymástól;
    - megkülönböztetik a mobiltól vagy a bázistól származó jeleket;
    - azonosítják, hogy átjátszótól, vagy közvetlen módú készüléktől származik a kisugárzott jel;
    - azonosítják /elkülönítik/ a TDMA közvetlen módú összeköttetés 1. és 2. időrését.
- a szinkronizációs bitek alapján a következő szinkronizációs bitsorozatokat (SYNC Pattern) definiálták a szabványban, amelyek az időrések tartalmára utalnak:
    - Átjátszótól származó beszéd /BS sourced voice/;
    - Átjátszótól származó adat /BS sourced data/;
    - Mobiltól származó beszéd /MS sourced voice/;
    - Mobiltól származó adat /MS sourced data/;
    - Mobiltól származó egyedi visszirányú adat /MS sourced standalone RC/;
    - TDMA közvetlen módú beszéd az 1. időrésben;
    - TDMA közvetlen módú adat az 1. időrésben;
    - TDMA közvetlen módú beszéd az 2. időrésben;
    - TDMA közvetlen módú adat a 2. időrésben.

A fenti adattartalmakat azonosító szinkronizációs bitek megállapításával tudják a dekódoló programok megállapítani, hogy milyen jelet vettek és azt hogyan kell a tartalmuknak/jelentésüknek megfelelően tovább feldolgozni.

A fentiek alapján látható, hogy a DMR de a P25 szabvány is meglehetősen összetett a TDMA működésmód miatt, és az IP alapú adatátvitellel és adatcsomagok felépítésével nem is foglalkoztam, csak a beszédinformációk átvitelét elemeztem, mivel ez volt az eredeti célkitűzésem. Azonban a beépített jelzésátvitelnek és az ismert paraméterű (szabványokban definiált) hibakorlátozó és hibajavító kódolásoknak köszönhetően megfelelő vevőmegoldásokkal lehetséges a DMR és más TDMA típusú jelek dekódolása, a megfelelő egyedi azonosítók kinyerése, illetve ha az adott típusú beszéddekódoló is rendelkezésre áll, akkor a beszédinformáció visszaállítása is a digitális jelfolyamból. Természetesen azt feltételezve, hogy nem alkalmaznak kiegészítő titkosítást az átvitel során. Azonban olcsóbb rendszerek esetében ez jelentősen megdrágíthatja a rendszerek vagy egyedi készülékek árát, ezért ennek alkalmazása ezeknél anyagi megfontolást is igényel, ahogyan ezt egy publikációmban [22] kifejtettem.

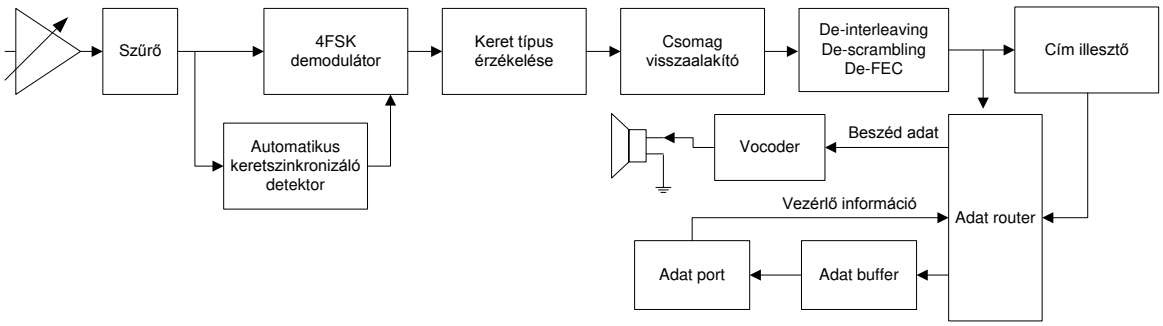
A DMR alapú digitális PMR szabványok alapsávi jelfeldolgozása

Az adott rádiószabvány protokolljának megfelelően létre lehet hozni egy valódi jelfeldolgozó struktúrát, ami hardveres, tisztán szoftveres, illetve hibrid (hardver+szoftver) felépítésű is lehet. A lehetséges megoldásokat egy későbbi cikkben fogom áttekinteni. A DMR adásmódok vételi mechanizmusa teljesen hasonló, azonban a 4FSK, illetve P25 esetén a C4FM demodulátor frekvenciaeltolás paramétereik különböznek egymástól, valamint a keretszervezésben és a logikai csatornák típusában és felépítésében is vannak eltérések. A következő 2. táblázat a 4FSK/C4FM moduláció paraméterek eltéréseit foglalja össze. [12],[13],[14],[16]

1. táblázat: A TDMA szabványok modulációinak frekvencia-eltérés összehasonlítása

		C4FM	HCPM, HDQPSK	4 FSK	
Dibit	Szimbólum	P25 P.I. C4FM	P25 P. II. HCPM HDQPSK	DMR 4FSK	PDT 4FSK
01	+3	+ 1800	Nem értelmezhető, mert nem 4 állapotú	+1944	+n.a.
00	+1	+ 600		+648	+n.a.
10	-1	- 600		-648	- n.a.
11	-3	- 1800		-1944	- n.a.

Ennek ellenére a vétel folyamata – mely a felderítés szempontjából leginkább érdekel bennünket – egymástól jól elkülöníthető részfeladatok sorozatára bontható fel. A DMR típusú szabványok digitális vételéhez a 17. ábrán látható univerzális felépítésű struktúra rádióvevő alkalmazható [23], amelyik csak az alapsávi jelfeldolgozás folyamatát mutatja be, az RF vevőrészek ismertetése nélkül. A rádiófrekvenciás vevő tetszőleges kivitelű lehet, pl. direkt konverziós vevő, vagy valamilyen szélessávú szoftverrádió, de akár keskenysávú hagyományos vevő is.



17. ábra: A DMR vevő általános logikai felépítése [22, szerző által szerkesztett]

A fenti elrendezésnek megvalósítható mind a hardveres, mind a szoftveres implementációja. Mindkét esetben a különféle szabványok feldolgozási paramétereit kell megváltoztatni (a különálló blokkoknál) az egyes eltérő szabványoknak megfelelően. Erre a kézenfekvő megoldást a szoftverrádió (SDR) technológia jelenti, azonban az alkalmazott hardvertől függően ennek kivitelezése a gyakorlatban többféle módon történhet: hagyományos mikroprocesszorral, DSP[61], FPGA[62], a CML Microcircuit cég által alkalmazott

[61] DSP: Digital Signal Prosessor

FirmAsic[63] technológia segítségével. Ez utóbbi a legújabb CMX7341 típusú rendszercsip segítségével szinte az összes típusú analóg és digitális PMR szabvány vételére képes [24].

A szoftveres megoldások közül a DSD Plus alkalmazást említeném meg [25], amelyik akár egy olcsó szélessávú rádióvevő komplex kimenőjelét is képes feldolgozni egy hagyományos számítógéphez csatlakoztatva annak digitális kimenetét és annak jelét az említett szoftverrel feldolgozva. A program képességei láthatók a következő 18. ábrán:

Event Log Features

FORMAT	Voice	CC-Decode	Radio ID	Talkgroup	Access Code	Time-Slot	GPS Data
DMR	YES	YES	YES	YES	CC	YES	YES
D-STAR	NO						
IDAS	YES	NO	YES	YES	RAN	N/A	
NXDN	YES	YES	YES	YES	RAN	N/A	
P25	YES		YES	YES	NAC	N/A	
ProVoice	YES		YES	YES			
X2-TDMA	YES					YES	

18. ábra: A DSD plus szoftver képességei [25]

A KOMMUNIKÁCIÓS ELLENŐRZÉSSEL KINYERHETŐ INFORMÁCIÓK

A rádiók egyedi modulációs paramétereiből kézi, vagy automatikus jelelemzés segítségével megállapíthatók az 1. táblázatban összefoglalt modulációs paraméterek 4FSK frekvencia-eltérések. Ezekből és más egyéb paraméterekből pl. a 48 bites ismert keretszinkronizációs bitsorozatokból (P25 és DMR esetében egyaránt) következtetni lehet az adás szabványára, továbbá a DMR-nél részletesen leírt (de a P25-nél is nagyrészt érvényes) egyéb információkra pl. az adás irányára (felmenő, lejövő, közvetlen módú), az aktuális átvitel tartalmára (beszéd, adat, vezérlőjel), a használt TDMA időrés számára.

A hálózat vagy átjátszó azonosítására a P25 esetében a 12 bites NAC kód, míg DMR-nél a 4 bites CC színkód szolgál az analóg rendszereknél alkalmazott CTCSS és DCS kódokhoz hasonlóan. Ezek elkülönítik az azonos földrajzi területen működő, de egymástól független hálózatokat, de egyéb információt is jelenthet adott értékük, pl. direkt módú összeköttetésre utalhat.

A hálózaton belüli hívócsoportok (felhasználók adott szempont szerinti beszédcsoportjainak) azonosítására szolgálnak a P25 esetében a 16 bites Talk Groups ID (TGID), illetve DMR esetében a 24 bites Group ID kódok. Ezek speciális értékeiből is további következtetések vonhatók le a rendszerekkel kapcsolatban, pl. a hívócsoportok számára és rendszeren belüli elérhetőségére vonatkozóan.

Az egyedi készülékek azonosítására szolgálnak a P25-nél és a DMR-nél is egyaránt 24 bites Unit ID, melyből egyértelműen azonosítani lehet a kommunikációban résztvevő rádiókészülékeket. Két típusa van a Source ID a hívást kezdeményező (adó) címe, míg a Destination vagy Target ID a hívott fél (a vevő) egyedi címe. Az ID kódokat a felhasználók szabadon programozhatják a készülékbe.

A gyártóazonosító MFID kódok a gyártóspecifikus átvitel jellemzőire utalnak, melyek a szabványostól eltérő funkciókat is alkalmazhatnak az átvitel során.

A fentiek jóval több műveleti információt hordoznak magukban, mint az analóg rádiók vételéből származó adatok.

További információkhoz juthatunk az átvitel titkosításával, védelmével, az alkalmazott beszédkódoló típusával, illetve a kommunikáció formája, módja, tartalma tekintetében, még akkor is, ha nem tudjuk visszaállítani az eredeti hangüzenetet vagy adattartalmat.

---

[62] FPGA: Field Programmable Gate Array

[63] FirmAsic: un. Function Image-ek betöltésével konfigurálható a vevő képessége és működésmódja

ÖSSZEGZÉS

Jelen cikkben és annak első részében [1] bemutattam és összefoglaltam az FDMA és TDMA típusú elterjedtebb digitális PMR szabványok jellemzőit, működésmódját. Elemeztem és összefoglaltam a rádiófelderítés által az ilyen típusú kommunikációs rendszerekből kinyerhető technikai és műveleti információkat, melyek jóval pontosabb azonosítást tesznek lehetővé az analóg rendszerekhez képest, mind a kommunikáció módja, tartalma, mind a résztvevő felek, illetve az alkalmazott rádiókészülékek azonosító és technikai adatai tekintetében.

Az összefoglalás megfelelő technikai alapot jelent egy digitális PMR-ek univerzális vételére szolgáló összeállítás megtervezésére, illetve elvárható technikai műveleti képességeinek meghatározására, és gyakorlatban történő kipróbálására. További kutatásaimat ebben az irányban kívánom folytatni.

Felhasznált irodalom

[1] Balog Károly: Digitális PMR rendszerek összehasonlítása I., Hadmérnök IX. évfolyam 3. szám - 2014. szeptember pp. 98-112. ISSN 1788-1919; http://hadmernok.hu/143_08_balogk.pdf

[2] Trevor Laughton: China's Trunking Startegy, Tait Communications 2012 http://www.taitradio.com/__data/assets/pdf_file/0009/79605/Chinas-Trunking-Strategy.pdf (2016. 04. 27.)

[3] PDT Digital Trunking Communication Thematic Seminar Was Held In Shenzhen, 2010, 03. 23.; http://www.pdt.org.cn/Html/971/980/1762.html (2016. 04. 27.)

[4] Actec: Standard and Patent, 2014/03/27 16:58 http://www.acteccom.com.cn/en/tech/biaozhunyuzhuanli/11710.html (2016. 04. 27.)

[5] Actec, Standard and Patent, Standard introduction /2014-03-27 16:54/ http://www.acteccom.com.cn/en/tech/biaozhunyuzhuanli/11708.html (2016. 04. 27.)

[6] Pengfei Sun, Guanyuan Feng, Kai Guan and Yicheng Zhang: Comparison Between Operational Capability of PDT and Tetra Technologies: A Summary, Q.-A. Zeng (ed.), Wireless Communications, Networking and Applications, Lecture Notes in Electrical Engineering 348, pp. 179-187. Springer India 2016, DOI 10.1007/978-81-322-2580-5_18

[7] Pengfei Sun, Run Tian, Hao Xue and Ke Wan: Development and Analysis of Police Digital Trunking Channel Technology of PDT, Q.-A. Zeng (ed.), Wireless Communications, Networking and Applications, Lecture Notes in Electrical Engineering 348, pp. 189-199. Springer India 2016, DOI 10.1007/978-81-322-2580-5_18

[8] Actec, Service and Support, May I ask the overall development situation of PDT technology and products?; http://www.acteccom.com.cn/en/faq/zaixianfuwu/ (2016. 04. 27.)

[9] Professional Network Trunking Communication System, China Volant Industry Corporation www.volinco.com October, 2014.; http://emarketimg.volinco.com/file/2015/09/06/201509061058255.pdf (2016. 04. 27.)

[10] Hytera DMR Conventional Series Radios Release Notes for DMR Conventional Software Release version: 7.00, 2015. 02.; http://ham-dmr.nl/?wpfb_dl=120 (2016. 06. 18.)

[11] Excera DMR Portable Radio EP8100 Secifications
www.excera.com.cn/en/EditorV8/UploadFile/2015317104223717.pdf (2016. 06. 18.)

[12] Codan Radio Communications: P25 Radio System Traning Guide, September 2013.
www.codanradio.com/wp-content/uploads/TG-001-4-0-0-P25-Training-Guide.pdf
(2016. 07. 20.)

[13] Tait Communications: Introduction to P25, TRG-00001-01-M Issue 1 October 2015
http://www.taitradioacademy.com/courses/intro-to-p25/ (2016. 07. 20.)

[14] TIA Standard, Project 25 FDMA – Common Air Interface, New Technology Standards Project – Digital Radio Technical Standards, TIA-102.BAAA-A, September 17. 2003.
https://archive.org/stream/TIA-102_Series_Documents/Tia-102-baaa-aProject25FdmaCai#page/n0/mode/2up

[15] ETSI Digital Mobile Radio (DMR) Standard TS 102 361: Systems: Part 1: DMR Air Interface (AI) protocol, Part 2: DMR voice and generic services and facilities, Part 3: DMR data protocol, Part 4: DMR trunking protocol. ETSI 2005.
http://www.etsi.org/index.php/technologies-clusters/technologies/digital-mobile-radio

[16] ETSI TS (Technical Specification) 102 361-1 V2.4.1 (2016-02)
Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface (AI) protocol
http://www.etsi.org/deliver/etsi_ts/102300_102399/10236101/02.04.01_60/ts_1023610 1v020401p.pdf

[17] Alessandro Guido (DMR System Design Selex Elsag): How DMR Works, Benefits Part1 – Appendix on DMR Technology,
https://hamgear.files.wordpress.com/2014/02/dmr-primer.pdf (2016. 05. 21.)

[18] ETSI TS 102 361-2 V2.3.1 (2016-02)
Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 2: DMR voice and generic services and facilities
http://www.etsi.org/deliver/etsi_ts/102300_102399/10236102/02.03.01_60/ts_1023610 2v020301p.pdf

[19] DMR Association: Benefits and Features of DMR, White Paper
http://dmrassociation.org/downloads/documents/DMR-Association-White-Paper_Benefits-and-Features-of-DMR_160512.pdf (2016. 05. 21.)

[20] Tait Radio Communications (White Paper): Technologies and Standards for Mobile Radio Communications Networks
http://utilities.taitradio.com/__data/assets/pdf_file/0005/39461/tait_technologycomparison_whitepaper_eng.pdf

[21] Panpaliya et al.: Method for Resolving Call Collisions in a Digital Conventional Direct Mode, United States, Patent Application Publication. US 2016/0057782 A1, Feb. 25, 2016
http://www.freepatentsonline.com/20160057782.pdf

[22] Balog Károly: Digitális PMR-ek támadási és védelmi lehetőségei, Bolyai Szemle XXV. évfolyam, 2016/1. szám, ISSN 1416-1443
http://uni-nke.hu/uploads/media_items/bolyai-szemle-216-1.original.pdf (2016. 09. 10.)

[23] CML Microcircuits: CMX7241 and CMX7341 PMR Common Platform Processor
http://www.cmlmicro.com/DesignSupport/resources/2015/10/29/CMX7241-7341FI2-Datasheets (2016. 09. 10.)

[24] Wireless-mag.com: CML Microcircuits unveils single chip for all digital and analogue PMR systems 2016. 09. 06.

[25] http://www.wireless-mag.com/News/43102/cml-microcircuits-unveils-single-chip-for-all-digital-and-analogue-pmr-systems-.aspx?utm_medium=twitter&utm_source=twitterfeed (2016. 09. 06.)

[26] RadioReference.com: DSD Plus http://wiki.radioreference.com/index.php/DSDPlus (2016. 09. 06.)

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Kovács Zoltán
zkovacs.24@gmail.com

BIZTONSÁG VS. TÖRVÉNYES ELLENŐRZÉS AZ INTERNET ALAPÚ KOMMUNIKÁCIÓBAN - ELLENTÉTES VAGY EGYMÁSSAL MEGFÉRŐ KÖVETELMÉNYEK? I.

Absztrakt

A cikksorozat összefoglalja a kommunikáció változását, a változások hatását a szolgáltatói modellre és a törvényes ellenőrzésre. Rámutat azokra a jogi hiányosságokra, problémákra, amelyek hatással vannak az internet alapú kommunikáció törvényes ellenőrzésének hatékony ellátására, majd nemzetközi kitekintéssel bemutatja az ellenőrzésére jelenleg rendelkezésre álló, jellemző technikai eszközöket és azok főbb tulajdonságait. Rávilágít a hazánkban újonnan hatályba lépett jogszabályok adta lehetőségekre, pontosítva annak kereteit, valamint ismerteti, hogy milyen hatásai lehetnek a kommunikáció biztonságára. Az első rész a kommunikáció, a szolgáltatói modell változásának és a törvényes ellenőrzés lehetőségeinek a téma szempontjából lényeges elemeit foglalja össze.

This article series summarizes the changes of communication and the effects of these changes on the service-provider model and on the lawful monitoring. This article series points out the insufficiencies and problems of the current laws which affect the lawful monitoring of the internet-based communication, then describes the currently and typically used possible technical solutions of lawful monitoring, and their major characteristics with an international view. It highlights the possibilities given by the Hungarian law that entered into force nowadays, on lawful monitoring of the application service providers, specifies its frames, and describes its effects on the security and privacy of communication. The first part of this article series is reviewing and summarizing the changing of the communication and the service provider model, as well as the possible technical solutions of lawful monitoring, which are relevant to the subject.

Kulcsszavak: *hírközlés, kommunikáció, alkalmazásszolgáltató, törvényes ellenőrzés ~ electronic communication, communication, application service provider, lawful monitoring*

BEVEZETÉS

Napjaink egyik legtöbbet vitatott kérdése az internet alapú szolgáltatások – ezek közül is kiemelten a kommunikációt lehetővé tevők – törvényes ellenőrzése. Érdemes ugyanakkor megemlíteni, hogy a hibrid hadviselés szempontjából is komoly jelentőség tulajdonítható az internet és a mobil kommunikáció egyes területeinek. [1] A viták fő oka az, hogy miközben a kommunikáció formái, lehetőségei az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek, addig az azok ellenőrzését szabályozó törvények jellemzően nem követik azokat. A jogszabályi lemaradás természetesnek mondható, hiszen ez szinte minden új, a nemzetbiztossági szolgálatok és a rendvédelmi szervek által ellenőrizni kívánt technológia esetében hasonló módon megy végbe. A hosszabb távon is megfelelő törvényi szabályozáshoz ugyanis célszerű nem egy-egy szolgáltatásra kihegyezett, hanem általánosan érvényes szabályokat leírni, amelyhez azonban több feltételnek is teljesülnie kell. Először is ismerni kell, melyek azok a technológiák, amelyek felhasználása eléggé elterjedt ahhoz, hogy azokat a szabályozó mindenképp lefedje. Ezáltal a jogszabályokat oly módon kell megfogalmazni, hogy ezekre valóban ki is terjedjen a hatályuk. Másrészt ezen technológiák már műszakilag kellőképpen kiforrottak kellenek legyenek ahhoz, hogy egy-egy műszaki változtatás várhatóan ne lehessen olyan hatású, hogy a frissített rendszerre már nem érvényesíthető a leírt jogszabály, így az ne okozhassa a törvényes ellenőrzés ellehetetlenülését. Az ugyanis a kezdeti, mondhatni bevezetési fázisban lévő kommunikációs szolgáltatásoknál jellemző, hogy sokszor egy-egy új szoftver verzió kiadásával gyökeres változásokat eszközölnek a készítők, többször teljesen új technológiai alapra helyezve a szolgáltatást, akár úgy is, hogy a korábbi verziók kompatibilitását sem biztosítják.

Az internet alapú, ezek közül is kiemelten a kommunikációt lehetővé tevő szolgáltatások törvényes ellenőrzése minden országban kihívást jelent. Egyrészt azért, mert az elektronikus úton folytatott kommunikáció ma már jóval tágabb értelemben értelmezhető fogalom, mint a hagyományos hírközlés, hiszen lehetőségei, a kommunikációs formák száma messze meghaladják ez utóbbiét. Ennek következtében rengeteg olyan új rendszer, technológia jelent, jelenik meg, amelyek törvényes ellenőrzését az arra feljogosított szolgálatoknak meg kell, vagy legalábbis meg kellene oldani. Másrészt pedig azért, mert strukturális átalakulás is zajlik, amelyben a – korábban mindenki által elfogadott és már jól szabályozott ellenőrzési módszereket is tartalmazó – klasszikus hírközlési szolgáltatói modellt egyre inkább felváltja az infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modell. Ez utóbbi esetében azonban nincsenek egységes, mindenki által elfogadott törvényes ellenőrzési módszerek és szabályzók.

A törvényes ellenőrzés kialakítását alapvetően három – egymással szorosan összefüggő – probléma nehezíti. Az egyik, a már említett jogi szabályozás hiányosságaiban keresendő. A hatályos jogszabályok ugyanis nem, nem teljes mértékben vagy csak erős „beleértéssel” teszik lehetővé az említett rendszerek ellenőrzését, mindenki – vagy legalábbis a fejlett demokráciával rendelkező országok – által elfogadott, irányadó szabályozók pedig nincsenek. A másik a technikai megoldások hiánya, vagy a meglévők hiányossága jelenti, hiszen sokszor vagy még nincsenek meg azok a technikai eszközök, amelyekkel az új technológiák törvényes ellenőrzését egyáltalán végre lehet hajtani, vagy a meglévők technikailag korlátozottan képesek az elvárt – és a hírközlés-ellenőrzésnél már megszokott – feladatok elvégzésére. A harmadik nagy problémát pedig az okozza, hogy a hírközlés ellenőrzésnél régóta kialakult és elfogadott rend, miszerint az infrastruktúrával és szolgáltatással az adott országban egyaránt jelen lévő szolgáltató együttműködik a nemzetbiztonsági és bűnüldöző szervekkel, ebben az esetben nem, vagy nem teljes mértékben működik.

A fenti problémakör kezelésére 2016-ban Magyarországon megszületett egy merőben új jogi szabályozás. Ez azonban újszerűsége okán meglehetősen sok vitát váltott ki és félreértést okozott, főleg abban, hogy az egyes szereplőknek, beleértve a felhasználót is milyen

kötelezettségei vannak, és adott esetben annak megszegése hogyan szankcionálható. Mindehhez még hozzájárult a nemzetközi sajtóban fellángolt vita arról, hogy az ellenőrzés biztosítása az arra feljogosított szolgálatok számára milyen esetben és hogyan okozza, okozhatja a kommunikáció biztonságának romlását. Éppen ezért célszerű megvizsgálni, hogy milyen módszerek állnak a titkos információgyűjtést végző szervezetek rendelkezésére, és azok alkalmazása során milyen buktatókba ütköztek, valamint azt is, hogy a nemrégiben elfogadott hazai szabályozás milyen hatással van, lehet egyrészt a törvényes ellenőrzésre, másrészt a felhasználó szemszögéből nézve a kommunikáció biztonságára.

A KOMMUNIKÁCIÓ ÉS A SZOLGÁLTATÓI MODELL VÁLTOZÁSA

A „Felhő alapú rendszerek törvényes ellenőrzési problémái”, [2] a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. és II.” [3] [4] valamint az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből” [5] című cikkek részletesen megvizsgálták és leírták az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére szolgáló lehetőségeket, azok előnyeit, hátrányait, valamint definiálták a jelenlegi hírközlési modellt potenciálisan felváltó infrastruktúra-, alkalmazás- és tartalomszolgáltatói modellt, pontos meghatározásokat adva annak egyes szereplőire. Fenntartva és elfogadva az ott leírtakat az alábbiak röviden összefoglalják a jelen cikk témájának kibontásához szükséges, az említett cikkekben megjelenített főbb elemeket.

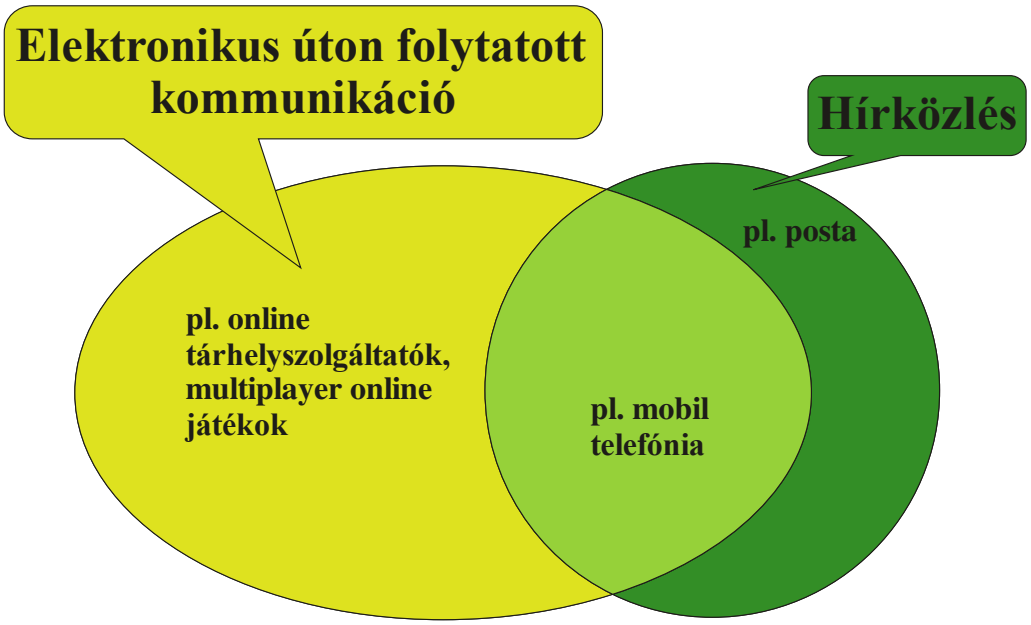
A kommunikáció változása

A kommunikáció formái, lehetőségei az internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. Ebben nagy szerepük van az internet-technológiára épülő szolgáltatásoknak. Ezek azok a mindenki számára elérhető, meglévő eszközeivel (pl. notebook, okostelefon stb.), akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, Gmail, Dropbox, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak.

Az említett rendszerek azonban nem csak a felhasználói szokásokat változtatták, változtatják meg alapjaiban, hanem a hírközlés struktúráját is teljesen átformálják. Ennek talán a leglényegesebb eleme az, hogy a tényleges kommunikációs szolgáltatást valamint az ahhoz szükséges infrastruktúrát – ellentétben például a hagyományos telefóniával – nem egyazon szervezet biztosítja a felhasználó számára. Sőt, ezek a legtöbb esetben nem is tudnak egymásról, nincsenek semmilyen kapcsolatban egymással. Így a korábbi hírközlés helyett ma már sokkal inkább elektronikus úton folytatott kommunikációról beszélhetünk.

Az elektronikus úton folytatott kommunikáció megnevezés teljesen tudatos szóhasználat. Napjainkban ugyanis az említett fogalom alatt nem csak a hírközlő rendszereken folytatott kommunikációt értjük, hanem minden olyan kommunikációs lehetőséget, formát, amely lehetővé teszi két – vagy adott esetben több – fél között információk, adatok áramlását, cseréjét. Ez pedig messze túlmutat nemcsak a hírközlés, de a kifejezetten kommunikáció céljából kifejlesztett internet alapú rendszereken is.

Húsz évvel ezelőtt a hírközlés teljes egészében lefedte az elektronikus úton folytatott kommunikációt, ez utóbbi a hírközlés mintegy részhalmazát képezte. Mára ez a kép jelentősen megváltozott. Ha ábrázolnánk, akkor talán az 1. ábra megfelelően szemléltetné a kettő kapcsolatát. A területek nagyságával az egymáshoz képesti jelentőséget is szemléltetni kívántam.



1. ábra. Az elektronikus úton folytatott kommunikáció és a hírközlés viszonya

Ma az elektronikus úton folytatott kommunikáció lehetőségei messze meghaladják a hagyományos hírközlését. A végeredmény szempontjából ugyanis nincs különbség a között, hogy megírok és elküldök egy elektronikus levelet, vagy megírás után a piszkozatok közé teszem, de a másik félnek megadom a postafiók eléréséhez szükséges felhasználónevet és jelszót. Hiszen ez utóbbi esetben is hozzáfér, olvashatja ugyanazt az üzenetet. De itt még legalább a „levélszerűség" megvan, a „hagyományos" hírközlési forma fellelhető. Ha a továbbítani szánt információkat azonban egy felhő alapú tárhely szolgáltatónál kialakított fiókba helyezem el fájlként, majd ennek adom meg a belépéshez szükséges adatait a másik félnek, akkor a végeredmény ugyanaz: „A" felhasználótól „B" felhasználóhoz eljutott az információ. Ez a forma azonban már „nyomokban sem tartalmaz" hagyományos hírközlést. Ugyanilyen jellegű példa a multiplayer online játékok esete. Ezeket nem azért fejlesztették ki, hogy a felhasználók kommunikálni tudjanak egymással, az csak egy kiegészítője, hozadéka a játékoknak. Ugyanakkor tényszerűen vizsgálva, a végeredményt tekintve itt sincs különbség a játék során folytatott beszélgetések, chatelések és egy kifejezetten erre szakosodott hírközlő rendszeren folytatott beszélgetés vagy üzenetküldés között.

Az internet-technológiára épülő, azokon belül is elsősorban a kommunikációs szolgáltatások törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, ugyanakkor a törvényes ellenőrzést végző szervek több, már említett jogi és technikai problémával is szembesültek, szembesülnek. A törvényes ellenőrzést végző szervezeteknek alapvetően az a feladata, célja, hogy a kijelölt célszemélyek kommunikációját lehetőség szerint teljes mértékben ellenőrizzék függetlenül annak formájától, a felhasznált technológiától. Az ehhez megfelelő, hatékony törvényi szabályozás megalkotásához és technikai eszközrendszerek kialakításához azonban figyelembe kell venni a szolgáltatói modell változását is.

A szolgáltatói modell változása

Megállapítható, hogy a klasszikus hírközlési szolgáltatói modell egyre inkább eltűnik, helyét új szolgáltatói struktúra veszi át, és ez a tendencia a jövőben várhatóan tovább erősödik. Az új modell legjelentősebb hatása a hírközlésre az, hogy a hírközlési hálózatot – vagy célszerűbb megfogalmazással internetelérést – és a tényleges kommunikációt más szolgáltatató biztosítja. Ennek a leírására a korábbi hírközlési szolgáltatói modell helyett az azt potenciálisan felváltani képes infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt célszerű

alkalmazni, amely teljes körűen képes leírni mind a jelenlegi helyzetet, mind a korábbi hírközlési modellben szereplőket, valamint azok feladatait.

Fel kell azonban tenni a kérdést, hogy mit is takarnak az infrastruktúra-, alkalmazás-, és tartalomszolgáltató fogalmak. Ezekre részletes választ ad az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből” című cikk, [4] definíciós javaslatot is adva mindhárom szolgáltatóhoz. Mindezeket továbbiakban is fenntartva, röviden és egyszerűsítetten az alábbiak szerint fogalmazhatók meg az egyes említett szolgáltatók – a téma szempontjából – lényegi tulajdonságai:

Tartalomszolgáltató: kizárólag egyirányú információáramlást szolgál, azok tartalmára a fogyasztónak semmilyen befolyása nincs, a felhasználó „passzív” fogyasztó, a szolgáltató a tartalomért szerkesztői felelősséggel tartozik. Nem tekinthetők tartalomszolgáltatásnak a magáncélú vagy szűk, meghatározott körben elérhető tartalmak. Sem a szolgáltató, sem a felhasználó a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen. A szolgáltatás Magyarországon elérhető és igénybe vehető, függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e.

Alkalmazásszolgáltató: az információáramlás ebben az esetben többirányú, a felhasználó aktív, tevékeny résztvevő, az információk adattartalmára befolyással rendelkezik. Sem a szolgáltató, sem a felhasználó a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen. A szolgáltatás Magyarországon elérhető és igénybe vehető, függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e.

Infrastruktúraszolgáltató: valamilyen infokommunikációs rendszert üzemeltet és azon keresztül internetelérést biztosít, akár úgy is, hogy más szolgáltatótól vásárolt internetelléréshez biztosít harmadik félnek (feleknek) hozzáférést. Sem a szolgáltató, sem a felhasználó a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen. A szolgáltatás Magyarországon elérhető és igénybe vehető, függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e.

Vegyes szolgáltatások: Természetesen előfordulhat, hogy valamely cég vegyes szolgáltatást nyújt. Ma például egy internetszolgáltató internetelérést és például e-mail-ezési lehetőséget is biztosíthat, vagy egy online tartalomszolgáltatással foglalkozó cégnél, például egy internetes újságnál pedig lehetőséget biztosíthatnak kommentek írására, ezen keresztül pedig kommunikáció megvalósítására is. Ezekben az esetek is kezelhetőek a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikkben [2] bemutatott hármas tagozódásban szereplő tartalom-, alkalmazás-, és infrastruktúraszolgáltató modellel.

A törvényes ellenőrzés kapcsán a három szolgáltatónak eltérő kötelezettségei származnak. Míg a tartalomszolgáltatónak alig, az infrastruktúra szolgáltatónak korlátozott (elsősorban előfizetői adatszolgáltatási), addig az alkalmazásszolgáltatóknak – a hagyományos hírközlési szolgáltatóhoz hasonlóan – szinte teljes körű (például az összes felhasználói adat, így bejelentkezési IP címek, felhasználónevek, valamint az általa nyújtott szolgáltatás kapcsán keletkező tartalmak, így e-mailek, hangkommunikáció, chat, stb.) információ-, és adatelérést kell biztosítania az arra felhatalmazott szervezetek számára.

Amennyiben egy cég vegyes szolgáltatást nyújt, akkor a szolgáltatásfajtáknak megfelelően kell a törvényes ellenőrzést lehetővé tennie. Maradva a fent említett példáknál, ha egy mai értelemben vett internetszolgáltató e-mail lehetőséget is biztosít, akkor erre az alkalmazásszolgáltatóknál kialakítandó kötelezettségeket kell figyelembe venni. Ugyanez igaz az online újság esetében is, ahol a fórumok, kommentek esetén már az alkalmazásszolgáltatókra kirótt kötelezettségeket kell teljesíteniük.

Érdemes megvizsgálni a mai hírközlési szolgáltatók helyzetét is. Esetükben a problémakör két részre bontható. Amennyiben internet-szolgáltatást is végeznek, akkor a fent leírtak alapján lehet eljárni. Amennyiben a hagyományos – például vezetékes telefon – szolgáltatásokat nézzük, akkor ott is megjelenik az infrastruktúra-, és alkalmazásszolgáltatás,

csak kizárólagosan egy, azonos és elválaszthatatlan infrastruktúrával és szolgáltatóval. Ebben az esetben is ugyanúgy kezelhető a probléma, mint a fent már leírt egyéb vegyes szolgáltatások esetében.

A fentiek alapján megállapítható, hogy a tartalom-, alkalmazás-, és infrastruktúraszolgáltató modellbe minden szolgáltató egyértelműen besorolható, így törvényes kötelezettségeik is egyértelműen meghatározhatóvá válnak. Igaz ez a mai jogszabályokban leírt hírközlési-, és internetszolgáltatók esetében is.

Mindezek mellett a hírközlési szolgáltató és szolgáltatás fogalmát a továbbiakban is célszerű fenntartani, egyrészt azért, mert így például a hagyományos telefonszolgáltatások a jelenlegi szabályoknak megfelelően a továbbiakban is egyszerűen, mindenki számára vita nélkül elfogadott módon kezelhetők, másrészt pedig azért, mert a nemzetközi jogi szabályozásban ezek törvényes ellenőrzése egy mindenki által elfogadott meghatározás és normarendszer szerint történik.

A TÖRVÉNYES ELLNŐRZÉSI MÓDSZEREK

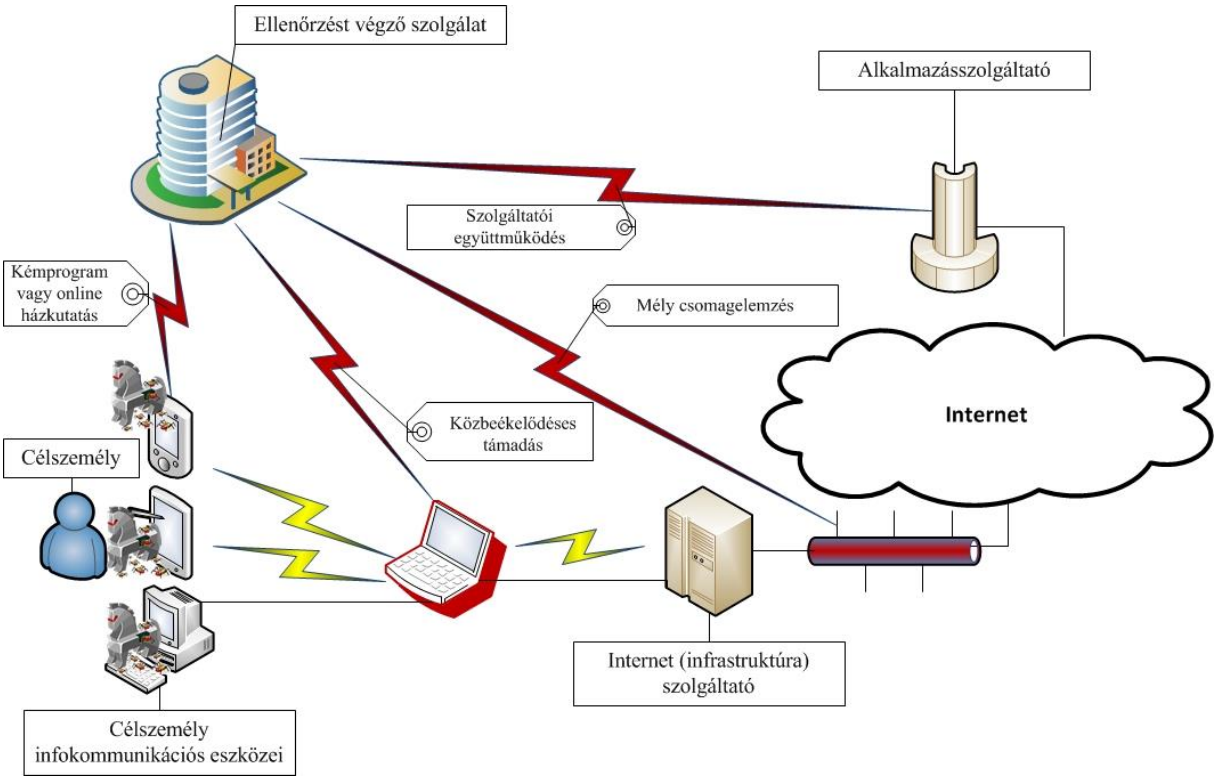
Annak érdekében, hogy tisztázni lehessen, milyen hatása van vagy lehet az erre vonatkozó újonnan hozott hazai jogszabályoknak az internet-technológiára épülő szolgáltatások törvényes ellenőrzésének hatékonyságára, valamint hogy sérülhet-e a kommunikáció biztonsága, célszerű megvizsgálni, hogy a szolgáltatói modell változása milyen hatással van a törvényes ellenőrzésre, milyen jellemző technikai eszközök állnak rendelkezésre annak megvalósításához.

Az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére alapvetően az alábbi négy módszert használhatják az arra felhatalmazott szolgálatok:

a) aktív ellenőrző eszköz,
b) közbeékelődéses ellenőrzés (MitM),
c) mély csomagvizsgálat (DPI),
d) együttműködés a szolgáltatóval.

A módszerek elnevezései önkényesek. Valódi, mindenki által elfogadott magyar megfelelőik vagy nem alakultak ki, vagy az ezekről szóló szakirodalom is többféle megnevezéssel használja azokat. [6] [7]

A fenti módszerekre rendkívül jellemző az alkalmazásukkor használt adatszerző, elfogó eszközök – ebbe bele kell érteni a hardver és szoftver elemeket egyaránt – távolsága a célszemélytől. Ezt jól szemlélteti a 2. ábra.



2. ábra. Az adatszerző, ellenőrző eszközök távolsága a célszemélytől

Aktív ellenőrző eszköz

Az aktív ellenőrző eszközök, vagy közismertebb, a fejezet első részében említett nevükön kémprogramok vagy online házkutatási eszközök esetében a célszemély infokommunikációs eszközére, eszközeire (pl. számítógép, telefon, táblagép stb.) egy speciális „kártékony" szoftvert telepít az ellenőrzést végző szolgálat. Ez sok hasonlóságot mutat a valódi kártékony szoftverekkel, de ebben az esetben ez törvényes célokat szolgál. Talán azt az analógiát lehetne erre alkalmazni, mint amikor egy lőfegyverről beszélünk, amely más értelmet nyer egy bűnöző és mást egy rendőr kezében.

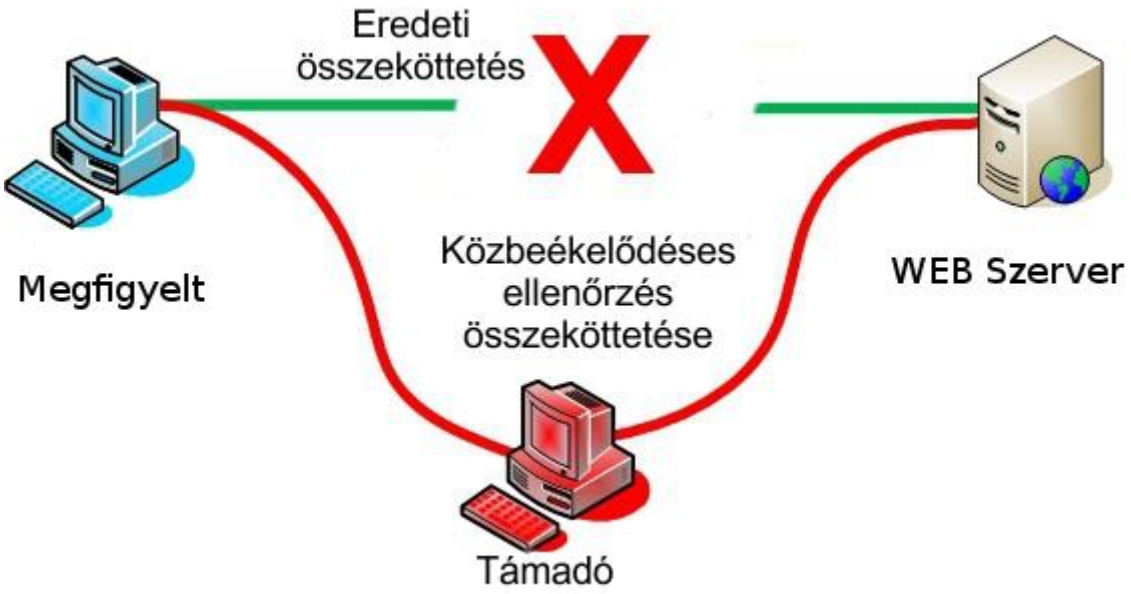
Az aktív ellenőrző eszköz bejuttatása a célszemély eszközére többféle módszerrel is lehetséges, hasonlóan a kiberbűnözők által használt módozatokhoz (pl. elektronikus levél csatolmányaként, fertőzött weboldal segítségével, 0. napi sebezhetőség kihasználásával stb.). A működés során ezek képesek az online kommunikáció elfogására, de billentyűzetleütések rögzítésére, a háttértárban található adatok megszerzésére, vagy akár – ha van – a webkamerával képek készítésére is. Az információkat azután összegyűjtve küldik el az aktív ellenőrző eszköz tulajdonosának. [8] [9] [10] [11] [12]

Az online házkutatásra alkalmas eszközök, azaz kémprogramok természetesen jóval több információt tudnak biztosítani a célszemélyek számítógépéről (pl. tárolt fájlok), a számítógép technikai eszközein keresztül a célszemély tevékenységéről (pl. webkamera képek), mint amit pusztán az elektronikus úton folytatott kommunikációt biztosító alkalmazásszolgáltató – a törvényi feltételek megléte és maximális segítőkész hozzáállás mellett – képes.

A törvényes ellenőrzések során alkalmazott kémprogramokról Németországból szivárgott ki a legtöbb információ, ám – mint bizonyos körülmények között rendkívül hatékony vagy sokszor egyetlen alkalmazható eszközt – más országok titkos információgyűjtésre feljogosított szervei is használják, vagy legalábbis használni tervezik. Ilyen témájú hírek érkeztek Svájc, [13] Franciaország, [14] Ausztria, [15] Hollandia [16] és természetesen az USA [17] [18] [19] [20] és az Egyesült Királyság [21] vonatkozásában is.

Közbeékelődéses ellenőrzés (MitM)

Leegyszerűsítve a dolgot, a közbeékelődéses ellenőrzés esetében az ellenőrzést végző szolgálat úgy hallgatja le a két fél között zajló kommunikációt, hogy a kommunikációs csatornát megszakítja, legyen az vezetékes vagy vezeték nélküli, majd abba, a két kommunikáló fél közé „beállva" mindkettőjük számára a másik félnek adja ki magát. A kapcsolat ezáltal mindkét fél számára zavartalannak tűnik, valójában azonban a teljes forgalom „átfolyik" az ellenőrzést végző eszközén, amellyel az itt zajló kommunikációt lehallgathatja, ahhoz teljes mértékben hozzáfér. Ezt szemlélteti a 3. ábra.



16. ábra. Közbeékelődéses ellenőrzés. (a szerző szerkesztette a [39] alapján)

A sikeres közbeékelődéses ellenőrzéshez több feltételnek is teljesülnie kell. Az ellenőrzést végzőnek hozzá kell férnie a kommunikációs csatornához, képesnek kell lennie annak megszakítására (legyen az vezetékes vagy vezeték nélküli kapcsolat) oly módon, hogy megakadályozza az üzenetek eljutását a valódi címzetthez, majd le kell tudnia hallgatni a rajta küldött üzeneteket. Ez titkosítás nélküli kommunikáció esetében viszonylag egyszerű, de bizonyos esetekben, kis szerencsével és a valódi kommunikáló fél (felek) figyelmetlenségével akár titkosított kommunikáció esetén is megvalósítható. Ezt szemlélteti a 4. ábra.

4. ábra. Példa HTTPS kommunikáció ellenőrzésére. (a szerző szerkesztette a [25] alapján)

Sikeres közbeékelődéses ellenőrzés akkor hajtható végre viszonylag egyszerű eszközökkel és nagy valószínűséggel, ha a célszemélyhez (azaz az egyik kommunikáló félhez) az ellenőrzést végző a lehető legközelebb helyezkedik el. [22] [23] [24] [25] [26] [27]

Érdekes, hogy amíg a többi módszer törvényes ellenőrzésre történő felhasználásáról sok konkrét információ szivárgott ki, addig a MitM-ről ez nem mondható el. Ugyanakkor a

Snowden által kiszivárogtatott anyagokban található információ arra, hogy az Egyesült Államok szolgálatai használták ezt a technológiát is. [28]

Mély csomagvizsgálat (DPI)

A mély csomagvizsgálat azt jelenti, hogy az adatcsomagoknak nemcsak a fejlécét, hanem azok adattartalmát is vizsgálat alá vetik, majd az adattartalom alapján kiszűrik az „érdekes" adatcsomagokat. A szűrés jellege a mély csomagvizsgálat felhasználásának céljától függ, a csomagvizsgálati módszerek azonban technikailag függetlenek attól. [29]

A mély csomagvizsgálatot leggyakrabban három esetben szokták alkalmazni. Az első eset a behatolást észlelő és behatolás-védelmi rendszerekben (IDS/IPS) történő felhasználás. Ezek a rendszerek a csomagok elemzésekor speciális bitmintákat (ismert támadókódokat) keresnek erre dedikált eszközök segítségével, majd a felismert, rosszindulatú kódot tartalmazó csomagokat kiszűrik. [30] A második a hírközlési, internetszolgáltatók rendszereiben történő alkalmazás. Itt az internet protokoll alapú hangátviteli szolgáltatások (VoIP) és a peer-to-peer kapcsolaton alapuló fájlcsere forgalmának blokkolására használják a technológiát. [31] A harmadik a törvényes ellenőrzés, ahol a csomagok vizsgálata alapján dönthető el, hogy az az ellenőrzést végző számára érdekes-e (pl. adott célszemélyhez tartozik-e az email), vagy sem. Itt a szűrés azonban nem a kiválasztott csomagok blokkolását szolgálja, hanem azoknak az ellenőrzést végző szolgálathoz (is) történő eljuttatását. [32] [33] [34] [35]

Titkosítás nélküli kommunikáció esetén a lehallgatás viszonylag egyszerűen, sőt ebben az esetben, ellentétben a közbeékelődéses ellenőrzéssel, tömegesen is megvalósítható. Ugyanakkor titkosított kommunikáció esetén a tartalomhoz való hozzáféréshez feltétlenül szükséges a titkosítás feltörése, ez pedig hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a kommunikáló felek akár a nyílt forgalmaknál is egyszerű – és sokszor ingyenesen rendelkezésre álló – titkosító szoftvereszközök használatával (pl. HTTPS Everywhere) jelentősen megnehezíthetik vagy akár el is lehetetlenítik az ellenőrzést. [36]

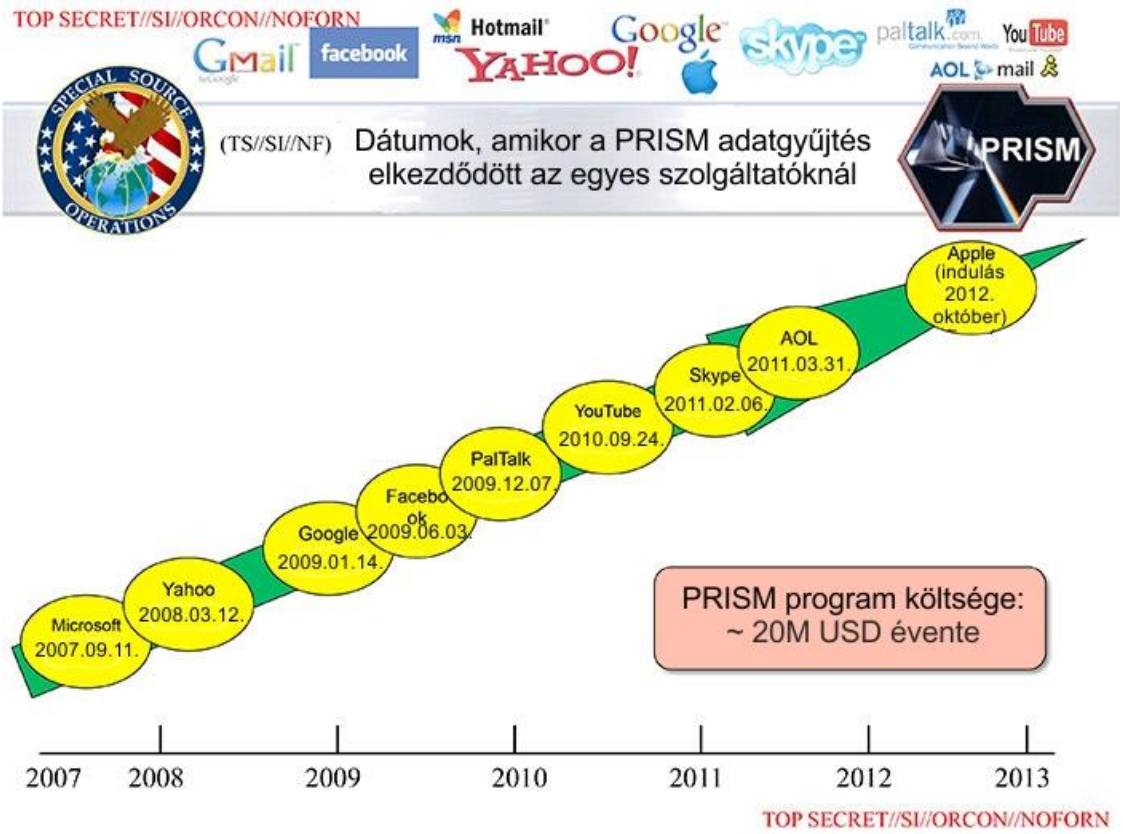
E korlát ellenére az „Öt Szem" országai (USA, UK, Kanada, Új Zéland és Ausztrália) együttműködve használják ezt a technológiát ellenőrzésre, és osztják meg egymás között az így kinyert információkat – a tartalmat és a kísérő ún. metaadatokat egyaránt. [35] [37]

Együttműködés a szolgáltatóval

A szolgáltatóval való együttműködés a hagyományos hírközlési szolgáltatóknál már egy jól ismert és bevált modell szerint működik. Ekkor az ellenőrzést végző szerv eljuttatja a célszemélyhez kapcsolódó releváns adatokat (pl. felhasználónév) a szolgáltató rendszerébe, majd a szolgáltató automatikusan (emberi beavatkozás nélkül) vagy egyedi kiszolgálással (emberi beavatkozással) biztosítja a – rendszerében rendelkezésre álló – kért adatokat, információkat, vagy akár a rajta átfolyó kommunikáció tartalmát is. [34]

Legjellemzőbb példaként itt talán az Egyesült Államok említhető. A Prism programról nyilvánosságra került adatok szerint is. Az ott leírtak szerint a vezető internetes alkalmazásszolgáltatók (Skype, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, YouTube, Apple) rendszerein tárolt és azokon átfolyó adatokhoz (pl. beszélgetések, video-chat, fényképek stb.) (12. ábra) – szolgáltatónként változó formában és mélységben – férnek hozzá az erre felhatalmazott szolgálatok. [38] Ezt mutatják az 5. és a 6. ábrák.

5. ábra. A Prism programban szereplő szolgáltatók és az általuk – különböző mértékben – biztosított adatok. [34]



6. ábra. A Prism programban résztvevő szolgáltatók és csatlakozásuk időpontja. [34]

A módszerek összehasonlítása

A fent említett módszerek – a téma szempontjából – legfontosabb előnyei és hátrányai az alábbi táblázatban foglalhatók össze:

1. táblázat. Az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére jelenleg rendelkezésre álló módszerek előnyei, hátrányai.

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
aktív ellenőrző eszköz	• nem csak az éppen folyó forgalmat, hanem a gépen tárolt minden adatot el lehet érni • titkosítás előtti elfogás – azaz a felhasznált titkosítástól függetlenül ellenőrizhető a forgalom	• egyedi ellenőrzés (egy trójai, egy eszköz) • a telepítés problémákba ütközhet • a célszemély minden eszközére kell telepíteni a teljes körű ellenőrzéshez • aktív, ezért működése adott esetben felfedezhető • működése, működő képessége nagymértékben függ a céleszköz beállításaitól, telepített szoftvereitől (pl. vírusirtó, tűzfal) • működése azonnali utasítással nem megszakítható • alapos előkészületek ellenére a képességet egy egyszerű (pl.: vírusellenőrző) frissítés ellehetetlenítheti • jogszabályi háttere nem egyértelmű

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
közbeékelődéses ellenőrzés (MitM)	• bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését (általában SSL, https esetén)	• egyedi ellenőrzés (egy internetforgalomra) • más titkosított forgalmak problémát okozhatnak • viszonylag közel kell menni • több eszköz és netelérés esetén problémás (pl. vezetékes és mobil net) • adott esetben a tevékenység felfedezhető • csak az éppen folyó forgalmat lehet vele megismerni • titkosított forgalom esetében az alkalmazónak szükséges hiteles tanúsítvánnyal rendelkeznie • jogszabályi háttere nem egyértelmű
mély csomagvizsgálat (DPI)	• tömeges – egyszerre több célszemély forgalma is ellenőrizhető • teljesen passzív • tartalom alapú szűrést tesz lehetővé • jogszabályi háttere egyértelmű	• nagy beruházási igény • az egyre növekvő sávszélesség miatt egyre gyorsabb, nagyobb sávszélességű elfogókat kell használni • a titkosítás problémákat okozhat • adott „csatornán” átfolyó forgalmat elemzi, ha nem ott megy a célszemély forgalma, nem fogja el – nem teljes körű • csak az éppen folyó forgalmat lehet vele megismerni

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
együttműködés a szolgáltatóval	• tömeges – egyszerre több célszemély is ellenőrizhető • teljes információkör elérhető, a használt eszközöktől, interneteléréstől függetlenül • nem csak az éppen folyó forgalmat, hanem a szolgáltatónál tárolt minden adatot (pl. piszkozatok) el lehet érni • a szolgáltató által alkalmazott titkosítás nem probléma	• a szolgáltatók nem mindig partnerek, csak jogszabályi alapon működik (hatékonyan) • külföldi szolgáltatók felhasználóinak ellenőrzése esetén ráadásul nemzetközi jogszabályok szükségesek • a célszemély adatait szolgáltató is megismeri – titoktartási, konspirációs gondot okozhat • több szolgáltatót használó célszemélyeknél mindegyikkel együtt kell működni

A fentiek alapján megállapítható, hogy bár az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére technikailag jelenleg többféle módszer is az érintett szolgálatok rendelkezésre áll, ám ezek egyike sem nyújt teljes körű megoldást. Kijelenthető az is, hogy az alkalmazásszolgáltatóval való együttműködés kikerülhetetlen. Ez biztosítja ugyanis, hogy egyszerre több célszemély is ellenőrizhető úgy, hogy az adott szolgáltatáshoz kapcsolódó teljes információkör elérhető az adott szolgálat számára, függetlenül a célszemély(ek) által használt eszközöktől és interneteléréstől. Ez pedig az egyik leghatékonyabb és legköltség-takarékosabb ellenőrzési formává teszi.

Ugyanakkor – ahogy korábban Magyarországon is – éppen ennek a módszernek a jogi szabályozottsága kapcsán fellelhető hiányosságok okán, ma a legtöbb ország esetében is kizárólag az alkalmazásszolgáltató jóindulatán múlik, együttműködik-e az ellenőrzést végző szervekkel és teljesíti-e – az egyébként teljesen legális, hatályos és pl. a hírközlési szolgáltatók számára (is) kötelező érvényű bírói végzésben foglaltakat. Éppen ezt a problémát orvosolja, orvosolhatja – az egyébiránt nemzetközi kitekintésben is előremutató – új hazai szabályozás.

ÖSSZEGZÉS

A fentiek alapján megállapítható, hogy a kommunikáció változása a szolgáltatói modell és a törvényes ellenőrzés változását is magával hozta. Bár az elmúlt években megjelent, vagy akár az újonnan megjelenő internet alapú kommunikációs formák törvényes ellenőrzésére az arra felhatalmazott szolgálatok többféle technikai módszerrel, megoldással is rendelkeznek, ám önmagukban ezek egyike sem nyújt teljes körű megoldást. Ugyanakkor a jellemző módszerek előnyeit és hátrányait figyelembe véve elmondható, hogy a szolgáltatóval való együttműködés kikerülhetetlen. Ez utóbbit biztosítják hazánkban a 2016-ban hatályba lépett jogszabályi módosítások. Ezen új szabályozások kereteivel és a – felhasználó szemszögéből megvilágítva – a kommunikáció biztonságára gyakorolt hatásaival foglalkozik a cikksorozat második része.

Felhasznált irodalom

[1] Balog Fatime, Fekete Csanád, Németh András, Németh József Lajos: A hibrid hadviselés különös tekintettel a mobil kommunikációra, in: HADMÉRNÖK X:(4) pp. 120-131. (2015)

[2] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. Hadmérnök. VIII. Évfolyam 1. szám - 2013. március, pp. 233-241. ISSN 1788-1919 Online: http://hadmernok.hu/2013_1_kovacsz.pdf

[3] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 184-197. ISSN 1788-1919 Online: http://hadmernok.hu/133_18_kovacsz_2.pdf

[4] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 198-210. ISSN 1788-1919 Online: http://hadmernok.hu/133_19_kovacsz_3.pdf

[5] Kovács Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-3756 Online: http://uni-nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2014-4-2.original.pdf (2014.11.27.)

[6] Berta Sándor: Online házkutatásokat indítanának Németországban. 2006. 12. 08. http://sg.hu/cikkek/49079/online_hazkutatasokat_inditananak_nemetorszagban. Letöltés ideje: 2013. 06. 24.

[7] Dajkó Pál: Lebukott az állami kémprogram. 2011. 10. 10. http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html. Letöltés ideje: 2013. 06. 24.

[8] Chaos Computer Club analyzes government malware. 2011. 10. 08. http://ccc.de/en/updates/2011/staatstrojaner. Letöltés ideje: 2013. 06. 24.

[9] Golovanov, Sergey: Spyware. HackingTeam. 2013. 04. 23. http://securelist.com/analysis/publications/37064/spyware-hackingteam/. Letöltés ideje: 2013. 06. 28.

[10] Marquis-Boire, Morgan – Marczak, Bill – Guarnieri, Claudio – Scott-Railton, John: For their eyes only. 2013. 05. 01. https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf. Letöltés ideje: 2013. 06. 28.

[11] Rouse, Margaret: spyware. 2006. 10. http://searchsecurity.techtarget.com/definition/spyware. Letöltés ideje: 2013. 07. 16.

[12] Spyware. http://www.spywareguide.com/term_show.php?id=12. Letöltés ideje: 2013. 07. 16.

[13] ehe: Superintendent Trojan. 2006. 10. 09. http://www.h-online.com/security/news/item/Superintendent-Trojan-731613.html. Letöltés ideje: 2013. 06. 28.

[14] Cyberperquisitions. 2008. 02. 28. http://www.lemonde.fr/idees/article/2008/02/28/cyberperquisitions_1016773_3232.html Letöltés ideje: 2013. 06. 28.

[15] Ausztriában törvényes lesz az online házkutatás. 2007. 10. 18. http://sg.hu/cikkek/55658/ausztriaban_torvenyes_lesz_az_online_hazkutatas. Letöltés ideje: 2013. 06. 28.

[16] Berta Sándor: Külföldi szervereket is megtámadhat a holland rendőrség. 2013. 05. 06. http://sg.hu/cikkek/97134/kulfoldi_szervereket_is_megtamadhat_a_holland_rendorseg. Letöltés ideje: 2013. 06. 28.

[17] McCullagh, Declan: FBI remotely installs spyware to trace bomb threat. 2007. 06. 18. http://news.cnet.com/8301-10784_3-9746451-7.html. Letöltés ideje: 2013. 06. 28.

[18] http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf. Letöltés ideje: 2013. 06. 28.

[19] O'Neill, Patrick Howell: Hackers claim to be selling NSA cyberweapons in online auction. 2016. 08. 15. http://www.dailydot.com/layer8/shadow-brokers-nsa-equation-group-hack/. Letöltés ideje: 2016. 08. 28.

[20] Franceschi-Bicchierai Lorenzo: Hackers Say They Hacked NSA-Linked Group, Want 1 Million Bitcoins to Share More. 2016. 08. 15. http://motherboard.vice.com/read/hackers-hack-nsa-linked-equation-group. Letöltés ideje: 2016. 08. 28.

[21] Gardham, Duncan: Government plans to extend powers to spy on personal computers. 2009. 01. 04. http://www.telegraph.co.uk/news/uknews/law-and-order/4109031/Government-plans-to-extend-powers-to-spy-on-personal-computers.html. Letöltés ideje: 2013. 06. 28.

[22] Sanders, Chris: Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1). 2010. 03. 17. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html. Letöltés ideje: 2013. 07. 16.

[23] Sanders, Chris: Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing. 2010. 04. 07. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html. Letöltés ideje: 2013. 07. 16.

[24] Sanders, Chris: Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking. 2010. 05. 05. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html. Letöltés ideje: 2013. 07. 16.

[25] Sanders, Chris: Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking. 2010. 06. 09. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html. Letöltés ideje: 2013. 07. 16.

[26] Fisher, Dennis: What is a Man-in-the-Middle Attack? 2013. 04. 10. http://blog.kaspersky.com/man-in-the-middle-attack/. Letöltés ideje: 2013. 07. 16.

[27] DuPaul, Neil: Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks.

[28] Biddle, Sam: The NSA Leak is Real, Snowden Documents Confirm 2016. 08. 19. https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/ Letöltés ideje: 2013. 07. 19.

[29] Wawro, Alex: What Is Deep Packet Inspection? 2012. 02. 01. http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html. Letöltés ideje: 2016. 09. 28.

[30] Dubrawsky, Ido: Firewall Evolution - Deep Packet Inspection. 2010. 11. 02. http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection. Letöltés ideje: 2013. 06. 28.

[31] BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely. http://berec.europa.eu/doc/2012/TMI_press_release.pdf. Letöltés ideje: 2013. 06. 28.

[32] Wawro, Alex: A simple guide to Deep Packet Inspection. 2012. 02. 01. http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/. Letöltés ideje: 2013. 06. 28.

[33] Messmer, Ellen: US government's use of deep packet inspection raises serious privacy questions. 2013. 04. 24. http://news.techworld.com/security/3444019/dhs-use-of-deep-packet-inspection-technology-in-new-net-security-system-raises-serious-privacy-questions/. Letöltés ideje: 2013. 06. 28.

[34] NSA slides explain the PRISM data-collection program. 2013. 06. 06. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Letöltés ideje: 2013. 06 28.

[35] MacAskill, Ewen – Borger, Julian – Hopkins, Nick – Davies, Nick – Ball, James: GCHQ taps fibre-optic cables for secret access to world's communications. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Letöltés ideje: 2013. 07. 05.

[36] HTTPS Everywhere. https://www.eff.org/am/https-everywhere. Letöltés ideje: 2013. 06. 28.

[37] MacAskill, Ewen – Borger, Julian – Hopkins, Nick – Davies, Nick – Ball, James: Mastering the internet: how GCHQ set out to spy on the world wide web. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Letöltés ideje: 2013. 07. 05.

[38] Poitras, Laura – Gellman, Barton: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. 2013. 06. 07. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Letöltés ideje: 2013. 06. 28.

[39] Man-in-the-middle attack. https://www.owasp.org/index.php/Man-in-the-middle_attack Letöltés ideje: 2013. 07. 16.

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Tamás MÓGOR
tamas.mogor@hm.gov.hu

THE DEVELOPMENT OF JTAC CAPABILITIES OF THE HUNGARIAN DEFENCE FORCES

Abstract

Since 2000, Hungary has achieved a number of capability milestones in Close Air Support (CAS). From initial tasks, performed by combat helicopters, under the direction of designated helicopter aircrew with experience of air -to-ground weaponry employment, to accomplishing CAS missions supported by JAS -39 EBS HU aircraft. From the 8th to 12th of December, members of the Joint Terminal Attack Control/Forward Air Control (JTAC/FAC) Unit at 86th Szolnok Helicopter Base, supplemented with controllers of Special Operations Battalion, successfully performed the actual Program review with accreditation performed by evaluators of United States Joint Staff and NATO AIRCOM. Accreditation sites were Budapest, Szolnok and Kecskemét.

Magyarország 2000 óta jelentős eredményeket ért el a közvetlen légi támogatási képesség kiépítésében. A kezdeti, harci helikopterekkel – levegő-föld fegyverzetalkalmazásban jártas kijelölt helikoptervezetők irányítása mellett – végrehajtott feladatoktól eljutottunk a JAS-39 EBS HU repülőgépekkel támogatott CAS feladatokig. Az MH 86. Szolnok Helikopter Bázison (MH 86. SZHB) lévő Előretolt Repülésirányító Csoport (ERICS) – kiegészülve az MH 34. Bercsényi László Különleges Műveleti Zászlóalj (MH 34. BLKMZ) katonáival – 2014. december 8 – 12 között sikeresen teljesítette az újabb Program felmérést, akkreditációt, melyet az Egyesült Államok Összhaderőnemi Parancsnokságának és a NATO Légierő Parancsnokságának az ellenőrei hajtottak végre. Az akkreditáció helyszínei Budapest, Szolnok és Kecskemét voltak.

Keywords: *Close Air Support (CAS), JTAC, FAC, Hungarian Air Force ~ közvetlen légi támogatás, JTAC, ERICS, Magyar Légierő*

INTRODUCTION

One of the responsibilities of the Hungarian Air Force is to provide aerial operations against ground forces and one specific mission set is Close Air Support (CAS). CAS is air action by fixed or rotary winged aircraft against hostile targets that are close to friendly forces, and which requires detailed integration of each air mission with fire and movement of these forces. Close Air Support must be integrated with the fire and maneuvers of supported forces. Execution requires joint force planning, continuous coordination and the control of the supporting aircraft. Joint planning and synchronized usage is done by the Air Operations Control Centre (AOCC), Air Liaison Officers (ALO), the Tactical Air Control Party (TACP), Joint Terminal Attack Controllers (JTACs) and Forward Air Controllers (FACs).

In light of the above the Hungarian JTAC/FAC Program was re-assessed and reviewed in Hungary between 08th and 12th of December 2014. The survey, assessment – was carried out a second time by a combined standardization team – examined the compliance of Hungarian procedures to US and NATO requirements. JFS ESC and FCS designated inspectors had to examine the compatibility of two basic documents – the Joint Force Close Air Support Memorandum of Agreement (JCAS MOA, hereinafter referred to as MOA) and Forward Attack Control NATO Doctrine (along with the existing NATO Standardization Agreement (NATO STANAG 3797 Ed. 6, hereinafter referred to as STANAG) – and Hungarian Joint Fire Support Program (hereinafter referred to as Program).

This was not the first time that the inspectors had visited Hungary. They visited us with various groups between 2008 and 2014 and, in accordance with the steps required by the MOA and STANAG, they assessed the status of the Program. In addition to such briefings, training events were also held which contributed to the creation and maintenance of a high level of Hungarian JTAC/FAC capability.

This article is very timely because in many ongoing operations around the world, Joint Terminal Attack Controllers/Forward Air Controllers are used during the execution of joint fire support to increase the efficiency of air-to-ground strikes. This tendency, in light of the events of earlier wars, will most likely be observed even more in future operations. Finally, it is anticipated that the new Program assessment/accreditation will be accomplished in 2017 which my study, incorporating the lessons learned of the past events, aims to assist.

DOCTRINAL BACKGROUND, EVALUATION CRITERIAS

Before starting the program accreditation process, the following conditions must be met for the asking nation:

- With accession to the MOA and with inclusion the ATP 3.3.2.2 / STANAG the partner country accepts the basic requirements set out in the documents;
- Programme sustainability has to be corraborated with treaties, bilateral or multilateral agreements;
- The accreditation must be formally requested from the JFS ESC and from the Commander Allied Air Command (COM AIRCOM) Ramstein;
- The partner country has to have a regulation or handbook that describes the JTAC/FAC concept, sets out the various tasks, all of the requirements and the documentation necessary for the training;
- The partner country must have either her own accredited schoolhouse, or her designated JTAC/FAC had to pass a theoretical course of an accredited schoolhouse and had to obtain a qualified rating.

The standardization and continuous quality assessment offers the clients (MOA/STANAG members) and the capability providers (schools, training centers, military organizations) clear, coherent and continuous guidance. The level of training can be enhanced through exchange programs which envisage the exchange of capable, experienced instructors between schoolhouses. This has the added benefits of increasing transparency of the programs and creating competition.

The collaboration enhances the continuous development and clarification of basic doctrines, procedures, tactical tricks, and the intent of unification results, that the JTACs/FACs achieve a minimum level of training.

Based on the above the following areas will be assessed during the accreditation:

- Doctrinal, administrative, training, personnel background necessary for the Program, which consists of:
  - Training of instructors and candidates;
  - Manning and quality of JTAC/FAC positions;
  - Status of infrastructure;
- Quality support background;
- Training and simulation aids;
- Shootings, accomplished with real weapon systems, training events;
- Equipment;
- Compliance with safety regulations;
- Cooperation, training with CAS aircraft and helicopters;
- Application of new methods in JTAC/FAC training;
- Raising new issues that are important for the JTAC/FAC community.

The MOA also defines the factors and findings which could occur during Program accreditation and result in the inspectors not recommending accreditation of the Program. Suspension of the Program could be recommended if:

- The requesting country does not have trained JTAC/FAC instructors;
- The applied standards are not written in the relevant doctrines;
- The JTAC/FAC staff did not meet the minimum training requirements;
- During accreditation serious safety malpractice has been committed;
- JTAC/FAC staff are not able to show their participation on compulsory education and training events.

IN 2014 THE COMBINED ACCREDITATION TEAM MADE THE FOLLOWING ASSESSMENT

Administration

JTAC Program Regulaion: The Hungarian national regulation provides clear guidance on JTAC training, certification, and qualification. It has been appropriately staffed and approved by their Ministry of Defense.

JTAC Training Process Phases:

- Phase I - Personnel Selection: Proper background, English knowledge and Pre-courses.
- Phase II - Initial Training: Academic/Simulation - USAFE AGOS; Practical, Live and Dry training - in Hungary.

– Phase III - Sustainment Training: Includes Spring and Fall continuation training (4 weeks), international exercises and training events.

JTAC Instructor Training Program: The Program is modelled after the USAF JTAC Instructor Training Program and meets MOA and NATO requirements.

JTAC and JTAC Instructor Evaluation Folder (Training Jackets): Training folder complied with the requirements of the MOA and ATP-3.3.2.2

Manning: Hungary currently maintains four JTAC Instructors and two JTAC Evaluators, which is sufficient to develop additional capability and sustain their current JTAC capability.

JTAC Production: Hungary has a total force requirement of 14 JTACs: Air Force (9), Special Operations Forces (5). Future capability is planned for 18 Air Force and 12 SOF JTACs.

Facilities (Szolnok):

Classroom: Sufficient to accommodate force structure; proximity to CAS capable range are good.

Audio Visual Equipment: Adequate to support a multimedia learning environment.

Billeting: JTACs are billeted in the local area.

Messing: Available.

Academics: Hungarian JTACs attend accredited JTAC/FAC schoolhouses.

Simulation/Training aids: Hungary does not currently have a JTAC/Fires simulator but is planning for a future acquisition. There is currently the ability to utilize the JAS-39 Gripen simulator for video downlink training.

Live events: Fixed wing (JAS-39) supported JT AC training.

Range Facilities: Veszprem and Varpalota are available to conduct the employment of a variety of air-surface and surface-surface weapons necessary to conduct live/dry/day/night integrated fires missions incorporating lasers and IR pointers. Airspace parameters are sufficient to present a variety of CAS profiles to JTACs for efficient training. Currently, laser guided munitions such as GBU-12 is not authorized in Varpalota due to footprint/safety issues.

Sorties (Day/Night): Assets were formally tasked to support the qualification training.

Equipment:

Communication: PRC-117F/G, PRC-152

Laser Target Designator (LTD): GLTD II and III

Infra-Red (IR) Pointer: IZLID 1000P

Night Vision Devices: PVS-14/15

Thermal Imager: See SPOT III (AN/PAS-21)

Laser Range Finder (LRF): VECTOR-21/PLRF-15C

Global Positioning System (GPS): PSN-13 DAGR

Remote Video Receiver: ROVER-V

Digital CAS Equipment: None

Safety: Qualified JTAC Instructors supervised all JTACs during dry terminal attack control.

According to the observations above, the Combined Standardization Team recommended continued accreditation for the Hungarian JTAC Training program and the program should be reviewed again within the next three years.

As a result of the observations, the Combined Standardization Team made a recommendation regarding English language proficiency: STANAG 3797 requires "proficiency in the English language to the equivalent of NATO STANAG 6001 Level 3" (chapter I, para 1. 1.2) The JTAC MOA requires JTAC proficiency at Level 3 for listening,

speaking and reading, and Level 2+ for writing. JTAC-Instructors require Level 3 proficiency in all four areas. HUN authorities have to confirm that national national C I level corresponds to SLP 3 IAW STANAG 6001 and that all four areas (Listening, Speaking, Reading, Writing) are tested during examination.

There are some issues were identified in the 2012 initial accreditation and are still valid, however there is a planned way ahead to address all JAS-39 issues within the next two years:

- Hungarian JAS-39 aircraft do not use Night Vision Goggles (NVGs), therefore Hungarian JTACs rely on U.S. and other nations to conduct night training with IR Pointers and NVGs. Based on available resources and priorities, the ability to provide NVG capability to JAS-39 has to be investigated;
- Hungarian JAS-39 Litening III targeting pods are not configured to provide video downlink (VDL), therefore Hungarian JTACs rely on U.S. and other nations to conduct VDL training. Based on available resources and priorities, the ability to provide VDL capability to JAS-39 targeting pods has to be investigated;
- Hungarian JAS-39 lacks the less expensive training ordnance (e.g. BDU-33) to conduct CAS training. Having training ordnance will facilitate more controls with weapons be more cost effective, and allow the engagement of targets at closer range. Based on available resources and priorities, the ability to provide training ordnance for JAS-39 has to be investigated.

Prior to the review, Hungarian JTAC Regulation was reviewed and recommendations were made to meet the requirements of NATO STANAG 3797. This included recommending that evaluations and upgrade training be accomplished by dual accredited personnel to ensure that requirement of the MOA and applicable STANAGs are met. The recommendations were added and the updated regulation was signed.

Hungary does not recognize Laser Operator (LO) specialization for personnel to designate targets with a ground Laser Target Designator (LTD). Current ATP 3.3.2.2. requires all personnel utilizing LTDs for target designation to have LO specialization as described in chapter I, para 1.4.c. and chapter 5 of this document. If HUN does not wish to have this specialization, they must make a reservation to ATP and STANAG 3797. It should be noted that the next version of the ATP will eliminate the LO requirement.

To use helicopters for CAS missions HDF has to consider the way ahead to a future attack helicopter capability and – as a temporary workaround – recommend exploring the feasibility of using Mi-8/17s as CAS platforms.

SHORT HISTORY OF HDF JTAC CAPABILITY

In 2000: Training for CAS procedures was started by the HDF 87th Bakony Combat Helicopter Regiment. During the first period, Mi-24 helicopter pilots were assigned to control the actions of aircraft.

In 2006: HUN JTAC Unit was established as a subunit of HDF 86th Szolnok Helicopter Base – under the command of Base Commander. Specialized Forward Air Controller training was held by MI-24 experts of HDF 86th Szolnok Helicopter Base at 2008. The HDF has offered two TACPs as elements of Battalion Combat Teams.

In 2007 – HUN JTAC unit accomplished first basic national JTAC training, and from October 2009 with signing of JCAS MOA became possible to send two JTAC candidates to the US for "top off" training. They were the first Hungarian qualified JTACs.

Due to their qualification since 2009 HUN JTACs/FACs1 deployed to Afghanistan, and accomplished the following missions in PRTs, OMLTs and ODAs:

[1] Regular and SOF JTACs/FACs

2009 – 2012 ISAF Provincial Reconstruction Team (Baghlan, Pol-e Khumri), SOF TF-10, Hungarian Special Operations Task Unit (FOB Airborne, Wardak);

2012 – 2014 ISAF Operational Mentor and Liaison Team (Baghlan, Khelagay), ISAF SOF TF-10, Hungarian Special Operations Contingent (FOB Joyce, Kunar and FOB Fenty, Nangarhar);

2013 - ISAF Military Advisor Team (Camp Spann - Marmal) ISAF SOF TF;

2014 - 2015 Resolute Support SOF, Hungarian Special Operations Contingent (Camp Marmal, Mazar E Sharif).

PERSONNEL AND TRAINING

According to the current organization HUN JTAC Unit consists of 18 personnel: Commander (OF-3), Supply NCO (OR-7) 8 JTACs (OF-2) 4 Signal operators (OR-6), 4 Drivers (OR-4). In order to improve the capability of HUN JTAC Unit the next staffs have been planned for the future: Commander, Deputy Commander, SGT Major, 2 Assistant NCOs, 3 JTAC-I/Es, 4 JTAC/ALOs, 8 JTACs, 4 ROMADs[2] (all together 24 personnel).

The Concept of Training is for JTAC/FAC officers to meet the requirements determined in NATO STANAG/JTAC MOA – HUN JTAC Program.

The following HUN JTAC/FAC training steps were completed:

– 2006 - 2008:

- English language courses (STANAG 6001 Level 3)
- FAC basic training in HU (based on ATP 3.3.2.1 (A))
- Foreign training courses:
  - NLAGOS[3]: Air Ground Operation Orientation Course
  - USAFE AGOS[4]: CAS orientation course in Croatia
  - French - German AGOS: FAC academic training
  - IMET[5]: Infantry officer course, Airborne, Ranger

– 2009 - 2014:

- Foreign training courses:
  - USAFE AGOS: Joint Firepower Course, JTAC Qualification Course
  - USMC EWTGLANT[6]: TACP Course
  - Grayling Air Gunnery Range: Top-off training

Actual Concept of Training:

A. Warrior Preparation Phase

1. Recruit from Military Academy
2. Basic Infantry Officer Course

B. General JTAC Training

1. National JTAC Pre-Course
2. JTAC Certification Process
   a) JTAC Qualification Course

[2] Radio Operator, Maintainer And Driver
[3] Netherlands Air-to-Ground Operations School
[4] United States Air-to-Ground Operations School
[5] International Military Education and Training
[6] United States Marine Corps Expeditionary Warfare Training Group, Atlantic

b) National Certification Training

3. Continuation Training

C. JTAC-I Upgrade Process

CONCLUSIONS

The Joint Terminal Attack Control is the single real joint area of warfare, which, with continuous processing of battlefield experiences, is the most dynamic battle impact. Its effects – mainly friendly fires causing war casualties – are the most sensitive issues concerning the media and the public opinion. This is the reason why it is very important that Hungary incorporates lessons learned from real operations to coninuously develop the Hungarian JTAC capability toensure that it remains modern and credible.

In the last 6-8 years the Hungarian air-ground capability has evolved considerably thanks to the commitment and motivation of its personnel, and thanks to the continuous support of staffs level of commands. We have to owe much to the United States Office of Defence Cooperation in Budapest for the procurement, training, exchange of experience and the organization and running of events.

The Hungarian JTAC/FAC ability can only be maintained in the long term with the development of a suitable career model, ensuring the replacement of staff. For the national defence and allied missions necessary to keep at constant level the capabilities of JTAC/FAC personnel, and furthermore – according to combat experience – should be improved.

The JAS-39 has a very capable mission debrief system which provides a complete playback of the entire CAS mission with full cockpit display, audio and targeting pod recording to facilitate debrief of both airerew and JTACs. This can be demonstrated to the team as a standard practice following CAS missions. The Hungarian Air Force has designated pilots and flying hours from the JAS-39 to aid in JTAC training. Furthermore, the cooperation and integration between the flying squadron and the conventional and SOF JTAC teams is vital.

Hungary still lacks a JTAC simulation system. Simulation could be used to train to rotary and fixed wing CAS procedures as well as providing for additional JTAC proficiency training at any time. Due to the high cost of aircraft and helicopter operations simulators are increasingly being used, which are connected to a network, and those are able to make practice the real mission execution, without actual fuel consumption and involving other resources. These reasons support, that acquisition of an accreditable simulator is essential.

All in all the latest Combined Standardization Team Report on the Hungarian Joint Terminal Attack Controller (JTAC) Program Review highlighted the solid foundations of the Program and emphasized the quality indicators over quantitative indicators.

Hungary has to continue the regional cooperation as well with delegation JTAC-I for SVN National JTAC courses, and would be beneficial to send and receive JTACs during Czech and Hungarian air weeks. In order to reduce the catering, travelling, training and accomodation costs with bartel procedure within CEDC countries (AUT, CZE, CRO, SLO, SVK) is preferable.

With the review of these experiences, and by adopting an innovative and progressive approach, this capability can be accredited next year again, which will also cement good relations between NATO member countries.

REFERENCES

[1] Hungarian Joint Fire Support Program

[2] STANAG 3797 ed.4.; MINIMUM QUALIFICATIONS FOR FORWARD AIR CONTROLLERS & LASER OPERATORS IN SUPPORT OF FORWARD AIR CONTROLLERS; NSA 2009.

[3] JCAS AP MOA 2004-01 Joint Terminal Attack Controller (JTAC) (Ground) 1 Jan 2012.

[4] Close Air Support JP-3-09.3, 2009.

[5] ATP-3.3.2.2 MINIMUM QUALIFICATIONS FOR FORWARD AIR CONTROLLERS & LASER OPERATORS IN SUPPORT OF FORWARD AIR CONTROLLERS, NATO 2014.

[6] Mógor Tamás: A Magyar Előretolt Repülésirányító (JTAC/FAC) Program értékelése a kettős felmérés tükrében; Repüléstudományi Közlemények XXVI./3. szám, pp. 7-14.; 2014.

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Pető Richárd
petorichard.mk@gmail.com

DRONE'S SAFETY AND SECURITY QUESTIONS I.

Abstract

Unmanned aerial vehicles (UAV) gained significant popularity in the past few years. Manufactured worldwide, used by both civilians and the military, as they are very versatile. Certain people and criminal organisations use them for nefarious purposes. Thousands of types are in existence, their sizes can range from the tiny mosquito to several meters. The author will describe the positive and criminal usages of UAVs, and will visit the life- and property safety questions regarding them.

A pilóta nélküli légijárművek (PNR) az elmúlt néhány évben jelentős népszerűségre tettek szert. Világszerte gyártják és fejlesztik, a katonai és civil szervezetek egyaránt használják, hiszen számos területen alkalmazhatóak. Sajnos egyes személyek és bűnszervezetek kifejezetten bűnös célokra használják fel. Jelenleg több ezer típusuk létezik, amelyek az egészen apró szúnyog mérettől a több méteres nagyságig elérhetőek. A szerző a cikkben röviden ismerteti kereskedelemben elérhető PNR-ek jó és bűnös szándékú felhasználási lehetőségeit, továbbá kitér PNR-rel kapcsolatos élet és vagyonbiztonsági kérdésekre.

Keywords: *UAV, drone, safety and security, terrorism ~ UAV, drón, PNR, élet- és vagyonbiztonság, terrorizmus*

DRONE'S SAFETY QUESTIONS

An unmanned aircraft[1] or drone is an aerial vehicle designed to be used without a human pilot on board. That makes it so impressive. Drones can be remote controlled, half automated and full automated. If you use half or full automated mode you don't need to watch and control continuously the flying machine because of the global positioning system (GPS) module communicating with the Flight Controller (FC) to hold the right course. Electronic speed controller (ESC) manages the rotation speed of motors.

Many people say if you want to drive you need to practice a few hours then you are ready. I think they are right and wrong at the same time. Why do I say that? Some hours are enough to learn the standard rules of flying with a UAV but not for safe flying. [1]

The most significant (working) categories of UAVs:

- home UAV,
- hobby UAV,
- hobby film and photo making UAV,
- professional film and photo making, surveying UAV,
- surveillance UAV,
- racing UAV,
- supplier UAV,
- construction UAV.

Each type of UAV has specific abilities, parameters and additional parts. Usages of the environments are greatly different from each other. Summarizing these differences you can recognize that all of them have variable usage risk.

Categories of UAVs

Home UAV

It is the simplest vehicle which is cheap and easy to fly. It has only manual control and comes without any remarkably useful payload, but hard to crash and the most of owners have.

It can be used only 1 to 15, or maximum 50 m with a flying time of maximum 7 minutes. The newest have gyro control so they are stable enough to hold position in the air without continuously controlling. Those which have integrated or portable cameras give more utility.

The most of mobile phones system (Android, IoS) have their own applications which give the possibility to capture video and photo if the phone is connected to the UAV. (see *Picture* 1) Place of usage are the garden or inside the home.

Picture 1: UAV with camera [2]

[1] Note: Author uses own definitions and categories (not NATO definition and categories).

Hobby UAV

Picture 2: Hobby UAV [3]

It is a more expensive category than the home UAV. Parts can be purchased separately or in a ready to fly kit. The practice is that UAVs built by owner is more frequent so it could have a wider range of add on equipment, for example GPS, camera, camera combined with transfer module and first person view (FPV) system. People who has hobby UAVs are most likely skilled because they enjoy controlling air vehicles. Place of usage are larger parks or large fields where there is nothing and nobody. (see Picture 2)

Hobby and professional photo, video (media) making, surveying UAV

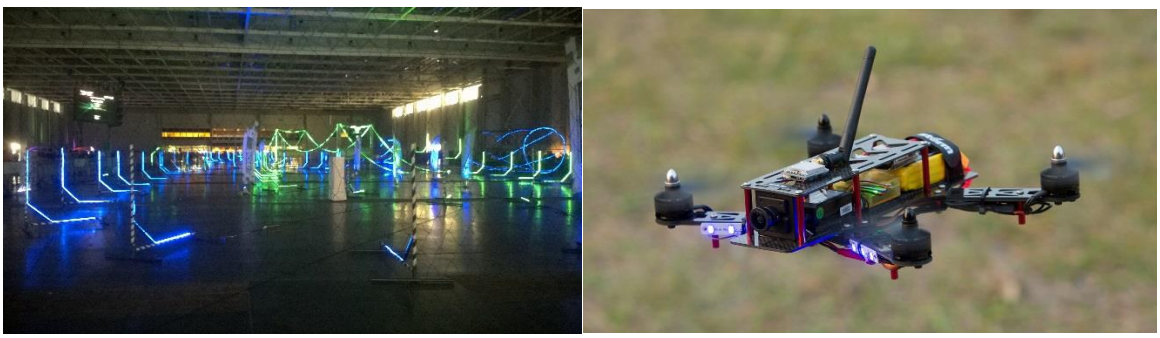
Hobby and professional media making category are similar, but professional equipment is 1 to 10 or more times expensive. Usually the UAVs have a lot of safety of software and hardware solutions to protect the vehicle from erratic flight, communications and to prevent crashes.

The pilot must be well skilled. Place of usage are forest, parks, plantations, programs inside or outside built in areas.

Surveillance UAV

UAVs are used for field, territory, objects monitoring and person scouting or searching. It needs to be a well-constructed and high performance UAV and Unmanned Aircraft System (UAS). The system is either half or full automatized, has high level safety solutions and it needs to be silent. These UAVs must be capable of long range flight and carrying a night and day camera, thermal camera, etc.

Racing UAV



Picture 3: Race place [4] and racing drone [5]

It is one type of hobby UAV, but the pilot and UAV requirements are higher. The racing UAVs able to fly on high speed (sometimes it is more than 110 km/h), must be low weight (ordinary it is 400-800 g) and have good maneuver ability to change flyway fast. All of them have small camera which connect to FPV google. Pilot must be skilled and have good reflexes. (see *Picture*3)

Supplier UAV

These air vehicles are capable transferring a heavy load (10-15 kg) for a long time.

Delivery shipments depend on the field they are used in. The Table 1 shows some fields and shipment possibilities.

Table 1: Exertions and shipments [6]

Exertions	Shipments or UAV additional equipment
Medical support	blade shape, drug, defibrillator,
SOS support	rope, water, lifebelt, antidote
Systematic logistic support	goods, commodity
Factory and agriculture support	toxic gas and radiation monitor; heat monitor;
Construction support	heat sensor, camera
Military support	weapon, camera

Medical and SOS supplier

Picture 4: Medical [7] and SOS supplier UAVs [8]

Many places on the Earth are hard to approach. High mountains, great deserts, oceans, seas, volcanic lands need lots of time and energy if someone wants to travel through, and last but not least, have potential threats. [9]

If someone receives a snake bite, has a fibrillation problem, falls into water or gets stuck on a mountain has perhaps only hours or minutes until they die.

The UAV's benefit is that it can avoid the most of the potential threats on land, because it moves in the air. They avoid barriers on land so it is possible to send quick help to any problematic event.

Systematic logistic support

Picture 5: Package delivering UAV [10]

Logistics is one of the key competitive factors for companies. The quick delivery by UAVs from a company is a future option parallel to the standard transportation of products and goods.

This task requires high level safety, and constant communication between the start and end point. In the future, UAV flights can be faster, more cost-efficient and more versatile.

Products and goods could be electrical equipment, food, clothes and other necessities, etc.

Factory and agriculture supplier

The UAV could represent a potential solution to monitoring and analysing factories and vehicles (train, truck, ship, etc). It could be a safe solution for disaster recovery organization to scout the area without endangering human and animal life.

Picture 6: Analysing fields [11] [12]

UAV providing with multispectral cameras can take combined pictures from fields of plant and able to highlights differences between healthy and distressed plants. UAV can help measuring status of giant plant field.

Construction

Picture 7: Suspension bridge under construction [13]

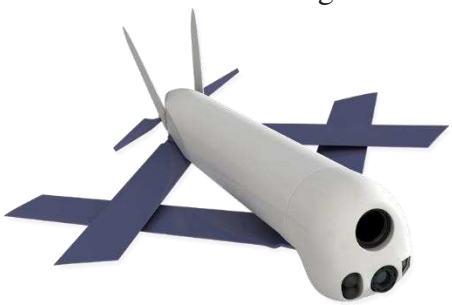
One of the future's most advanced technology is going to be the field of construction UAVs.

UAVs which are capable to work in teams and build light constructs without personal controlling. UAV must have accurately programmed and continuously working communication, and positioning systems.

DRONE'S SECURITY QUESTIONS

Military supplier UAV

Military sphere required special features from UAVs. Surveillance and transporting are standard necessities in military life. The most advance UAVs are capable of flying for a long time and distance, they are reliable and can function regardless of weather.



Picture 8: Military supplier UAV [14]

The newest line of UAVs is the tactical UAVs which can support friendly land units in the battlefield. These new machines can easily destroy enemy people in cover or light armoured vehicles. [15][16]

Criminal usage of UAV

Surveillance-, racing-, and supplier UAVs are the wonders of present and future. The delivery systems have wonderful possibilities, but also pose a big threat. [17][18]

" 

Picture 9: Smuggling drugs, weapons [19] [20]

UAVs have been called the ideal “smuggler mules” because they allow drug cartels, smugglers and criminals to transport shipments more quickly, with less of risk of being caught.

Unauthorized surveillance and delivery of illegal items, these are just some of the current concerns.

Picture 10: UAV delivers unidentified box [21]

In the hands of someone with a malicious intent, a box can be a weapon stuffed with hidden, remote-controlled or time controlled explosives. If the box explodes it can cause large damage to people and buildings.

In addition, there are so many ways that drones can be used, as either a supportive component or central part of terrorist attacks against innocent people, government officials, or infrastructure systems.

Without “useful” payload, driving them into airplanes taking off or landing can cause a huge catastrophe. If the plane crashes into a crowded city, many people may die and kerosene will cause a secondary disaster. [22] [23]

CONCLUSION

UAVs can be a great solution for a wide range of engineering problems and can make tasks easier to perform. It has only two “small” questions:

What will be the rules and limits of using an UAV? How can we find a way to encourage good use and prevent catastrophes?

What is the rule of usage of UAV demarcation line? How can make the balance drone technology for a good and bad use?

„ Az Emberi Erőforrások Minisztériuma ÚNKP-16-3/IV. kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült”

„ Supported BY the ÚNKP-16-3/IV. New National Excellence Program of the Ministry of Human Capacities”

Bibliography

[1] Electronic Privancy Information Center (EPIC) – Domestic Unmanned Aerial Vehicles (UAVs) and Drones. https://epic.org/privacy/drones/ (08/10/2016)

[2] UAV with camera: Author’s photo

[3] Picture: Hobby UAV: Author’s photo

[4] Race place: Author’s photo

[5] Racing drone https://i.ytimg.com/vi/dH9qEJb-c8c/maxresdefault.jpg (09/10/2016)

[6] Exertions and shipments: Author’s table

[7] Medical UAV; http://cdn.simplebotics.com/wp-content/uploads/2014/02/pars_drone.jpg?378dbc (09/10/2016)

[8] SOS supplier UAV; http://i.dailymail.co.uk/i/pix/2014/10/28/1414540757343_wps_24_epa04466923_A_woman_gives.jpg (09/10/2016)

[9] Simplebotics http://www.simplebotics.com/2014/02/lifeguard-drone-could-save-lives.html (09/10/2016)

[10] Package delivering UAV; http://i.dailymail.co.uk/i/pix/2013/12/09/article-2520818-19FB489500000578-0_634x345.jpg; (09/10/2016)

[11] Analyzing fields https://www.youtube.com/watch?v=8e4kcyUR_pw (09/10/2016)

[12] Analyzing fields; http://www.britishgas.co.uk/business/blog/wp-content/uploads/2016/08/Firefighting-Drones-jpg.jpeg (09/10/2016)

[13] Suspension bridge under construction https://www.youtube.com/watch?v=RCXGpEmFbOw (09/10/2016)

[14] Military supplier UAV https://www.avinc.com/images/uploads/prod_thumbs/833/01.png (09/10/2016)

[15] AV-AeroVironment https://www.avinc.com/uas/adc/switchblade (08/10/2016)

[16] Pető Richárd: Switchblade taktikai UAV a katonai alkalmazásban, Műszaki Katonai Közlöny XXIV. évfolyam, 4. szám; ISSN 2063-4986; pp. 101-108.; http://www.hhk.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2014_4sz/ossz_2014_4sz.pdf (09/10/2016)

[17] Brian McNary: Drones: The Good, The Bad & The Unknown; August 20, 2015; https://www.pinkerton.com/blog/drones-the-good-the-bad-the-unknown/ (09/10/2016)

[18] Pető Richárd: UAV-k alkalmazásában rejlő lehetőségek és veszélyek; Műszaki Katonai Közlöny XXIV. évfolyam, 3. szám; ISSN 2063-4986; pp. 105-115.; http://www.hhk.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2014_3sz/10_UAV-k%20alkalmazasban.pdf (09/10/2016)

[19] muggling drugs, weapons; https://sustainablesecurity.files.wordpress.com/2016/02/crahed-drone3.jpg (09/10/2016)

[20] Smuggling drugs, weapons; https://il4.picdn.net/shutterstock/videos/15257689/thumb/4.jpg (09/10/2016)

[21] UAV delivers unidentified boksz; http://i.dailymail.co.uk/i/pix/2015/03/24/15/26F35A5D00000578-0-image-a-25_1427211862103.jpg (09/10/2016)

[22] Federal Aviation Administration (FAA)-Unmanned Aircraft System; https://www.faa.gov/uas/ (09/10/2016)

[23] Civil Aviation Authority – Flying drones; https://www.caa.co.uk/Consumers/Model-aircraft-and-drones/Flying-drones/ (09/10/2016)

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Szabó András
szabo.andras@uni-nke.hu

KUTATÁSMÓDSZERTAN IT ALAPOKON

Absztrakt

A tudományos kutatások - hasonlóan a hétköznapok problémáinak megoldásához - egy-egy helyesen feltett kérdésre próbálnak választ találni. Hasonlítanak abban, hogy az aktuális problémára hasznos és a gyakorlatban is kivitelezhető megoldásokat keresnek, alapvetően eltérnek azonban a megoldás keresésének módszerességében, tervezettségében és szervezettségében. Jelen cikkemben azokat az innovatív módszereket mutatom be, amik segíthetik, vagy akár reformálhatják is a klasszikus kutatásmódszertant. A kutatások lépéseinek sorrendjében mutatom be az egyes fázisok végrehajtását könnyítő, gyorsító módszereket. Elsősorban a gyakorlatban könnyen kezelhető, egyszerűen tanulható újításokra fókuszáltam (hiszen általánosan elmondható, hogy egy informatikai innováció akkor lesz igazán sikeres, ha annak használatát az alkalmazók könnyen el tudják sajátítani).

Similar to solving everyday problems, researchers trying to find answers to questions which are posed correctly in a scientific manner. In both case we try to solve current problems, using methods which are feasible in practice, but fundamentally different in methodology. In a scientific research the participant follows a systematically designed and well-organized workflow. In my article, I present tools for researchers, which hopefully can simplify the time and effort for the research, or even can reform the traditional research methodology. IT innovations will be successful only if users can easily acquire the hands-on, so I focused on tools which are practical and easy to learn.

Kulcsszavak: *kutatás, módszertan, IT, informatika ~ research, methodology, IT based, Computer Science*

BEVEZETÉS

Jelen kutatásom céljául tűztem ki azt, hogy összegyűjtsem azokat az innovatív módszereket és eszközöket, melyek:

- segíthetnek minket tanulmányaink során[1],
- növelhetik kreativitásunkat (elősegítve ezzel egy tudományos felfedezést, innovációt),
- valamint hozzájárulhatnak tudományos vizsgálataink hiteles és eredményes végrehajtásához.

Közhelynek számít, hogy az informatika napjainkban mindenhol jelen van. Szinte biztos, hogy e sorok olvasója használja az interneten keresztül elérhető web szolgáltatásokat[2] mindennapi munkája, tanulmányai vagy éppen magánélete során. A web evolúciójában a 3.0 nál járunk [1], mely hasonlatosan az emberiség evolúciójához az önálló kezdeményezésektől a közösségi kollaboráció felé tart (pillanatnyilag az ember-ember és ember-gép kapcsolatok mellett már a gép-gép kommunikációra is látunk példát).

Elemzésem követi ezt a fejlődési tendenciát, és a kutatók által használható forrásgyűjtő- és feldolgozó eszközök bemutatása mellett a szakmai kapcsolatok keresésére, a közös munkát elősegítő alkalmazásokat és hálózati szolgáltatásokra is mutatok néhány példát.

AZ INTERNET SZEREPE

A számítástechnika, és az internet segítségével elérhető informatikai szolgáltatások szinte minden tudományterületeket érintenek. Kutatások sora bizonyítja, hogy gyorsabban, hatékonyabban oldanak meg korábban elképzelhetetlen problémákat. Ugyan napjainkban az internet a legtöbb ember számára az elektronikus médiatartalmak böngészésének, a szórakozásnak, a társas érintkezés egy eszközét jeleni, írásomban visszatérek az internet elődjének, az ARPANET[3]-nek eredeti funkcionalitásához, és rávilágítok arra, hogyan tudja a kutatásokat támogatni.

Az internet segítségével könnyíthetjük kutatásainkat (a már ismert módszerek megismerése révén), és rövidíthetjük a rá szánt időt (a trendek követésével, a tudományos „zsákutcák” elkerülésével, és a rossz koncepciókból való tanulás révén). Más kutatók gondolatai, javaslatai, kérdései akár szemléletmódunk változását is eredményezhetik, mely révén új nézőpontból kezdjük vizsgálni a problémát. A következőekben felsorolok néhányat a számtalan lehetséges felhasználási mód közül (kezdve a közismert felhasználásoktól, haladva a kevésbé ismertek felé).

Az internet, mint digitális könyvtár [2]

A legegyszerűbb megközelítés alapján az interneten keresztül elérhető adatbázisokat, könyvtárakat, online folyóiratokat, cikkeket használhatjuk pusztán információforrásként (legyen célunk a tanulás és általános tájékozódás, vagy tudományos kutatásunk

[1] Nehéz megkülönböztetni mikor kutatunk, és mikor tanulunk, hiszen a kettő összefügg: a kutatás során a korábban elsajátított tudást felhasználva, a megszerzett információkat újrarendezve, és újakat gyűjtve ismerjük meg az adott problémát. Az önálló tanulás során pedig új módszereket használva, felfedezve gyűjthetjük össze a szükséges információt, és újszerű tanulási módszereket használva sajátíthatjuk azt el.

[2] Pl.: tartalom, tárhely, chat, blog, közösségi-kapcsolati szolgáltatások

[3] Advanced Research Projects Agency Network

megalapozására szolgáló forrásgyűjtés). Ezeket napjainkban már kiegészítik a Web 2.0 [4] és a Web 3.0 [5] által nyújtott szolgáltatások.

Sajnos sokak számára az internet egyet jelent egy-egy közismert keresőmotorral, ezzel pedig a találatok beszűkülnek az adott kereső adatbázisára (ezért is érdemes egy-egy forráskutatás során több alternatívát is kipróbálni, pl.: a Google, a Yahoo és a Bing keresőmotorokat is felhasználni). Az alábbiakban (1. táblázat) a *„scientific research”* kifejezésre kerestem különböző keresőmotorokkal. Az eredmények mennyiségi különbségét a harmadik oszlop szemlélteti, de azt sem szabad elfelejteni, hogy ekkora mennyiségű találatnál (sokszor milliós értékek) a találatok pontossága (a keresés szempontjából releváns vagy sem) és prioritása (sorrendisége) sem elhanyagolható tényezők (melyeket csak az adott kutató tud megítélni).

1. táblázat. A WEB adatbázisok, keresőszolgáltatások találati arányáról

Keresett szöveg:”*scientific research*” (keresés dátuma 2016.01.04)		
Szolgáltató	**Elérési út (URL cím)**	**Találatok száma**
Google	*google.com*	426 000 000
	google.hu	105 000 000
	google.cn	132 000 000
Yahoo	*yahoo.com*	114 000 000
Bing	*bing.com*	54 700 000
Deeperweb	*deeperweb.com*	45 300 000
Zuula	*zuula.com*	38 400 000
IEEE Xplore Digital Library	*ieeexplore.ieee.org*	10 526
Internet Archive	*archive.org*	14 333
duckduckgoo	*duckduckgoo.com*	200
Yippy	*yippy.com*	276

Az internet, mint kommunikációs platform

Az internetet használhatjuk kommunikációs eszközként, mely segítségével együttműködünk más, akár a világ távoli sarkaiban tevékenykedő kutatókkal[6]. Ugyancsak kommunikációs célra felhasználhatjuk ezt a csatornát távoli eszközök, mérőberendezések, szenzorok vezérlésére, vagy a mérési eredmények letöltésére[7]. A hálózat nyújtotta előnyökre jó példák azok a kutatóprojektek, melyek az elosztott számítási kapacitások kollaborációjára épülnek[8].

Az un. rejtett szakértők [3] (akik a vállalatoknál végzett napi munkájuk megakadályoz abban, hogy publikáljanak, konferenciákra járjanak), és a kihasználatlan kutató potenciálok (pl.: nyugdíjba vonult szakemberek) problémájára is megoldási lehetőséget biztosítanak az internet tudományos témájú közösségi hálózatai.

[4] Web 2.0-nak nevezzük az olyan szolgáltatásokat, melyek az egyének közötti tevékenység támogatását, a közös munkavégzést, a közösségi tartalom előállítását teszik lehetővé. Itt jelentek meg a geolokáció alapú szolgáltatások (pl.: a keresők a nyelvterület, vagy az ország szerint más-más keresési eredményeket ad vissza).

[5] Web 3.0 a következő fejlődési lépcső, melynél már nemcsak a geolokáció, hanem a felhasználó személyisége (korábbi keresési előzményei, számítógép beállításai, stb.) is befolyásolják a találatokat.

[6] Akár a világ távoli sarkain túl is (pl.: az ISS nemzetközi űrállomás kutatásait figyelhetjük meg a http://spacestationlive.nasa.gov/timeline/ weblapon)

[7] Néhány példa az interneten elérhető szenzorhálózatra a költöző madarak útvonalát ábrázoló http://www.satellitetracking.eu/inds/showtable és a http://map.mme.hu/page/introduction, a rádióspektrum monitorozására alkalmas http://websdr.org/, vagy a villámok előfordulási helyét ábrázoló http://www.lightningmaps.org/realtime?lang=hu

8 Pl.: a SETI projekt http://setiathome.berkeley.edu

Az internet, mint elektronikus média

Az internet publikációs platform is az előzőek mellett, melyen beszámolhatunk elért eredményeinkről, jelenlegi kutatásaink állapotáról (pl.: az írott eredményekről online folyóiratokban, esetleg előadásainkról videó megosztó oldalakon), vagy csak kezdetleges ötleteinkről, javaslatainkról (pl.: saját weblapunk, blogunk segítségével). Multimédiás támogatással a korábban elhangzott előadásainkat megoszthatjuk másokkal, vagy akár már részt is vehetünk online konferenciákon[9].

Valójában akkor használjuk ki optimálisan a „Hálózatok hálózatát", ha nem csak egy-egy fent említett részfunkcióra, hanem ezek egészére használjuk.

A kutatás megkezdése

„Miért is kutatunk?" Tehetjük fel az örök kérdést. Számtalan oka, külső és belső motivációja lehet annak, hogy miért végzünk ilyen tevékenységet, például:

- egy hétköznapi probléma megoldása,
- kutatás-fejlesztési munka (pl.: fejlesztőmérnökként, doktoranduszként stb.),
- önálló tanulmányi munka (évközi beszámoló, TDK dolgozat, szakdolgozat, diplomamunka stb.),
- tanulás, önképzés,
- oktatóként jegyzetkészítés, vagy kiegészítés, tananyagfejlesztés céljából.

Ezek alapján eltérő mennyiségű idő, erőforrás, kutatószemélyzet áll rendelkezésünkre, mely ugyancsak fontos szempontja a helyes kutatási módszerek kiválasztásának. A megszerzett ismeretanyag, a saját tudásunk és képességeink is meghatározzák lehetőségeinket (pl.: ha a problémát algoritmizáljuk, és egy alkalmazás fejlesztésével szeretnénk megoldani, rendelkeznünk kell alapvető programozói ismeretekkel, vagy esetleg meg kell tanuljunk egy új programozási nyelvet, amely ideális az adott probléma leírásához).

Egy-egy probléma tudományos megoldásához kutatásunk tervezettsége és módszeressége visz minket közelebb. Ha előre elkészített, szisztematikus és logikusan felépített tervvel rendelkezünk, átláthatóvá válik munkák, így könnyebben fel tudjuk ismerni (és meg tudjuk különböztetni) esetleges hibáinkat, tévedéseinket, valamint a lehetséges megoldásokat. A tervezés nélkülözhetetlen, főleg ha a probléma megoldása túlmutat személyes kapacitásainkon (szakismeret, idő, pénz stb.) és másokkal kell együttműködnünk.

A KUTATÁS LÉPÉSEI

Először is nézzük meg hogyan állunk neki egy kutatásnak. Természetesen az egyes tudományterületeknek vannak sajátosságai, azonban az alapvető lépésekben megegyeznek. Az általános kutatás-módszertani elveket és módszereket nem kívánom részletezni, hiszen számtalan jegyzet [4] [5] [6], tanulmány [7] és könyv [8] [9] foglalkozik ezzel a témával. Arra azonban felhívnám a figyelmet, hogy az előzőekben említett szakirodalmak szerzői jellemzően csak a saját tudományterületek módszertanára fokuszáltak (pl.: a műszaki területen a mérések, a természettudományok esetén a kísérletek és megfigyelések, a társadalomtudomány területén pedig a kérdőívek összeállítása a jellemző adatgyűjtési eljárás). Érdemes a tudományterületünk jellemző módszerei mellett mások eljárásaival, metodikáival is megismerkedni, ezzel is bővülhet a saját eszköztárunk, nem is beszélve arról, hogy könnyebben tudunk majd más tudományterület kutatóival együttműködni.

9 Pl.: https://webcast.web.cern.ch/webcast/

Témaválasztás

Minden kutatás megkezdése előtt tájékozódnunk kell az adott téma aktualitásairól, hiszen egy kutatás nem lehet öncélú, elavult, haszontalan. Olyan témát kell tehát választanunk, mely a tudomány, a társadalom időszerű kérdéseivel foglalkozik, azokra próbál elismert módszerek segítségével tudományosan megalapozott válaszokat adni.

Ezek aktualitásának vizsgálatában is segítségünkre lehet az internet, a különböző weblapok és adatbázisok[10].

Módszerek meghatározása

Már magának a kutatási témánknak megfelelő módszerek összegyűjtése, és a megfelelő(k) meghatározása is egy külön kutatómunka eredménye. Kutatási stratégiánkban határozzuk meg a felhasználandó módszerek és eljárások kombinációját.

Kutatási stratégiák [10]:

Induktív kutatási stratégia - a kutatott probléma megértése érdekében a kutatás során gyűjtött adatokat elemezzük, és azok alapján általános igazságokat ismerünk fel.

> *Leíró kutatási stratégia* - a valóság adott állapotát, annak tulajdonságait rögzítjük.
> *Összefüggés feltáró kutatási stratégia* – ezzel a módszerrel a vizsgálat tárgyának két vagy több tulajdonsága között fennálló kapcsolat, összefüggést kívánjuk felfedezni.
> *Kísérleti stratégia* - a változók közti kapcsolatot kontrollált körülmények között végrehajtott változtatásokkal, azok hatásainak megfigyelésével ismerjük fel.

Deduktív kutatási stratégia – már felismert törvényszerűségek, általános szabályok alapján jutunk el a probléma megoldásához.

> Elegendő, ha csak irodalomkutatást végzek? Vagy szükséges kvalitatív, esetleg kvantitatív kutatást is folytatnom? Mérést végezzek, vagy elég ha szimulációval demonstrálom elméletemet? Ezekre és még számtalan hasonló kérdésre kaphatunk választ, ha áttekintjük kutatótársaink kutatási terveit[11] mielőtt belevágunk saját projektünkbe. Ezek mellett segítséget nyújthat a stratégia kiválasztásában a *SAGE Research Methods* weblapja[12] is, vagy egy általunk generált összehasonlító táblázat[13], ahol pro-kontra elven összehasonlíthatjuk ezeket, majd ezek alapján a számunkra megfelelőt kiválaszthatjuk.

Kutatásunk megkezdése előtt készítünk egy előzetes forráskutatást, annak érdekében, hogy megállapíthassuk:

- létezik-e már megoldás a vizsgált problémára,
- milyen módon próbálták már mások megoldani azt,
- melyik utat nem választotta még senki,
- hogyan tudjuk esetleg javítani a hatékonyságát egy már létező megoldásnak újszerű megközelítéssel vagy alternatív módszerekkel.

[10] Ha ötleteket keresünk, akkor például a hazai kutatók kutatási eredményeit a https://www.mtmt.hu/, a MTA kutatócsoportjainak témáit a http://mta.hu/cikkek/az-mta-lendulet-kutatocsoport-halozata-131393, a hazai és külföldi egyetemek doktori iskoláinak, szakkollégiumainak, különböző tudományos műhelyeknek, K+F szervezeteknek, vállalati kutatólaboroknak, tudományos konferenciáknak témáit pedig saját weboldalukon tekinthetjük meg.

[11] Pl.:doktori értekezések bevezető részei, melyek az alkalmazott módszertant mutatják be

[12] Link: http://srmo.sagepub.com/methodsmap#/T0/T5/T0-3/T0-0-14

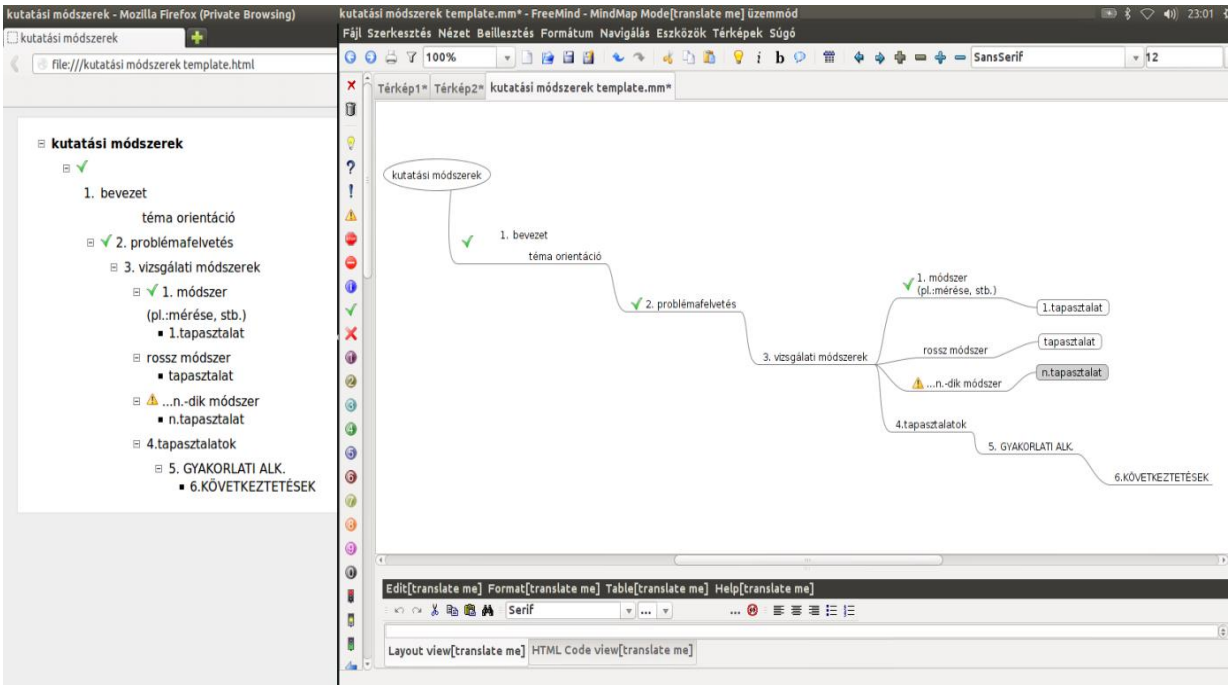
[13] Ezt elkészíthetjük egy táblázatkezelő segítségével, vagy online az alábbi táblázat, diagram készítő alkalmazások segítségével:http://www.makeuseof.com/dir/chartall/ , vagy a http://www.chartle.net/

A kutatási probléma megfogalmazása, célkitűzés

A jól megfogalmazott kérdés magában hordozza a választ is. Ahogy Douglas Adams, *A galaxis útikalauz stopposoknak* című regényéből megtudtuk a 42 a válasz az életet, a világmindenséget, meg mindent érintő végső kérdésre. Ha a válasz a 42, akkor vajon mi a helyes kérdés? Ennek a kérdésnek a keresése a regény fő mozgatórugója. Ebből is látszik tehát, hogy kutatásunk sarkalatos pontja a kutatási probléma és az elérendő célok pontos és egyértelmű definiálása.

Hasznos lehet, ha korai ötleteinket, kutatási kezdeményeinket vizuálisan ábrázoljuk, és un. „brainstorming”[14]-ot folytatva rendszerezzük gondolatainkat. Mivel a kutatások kezdeti fázisában járunk, így a kreativitást szabadjára engedve összegyűjthetjük ötleteinket, melyek közti logikai relációkat, ok-okozati viszonyokat később jelölhetünk (fogalomtérképen[15] ábrázolva azokat).

A *Freemind* nevű java[16] alapú alkalmazás ebben segít minket, mely a generált „ötletfát” akár web-re feltölthető formátumba is képes konvertálni. Az alábbi képen egy ilyen tervre látunk mintát (a *Freemind* grafikus felületét a kép jobb oldalán, a generált html lapot bal oldalon látjuk). Ezzel az alkalmazással hierarchikusan (egymás alá-felé rendelt módon) rendezett gondolattérképet tudunk generálni.

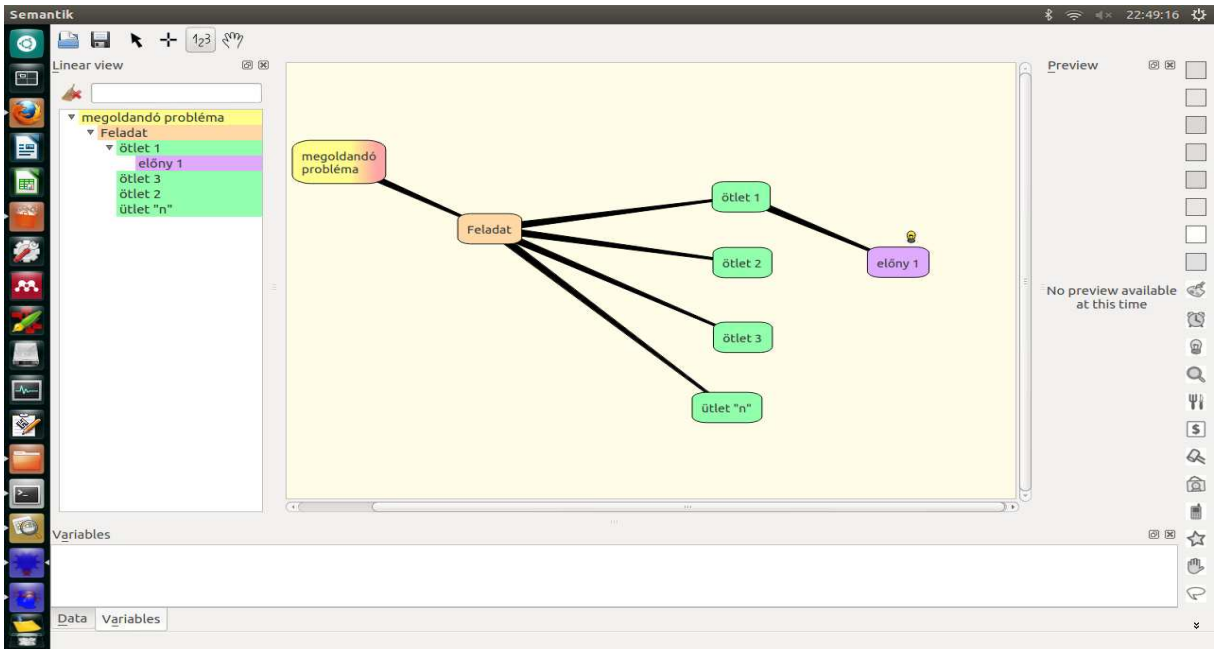


1. ábra. A Freemind web alapú (bal oldalt), és a grafikusan ábrázolt agytérképe (jobb oldalt)

Ha nem szeretnénk, vagy nem tudjuk ezt a rendet meghatározni, vagy a későbbiekben módosítani szeretnénk, akkor egy másik nyílt forráskódú alkalmazás, a *Semantik*[17] használatát javaslom, melyben a „gondolatok” közti logikai kapcsolatok könnyebben változtathatóak. Számtalan további ingyenes program érhető el a különböző operációs rendszerekre (*Windows, Linux, OSX, Android, stb.*), melyekkel hasonló agytérképeket tudunk szerkeszteni. Az „okos”

[14] Az angol „brainstorming” tevékenységet magyarul gondolat térkép készítésének nevezzük.
[15] A fogalomtérkép a különböző fogalmak közötti kapcsolatok megjelenítésének eszköze.
(Forrás: Duchon Jenő – Elektronikus tanulás (2015) http://www.tankonyvtar.hu/hu/tartalom/tamop412b2/2013-0002_elektronikus_tanulas/tananyag/JEGYZET-14-2.6._Vazlatok__jegyzetek__abr.html)
[16] Ennek köszönhetően Windows, Linux, Mac OSX operációs rendszereken is futtatható.
[17] Lásd: http://kde-apps.org/content/show.php/Semantik?content=55242

platformok segítségével pedig bárhol is járunk a világban, ki tudjuk egészíteni agytérképünket.

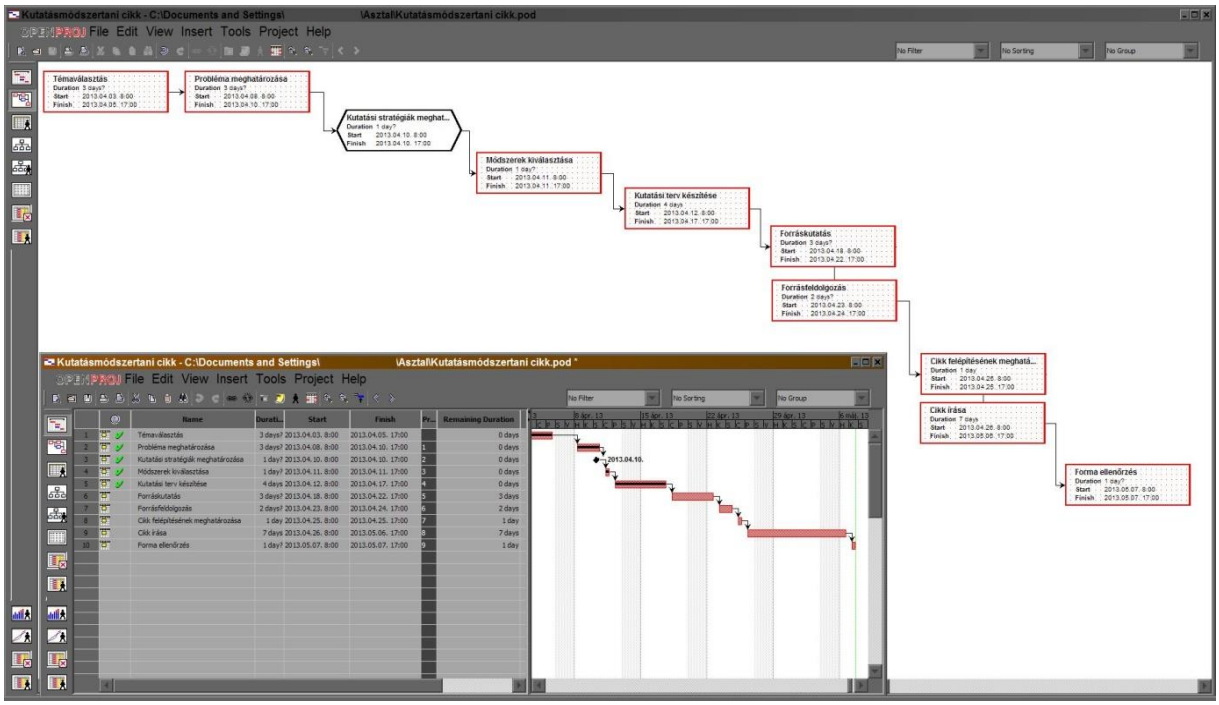


2. ábra. Egy, a Semantik programmal készített gondolattérkép

Kutatási terv készítése

Kutatási tervünk logikus formába önti kutatási problémánkat, összefoglalja a célkitűzésünket, a kiválasztott módszert, a felhasznált eszközöket és erőforrásokat, a kitűzött határidők (legyenek azok általunk meghatározott, vagy külső tényezők miatt betartandóak), a feladatok munkaigényét (munkaórában, vagy a feladathoz szükséges létszámban megadva).

Az üzleti életben tevékenykedő nagyvállalatok komplex projektjeik nyomon követése érdekében komoly informatikai fejlesztéseket folytattak, melyek eredményeképpen számos módszertant és szoftvert fejlesztettek ki. Ezeket akár kutatásaink tervezésre és lebonyolítására is felhasználhatjuk. Egy ilyen eszközre láthatunk példát az alábbi képen:



3. ábra. Jelen kutatásnak az Openproj alkalmazás segítségével elkészített terve (táblázatos formában alul, grafikusan felül)

Forráskutatás

Az információs társadalom „előtti” időszakban a kutatóknak csak korlátozott lehetőségek álltak rendelkezésünkre az információ gyűjtésére, és megosztására:

- könyvtárak,
- szakmai folyóiratok,
- konferenciák, és egyéb szakmai fórumok.

Az internet elterjedésének kezdetén ezeknek az elektronikus megfelelői alakultak ki először. Triviális példa az online könyvtárak és könyváruházak említése, melyekben ingyenesen, vagy fizetség ellenében jutunk hozzá a kívánt publikációkhoz. A technológia fejlődése következtében azonban már online könyvkölcsönzésre is lehetőségünk van [11], ezzel is csökkentve a kutatásra szánt költségeket[18].

A konferenciák előadásanyagainak szöveges formátumú és multimédiás megosztása, a kutatási eredményeket tartalmazó fájlok (mérések, algoritmusok, alkalmazások, stb.) feltöltése, az előadások online sugárzása leegyszerűsíti a kutatók dolgát, hiszen már nem szükséges fizikailag részt venni a kutatási területéhez kapcsolódó előadáson, továbbá akár évek múltával is megtekintheti az előadást.

Direkt keresési módszerek

Az internet, vagy ahogy szokták még nevezni, a „hálózatok hálózata” autonóm rendszerekből épül fel, tehát egységes rendezési elvtől mentes. Ezt a rendezetlenségét a különböző tematikus[19] és nyílt szavas[20] keresők próbálják átláthatóvá tenni. A korábban említett ötletek, kulcsszavak és keresni kívánt fogalmak és szakszavak (melyeket az agytérképek készítése

[18] A modern egyetemi könyvtáraknak érdemes lenne elgondolkodni a technológia felhasználásán.
[19] Pl.: http://www.lap.hu/ vagy http://www.dmoz.org/
[20] Pl.:google.com

során gyűjtöttünk össze) a kutatás ebben a fázisában is hasznosnak bizonyulnak. Javíthatja találataink hatékonyságát, ha a keresőket megfelelő kereső operátorokkal paraméterezzük[21].

A különböző keresőmotorok csak egy részét fedik le a teljes Világhálónak, továbbá eltérő algoritmusok szerint állítják fel a találatok közti sorrendet, így érdekes lehet, ha több keresőt is használunk forráskutatásunk során. Erre a feladatra is létrehoztak néhány keresőt[22], melyek a különböző „nagy" keresők találatait hasonlítják össze. Az internetnek a keresők által nem kategorizált részét mély web-nek (deep web) hívják, ezt csak próbálgatások útján tudjuk felfedezni[23]. Mivel számtalan olyan adatbázis van, melyek tartalma a keresők segítségével nem érhető közvetlenül el, így a mély web-en számos értékes forrás „lapulhat".

Indirekt módszerek

A publikációk bibliográfiáinak, irodalomjegyzékének elemzésével, és egyéb meta információk felhasználásával újabb forrásokra bukkanhatunk.

Például a *Maltego*[24] nevű OSINT[25] programmal a publikációk bibliográfiája alapján újabb, a szakterületen dolgozó kutatók felderítése, vagy a publikációból újabb hivatkozások kigyűjtése válik lehetségessé. Ezek az indirekt módszerek jellemzően csak végső esetben használandóak, hiszen jelentősen több időt és energiát igényelnek.

Feldolgozás

Napjainkban általában nem az a kérdés, hogy találunk-e információt a kérdéses témával kapcsolatban, hanem az, hogy a rengeteg találatot hogyan dolgozzuk fel. Meg kell azt is említeni, hogy az internet elosztott, koordinálatlan rendszere következtében a felhasználandó információforrásokat felül kell vizsgálni, és értékelni kell, hiszen a hitelességre nem garancia pusztán az, hogy megtalálható az interneten.

A források értékelési szempontja lehet a szerzők szakmai relevanciája[26], vagy ha a publikációk felől közelítünk, akkor a folyóiratok szakmai elfogadottsága. Az idő is fontos tényező, hiszen a tudomány fejlődése következtében az évekkel korábbi publikációk vesztenek aktualitásukból, pontosabb eredmények jelennek meg az évek múlásával.

Az internet jellege következtében előfordulhat, hogy már az adott szerverről eltávolították a keresett tartalmat. A közmondást alapul véve (mely szerint amit egyszer elérhetővé tettek az interneten, azt már nem lehet leszedni), lehetőségünk van különböző archivált állományok, adatbázisok[27] között is keresni**.**

Rendszerezés, adattárolás

A kutatásunk során számtalan elektronikus dokumentumot generálunk (saját írásaink, letöltött cikkek, e-könyvek, stb.), hasznos lehet, ha már a kutatás kezdeti fázisában módszeresen rendezzük azokat. Célszerű lehet egy mappastruktúrát felállítani, melyben azonos névkonvenció alapján nevezzük el a fájlokat, a publikációk, vagy a disszertáció fejezeteinek megfelelő mappákba mentjük el azokat. Az időszakosan végzett biztonsági mentések is hasznosak, melyeket célszerű akár több, földrajzilag és eltérő helyen tárolni, eltérő

---

[21] Bing kereső esetén lásd részletesen: http://msdn.microsoft.com/en-us/library/ff795620.aspx, Google Search, Gmail, vagy Google drive esetén:https://support.google.com/vault/answer/2474474?hl=enm,
Yahoo esetén: https://help.yahoo.com/kb/search/advanced-search-sln2194.html?impressions=true

[22] Ezeket metakeresőnek hívjuk, ilyenre példa:us.searchboth.net, www.2lingual.com, zuula.com, yabigo.com, googawho.com keresőalkalmazások

[23] Az alábbi linken néhány mély web kereső elérési útvonala látható http://deep-web.org/how-to-research/deep-web-search-engines/.

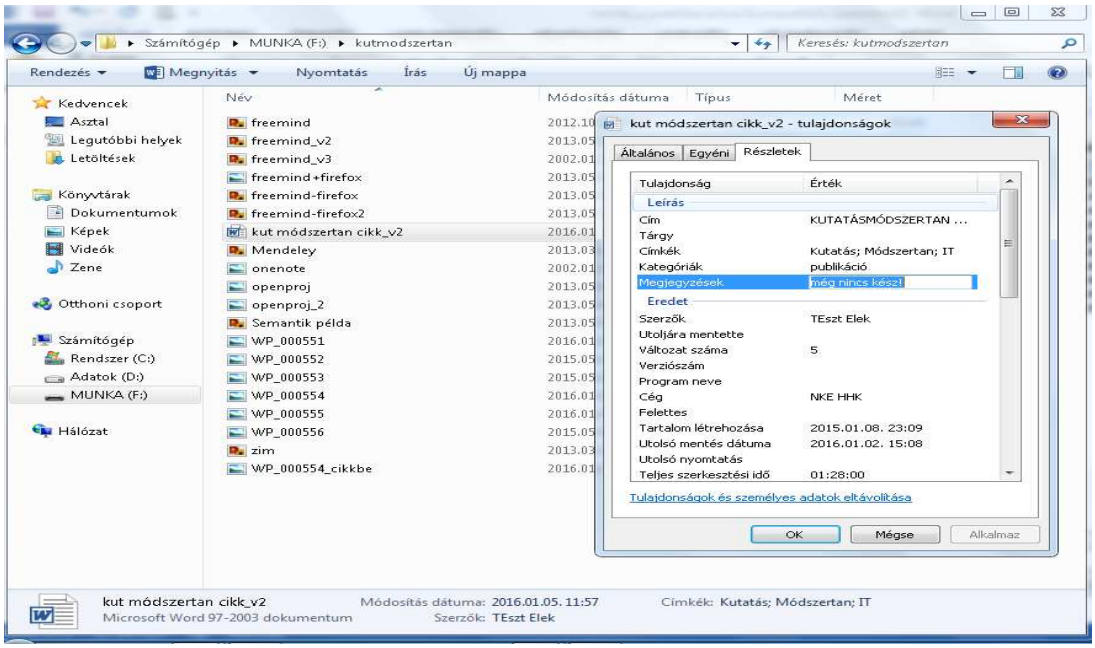
[24] https://www.paterva.com/web6/products/maltego.php

[25] Open Source Intelligence

[26] Az egyes cikkeket, szerzőket a citációs faktor alapján tudjuk megítélni, a folyóiratokat és publikációs gyűjteményeket az impakt faktor alapján (sokszor azonban kutatásunk szempontjából ezek az objektív mérőszámok félrevetőek lehetnek).

[27] Pl.: a google cache-elt rekordjai között, vagy az archive.org tárolt, statikus weblapjai között

adathordozókon (merevlemezen, DVD-n stb.). Az adatok bizalmas tárolását korszerű titkosító eljárásokkal garantálhatjuk (pl.: teljes merevlemez titkosítás az operációs rendszer segítségével, vagy olyan alkalmazással, mint a Windows és Linux rendszereken is egyaránt működő *VeraCrypt* program).



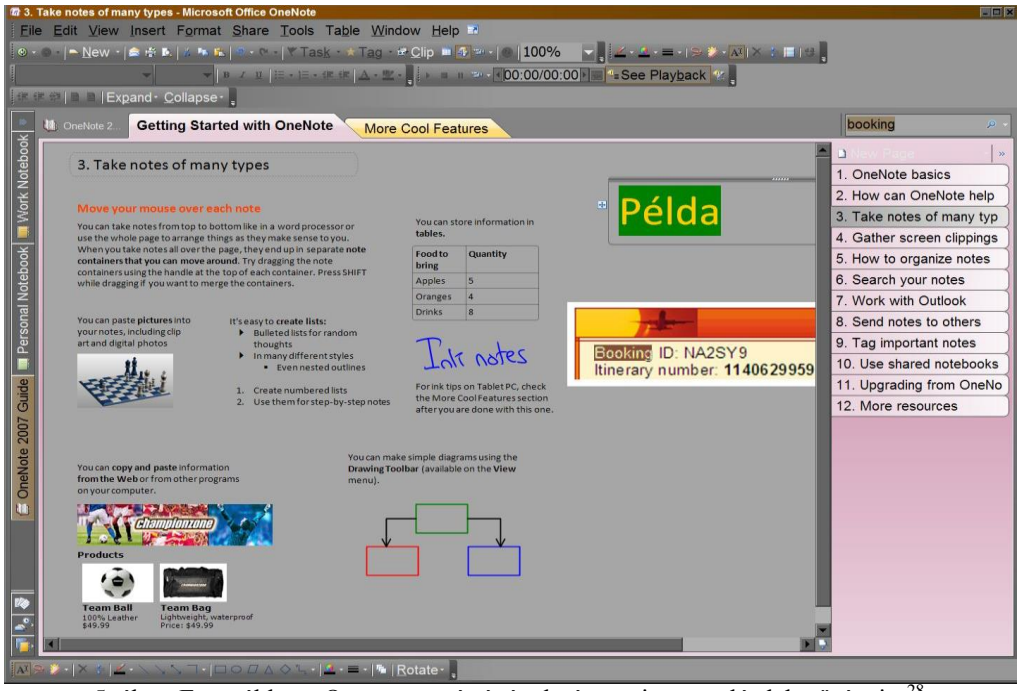
4. ábra. A Windows operációs rendszeren történő meta adat rögzítés egyik lehetősége

Érdemes már a forrásgyűjtés szakaszában metainformációkkal (4. ábra) ellátnunk a lementett dokumentumokat, és relevanciájukat, a feldolgozás sorendjét jelölnünk (piorizálás). Sokszor előfordul, hogy korábbi kutatásaink során gyűjtött forrásainkat is át szeretnénk fésülni az új téma érdekében, vagy konkrétan keresünk egy korábbi anyagot. Ekkor jól jöhet az operációs rendszerek lokális kereső szolgáltatása. A fájlnév, készítő, készítés dátuma sokszor kevésnek bizonyul, és a szöveges tartalom alapján (kulcsszavakkal) szeretnénk keresni (ez a Windows rendszerek esetén az indexelés szolgáltatás beállításainál, a tartalom alapú indexelés engedélyezése esetén fog működni, persze csak a rendszer által támogatott szövegformátumok esetén).

Szövegszerkesztés, Jegyzet készítés

A találatok (weblapok, elektronikus dokumentumok, e-könyvek) feldolgozásában felhasználhatjuk a megszokott irodai szoftvereket (pl.: szövegszerkesztő), azonban vannak olyan alkalmazások, melyek kibővítik az egyszerű szövegszerkesztők funkcionalitását.

Ilyenre példa a *Microsoft Onenote* alkalmazása (5. ábra), mely akár a weben keresztül is elérhető (un. web applikációként). Ennek köszönhetően mobil eszközről bárhonnan elérhetjük jegyzeteinket. Előnyként említhetjük még a más Microsoft termékekkel való kompatibilitást (adat importálása, exportálása a böngésző, prezentációs, szövegszerkesztő, levelező és táblázatkezelő szoftverekből) valamint a kezelt adatok tekintetében a nagyfokú rugalmasságot (webtartalom linkelten, kép, táblázat, video, hangjegyzet, stb. beszúrása).



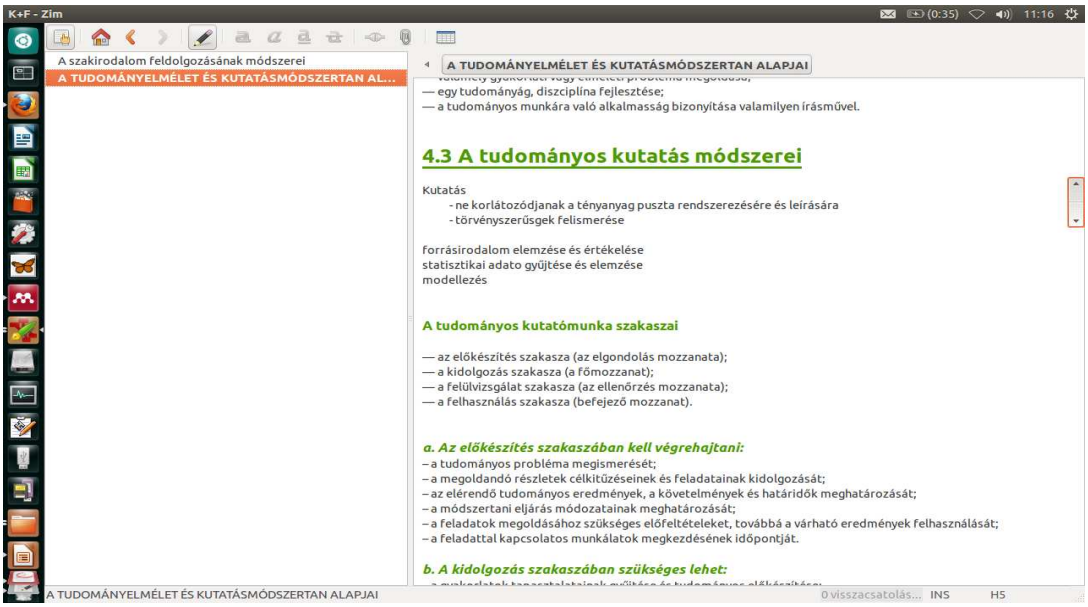
5. ábra. Egy példa az Onenote segítségével végzett jegyzetelés lehetőségeire[28]
(készítette a szerző, felhasználva a programban található mintafájl-t)

Egy másik hasonló, azonban nyílt forráskódú alkalmazásra jó példa a Zim (6. ábra), melyet a következő képen láthatunk[29]. Ennél az alkalmazásnál kartotéka szerűen tudunk összetartozó, logikailag összekapcsolható információkat egy saját wikipédiában tárolni.

Ennek az alkalmazásnak a jól kategorizálható és átlátható jegyzetek készítése mellett további előnye, hogy képes a tartalmat html lappá konvertálni (tehát ezáltal leegyszerűsödik a webes publikáció). A jegyzeteket egyszerű szöveges fájlként tárolja, ezzel kis méretet és könnyű keresést garantál (csoport munka támogatására már adatbázis alapú megoldásban kell közösen „gondolkodni").

[28] Megjegyzés: a „Booking ID" egy képen található szöveg, melyet fejlett szövegfelismerő algoritmusa segítségével ismert fel a szoftver

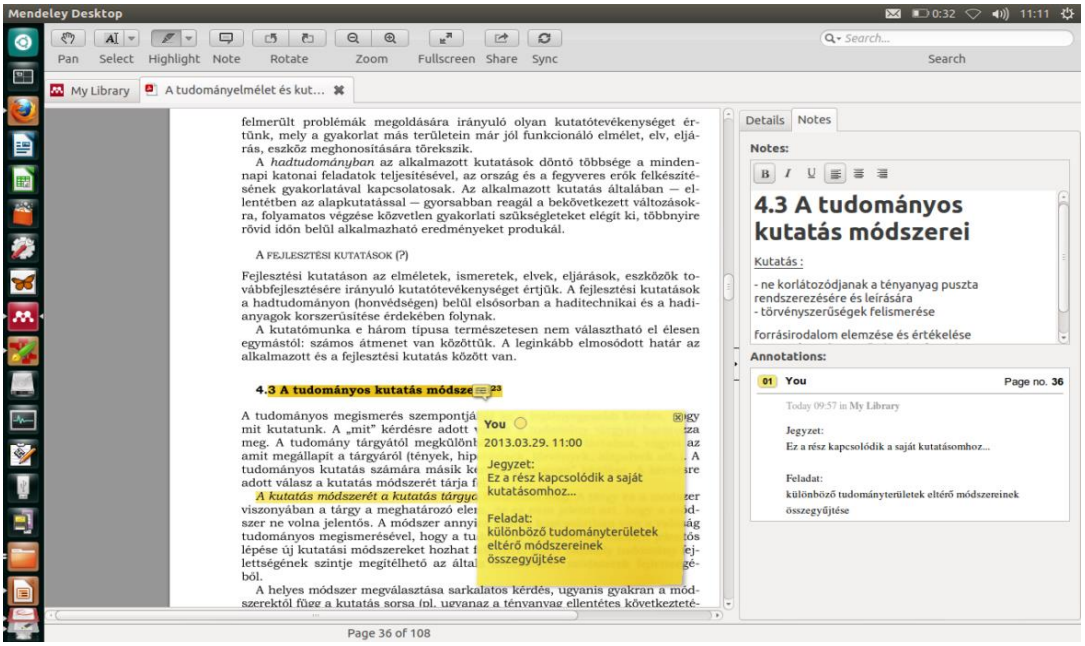
[29] Említhetnénk még a hasonló funkciókkal rendelkező *Keepnote* alkalmazást (mely Windows és Linux platformon is elérhető).



6. ábra. Példa a Zim segítségével készített jegyzetre

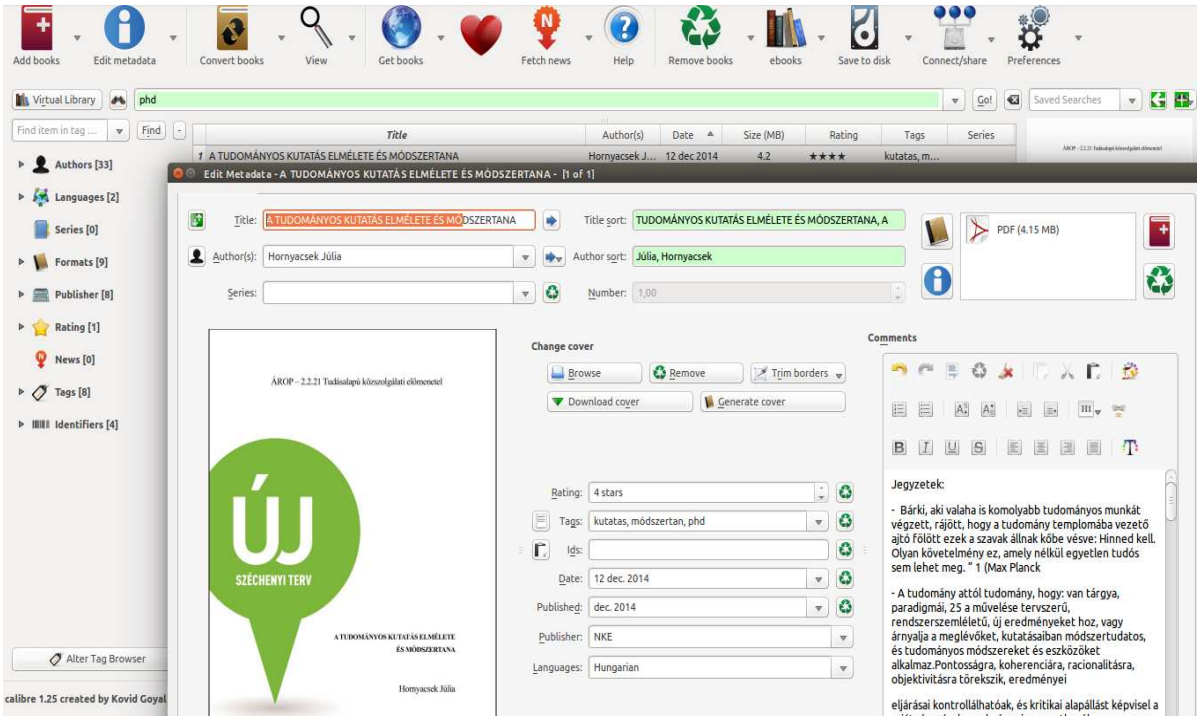
Elektronikus könyvtár alkalmazások

Az elektronikus dokumentumok tematikus tárolására alkalmazható programra jó példa a szintén szabad szoftverként elérhető *Mendeley Desktop (7. ábra)*. Segítségével a források kezelése, kategorizálása és címkézése egyszerűsödik (így későbbi kutatásaink során a saját igényekre szabott elektronikus könyvtár és jegyzet együttesen felhasználható forrásként).



7. ábra. A Mendeley Desktop használat közben

A program segítségével képesek vagyunk „elektronikus szövegkiemelő”-vel megjelölni a releváns részeket, azonban hátránya, hogy azokat nem képes exportálni külső fájlformátumba. Képes könyvtárunkat egy webes tárhellyel szinkronizálni, így csökkentve az adatvesztés valószínűségét és biztosítva a „bárhonnan” elérhető személyes könyvtárat.



8. ábra. A Calibre program felhasználása metaadatok rögzítésére

Az e-könyvek karbantartására és az elektronikus könyvtár katalogizálására szolgál a *Calibre* alkalmazás (8. ábra), mellyel a címkézés és kategorizálás mellett fájlformátum konvertálásra is lehetőségünk van.

Milyen platformot használjak?

Korábban csak a használt operációs rendszer[30], manapság már a használt számítástechnikai eszköz is kérdéses lehet[31]. Napjainkban már a kezelt adatainkhoz akár út közben is hozzáférhetünk mobil eszközeink segítségével. A régebben csak távközlési céllal használt mobiltelefonok mára már teljes értékű számítógépekké váltak, a nagyléptékű technológiai fejlődésnek köszönhetően. Így az asztali PC-k mellett számos más eszköz is segítheti kutatómunkánkat. A felhő alapú társzolgáltatások tovább könnyítik az adatok mobil hozzáférését.

A hordozhatóság, a könnyű kezelés, a számítási-, és tárolási kapacitás alapján tudunk választani. Azonban fontos szempont lehet a kompatibilitást is, hiszen munkánkat úgy tudjuk csak könnyíteni, ha a kezelt, feldolgozott és tárolt adatainkhoz minden eszközünkkel (asztali PC, laptop, okostelefon, e-könyv olvasó, stb.) egyformám hozzá tudunk férni, biztosított az átjárás a különböző fájlformátumok között.

A következő táblázatban összehasonlítottam a felhasználható eszközöket, a szemléletesség érdekében előnyeiket és hátrányaikat négyfokozatú skálán ábrázoltam (ahol a 4 a legmegfelelőbb, és 1 a legkevésbé megfelelő).

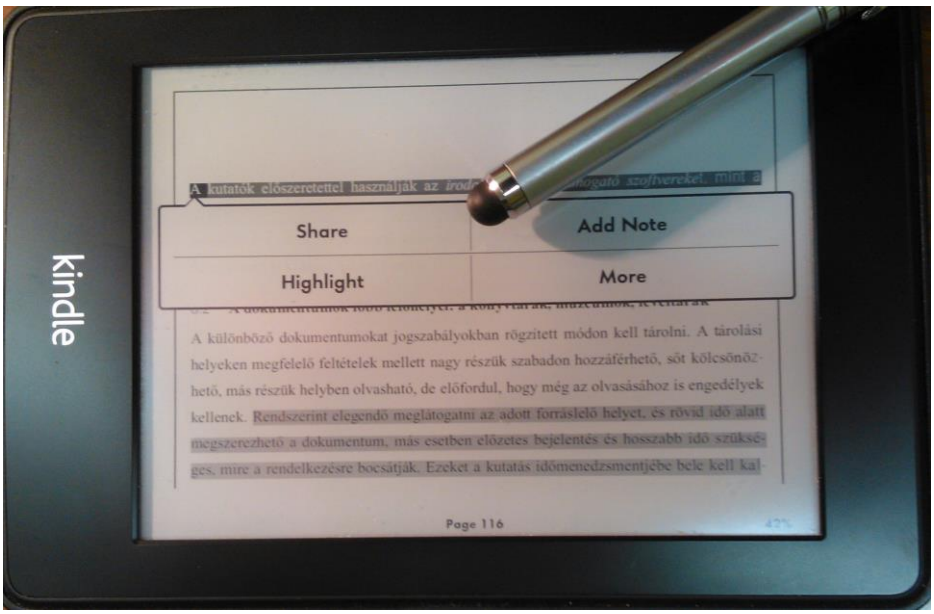
[30] Pl.: Windows, Linux, Mac stb.
[31] Asztali számítógép, laptop, GSM telefon, okostelefon, e-könyv olvasó, stb.

2. táblázat. Platform összehasonlító táblázat

Tulajdonság	Asztali PC	Laptop	Okostelefon	E-könyv olvasó
Számítási- és tárkapacitás	4	3	2	1
Mobilitás	1	2	3	4
Méret	1	2	3	4
Megjelenítés, olvashatóság	4	3	1	2
Kezelhetőség (adatbevitel, és feldolgozhatóság)	4	3	2	1

Ugyan erőforrások, kezelhetőség és megjelenítés szempontjából az asztali PC-k és a laptopok kerülnek ki elsőként az összehasonlításból, sok esetben rajtuk az elektronikus dokumentumok olvasása és jegyzetelése nehézkes.

Az e-könyv olvasók (9. ábra) előtt nagy jövő áll, hiszen reformálni tudják a napjainkig még jellemzően papír alapú publikációk olvasását. Azonban ezen eszközök gyártói jelenleg még csak a szépirodalmi művek és az elektronikus sajtó olvasóit célozzák, az elektronikus szakirodalom feldolgozása nehézkes (a Pdf dokumentumok konvertálása még problémás, főleg a táblázatok és képek tekintetében). Célhardverről lévén szó a számítási és tárkapacitása korlátozott, azonban alapfunkciójának tökéletesen megfelel, valamint az eszköz tárkapacitása a web alapú adattárak segítségével szinte a végtelenségig növelhető (megjegyzem, hogy a hétköznapi felhasználás esetén nem jellemző, hogy több tízezer könyvre van egy időben szükségünk egy eszközön).



9. ábra. E-könyv olvasó jegyzetelés közben

EGYÜTTMŰKÖDÉS

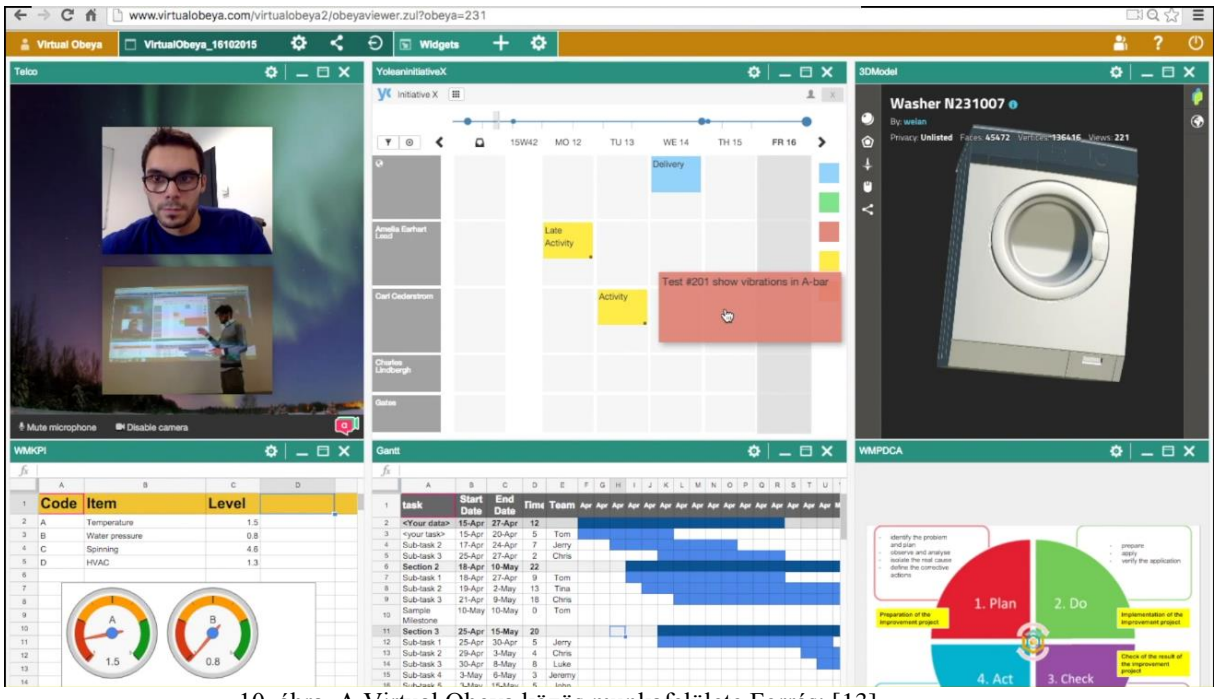
„Én távolabbra láthattam, de csak azért, mert óriások vállán álltam”

Sir Isaac Newton

Az ember társas lény, az elődeink által kitaposott ösvényen, társaink segítségével, velük közösen juthatunk csak előrébb. Az együttműködésnek számtalan előnye lehet [12]:

- költséghatékonyság (erőforrások, laborok, mérőeszközök megosztása),
- feladatmegosztás (időtényező, tudás, képességek miatt),
- több szemlélet, több nézőpont, több ötlet.

Érdekes kérdés azonban a közös munka, főleg egy kreativitáson és szakértelmen alapuló kutatás összehangolása. Induljunk ki abból, hogy a kommunikáció célja az emberi agyban kialakult fogalmak és gondolatok közlése egy, ehhez a fogalomhoz társított szimbólum (pl.: a nyelv) segítségével, egy közös médiumon keresztül (lehet írott és szóbeli, vagy akár multimédiás is). Minél hatékonyabb kommunikációs eszközt választunk, annál könnyebb lesz a közölni kívánt gondolatokat összehangolni, és közösen gondolkodni. A csoportkommunikációhoz használt eszköz a mi általunk valamilyen szempontból hatékonynak ítélt módszer (pl.: beszéd alapú kommunikációra VoIP szolgáltatás[32], dokumentumok közös szerkesztésére és tárolására felhő alapú adattár[33]), vagy azok kombinációja lesz (pl.: azonnali üzenetküldő alkalmazás és közös dokumentumtár egyidejű alkalmazása).



10. ábra. A Virtual Obeya közös munkafelülete Forrás: [13]

[32] Pl.: Skype, Webex stb.

[33] Pl.: Dropbox, Onedrive, Ubuntu drive, Google drive, Amazon cloud drive tárhelyek

A kommunikáció mellett a tervezés és szervezés is fontos felhasználási terület, egy jó szervezési modell az un. Obeya[34] (ez a párhuzamos munka modellje, mely során a folyamatban – pl.: kutatás, gyártás stb. - résztvevő összes személy egy „nagy teremben" dolgozik, hogy egyszerűsítsék és felgyorsítsák a kommunikációt). A web adta lehetőségek révén már „virtuális Obeya" platformon is dolgozhatunk, együttműködve akár más földrészeken tevékenykedő kutatótársainkkal [14] Ez a szolgáltatás többet ad, mint egy egyszerű kommunikációs felület (pl.:*Skype*), hiszem itt a dokumentumokat is meg tudjuk osztani, közös ütemtervet, naptárat tudunk használni a velünk egy projekten dolgozókkal.

Elgondolkodtató még a web 2.0 termékeként kialakult önszervező közösségi hálózatoknak[35] a kutatókra és a kutatásokra gyakorolt hatása is, hiszen ezek minden eddiginél komplexebb, sok résztvevős kutatásokat alapozhatnak meg. Az egy kutatási területben kutatók így követhetik társaik aktuális kutatási témáit, az adott területen elért áttöréseket.

PUBLIKÁCIÓS LEHETŐSÉGEK

A tudomány fejlődésének egyik alappillére a publicitás: hiszen a tudományos felfedezések eredményei, a felhasznált módszerek csak akkor fogadhatóak el, ha azokat független, külső szakemberek által is elismertek.

A gyártó-fogyasztó koncepció a web jövője, mely annyit tesz, hogy a statikus tartalom (web 1.0) mellett mi, a „felhasználók" is generálunk már tartalmat (web 2.0). Egyszerűsödik a publikáció, és gyorsul a megjelenés (korábban egy-egy mértékadó folyóirat, szaklap hónapokon keresztül visszatartotta a publikációkat lektorálás, terjedelmi, és egyéb feldolgozási okok miatt). A lektorálás, a tartalom feltöltése (megjelenítése a weblapon), és a hibás tartalom korrigálása is egyszerűsödik a weben publikálás esetén (a probléma, hogy kevesen lektoráltatják tartalmukat, vagy változtatnak a jogos kritikák alapján).

Számos online folyóirat, konferencia kiadvány a kiadott formai követelményeknek betartását automatikusan ellenőrzi[36] a beadott publikációkon, a lektoroknak így csak a tartalomra kell koncentrálniuk (ezzel is könnyítve, és gyorsítva a publikálást).

Az Amazon cégnek pedig forradalmi ötlete támadt: bárki publikálhat a webes könyvpiacán (az író, az eladások alapján százalékosan részesül)[37]. A különböző online folyóiratok, publikációs gyűjteményekre pedig jó példa a *Google Scholar* projekt[38], mely egyrészt saját feltöltéseket, másrészt külső adatbázisok tartalmát integrálja egy tudományos keresőbe.

ÖSSZEGZÉS

Hogyan kutassunk módszeresen? Ezzel a kérdéssel korábbi munkáim során szembesültem. Saját kutatásaim miatt kezdtem foglalkozni a kérdéssel, és alapvetően csak a web használata során jelentkező források és ötletek halmazát akartam egy könnyen átlátható rendszerbe foglalni. Azonban rájöttem, hogy a web evolúciója reformálta a tudományos kutatás módszertanát és eszközeit, így ennél jóval többet tud számomra - és ennek a cikknek elolvasása után remélhetően kutatótársaimnak is - nyújtani.

---

[34] Bővebben az Obeya módszerről: http://www.leancenter.hu/lean-menedzsment/projekt-program-es-transzformacios-lean-menedzsment-az-obeya.html, egy alkalmazásra példa: http://www.rapidiobeya.co.uk/overview

[35] A Google groups, Facebook, Twitter, Linkedin stb. szociális hálózatokon szervezett kutató projektek, vagy a kifejezetten kutatóknak szánt Researchgate, academia.edu és a Mendeley weboldalak.

[36] Ilyenre példa: https://www.ieee.org/conferences_events/conferences/publishing/pdfexpress.html és a https://www.ieee.org/publications_standards/publications/authors/pdf_checker.html

[37] Részletei: https://authorcentral.amazon.com/gp/help?ie=UTF8&topicID=200650270

[38] Lásd: scholar.google.hu

Érdekes volt felismerni azt, hogy már nemcsak a csoportos, hanem az egyéni kutatások során alkalmazható eszközök is a web technológiára alapulnak (képesek szinkronizálni webes adattár szolgáltatásokkal[39], megosztani jegyzeteinket, megjegyzéseinket közösségi hálózatokkal[40,] HTML formátumban menteni jegyzeteinket, könnyítve a weblapokra, blogokra való feltöltést[41] stb.).

Publikációmban a technológiák műszaki hátterével nem foglalkoztam, csak az általuk biztosított szolgáltatásoknak és új képességeknek a tudományos kutatásra kifejlett hatásait, továbbá az általuk nyújtott új lehetőségeket mutattam be.

Számtalan informatikai alkalmazás, eszköz és online szolgáltatás áll rendelkezésünkre a kutatás hatékonyságának javítására, vagy a folyamat felgyorsítására. Azonban ha ezeket a kellő ismeretek hiányába (mi-mire jó, mi az előnye vagy épp hátránya), nem módszeresen alkalmazzuk, akkor a kívánt hatással épp ellentétes váltunk ki, csak növeljük a kutatás sikeres végrehajtásához szükséges erőforrásokat (eszköz, pénz, munkaóra).

Ezért határoztam el, hogy bemutatom, és egyben rendszerezem a napjainkban használható technikákat és módszereket. Elsősorban mindezt a saját kutatásaimon keresztül, azonban igyekeztem olyan példákat hozni, melyek más tudományterületek kutatóinak is ötletet adhatnak.

A témához kapcsolódó írásaiban Dr. Németh András [15], [16] felhívta a figyelmet arra, hogy:”*A hallgatói létszám csökkenésével a lineáris képzésre való áttéréssel az elmúlt évtizedben jelentősen csökkent a tudományos utánpótlás bázisa, ami már középtávon is komoly problémát jelenthet a hadtudományok területén*”[42]. Ennek a problémának az egyik kezelési módja, hogy tudatosabban, célzottabban, szervezetten végezzük a hadtudományi kutatásokat. Jelen cikkemben bemutattam néhány olyan módszert, mellyel ezeket biztosítani tudjuk.

Kutatásaink során szem előtt kell tartani, hogy az innovatív technológiák csupán eszközök, mely segítenek minket problémáink megoldásában, és sosem maguk a megoldások. Ezek alapján úgy vélem a korábban felsorolt eszközök önmagukban nem változtatnak a kutatásokon, azonban ha azt kreatív és megújuló elmék használják, akkor valóban képesek lesznek fokozni produktivitásunkat.

[39] Pl.:Mendeley Desktop alkalmazás (7. ábra)
[40] Pl.:Kindle e-könyvolvasó (9. ábra)
[41] Pl.:Zim alkalmazás (6. ábra)
[42] Németh András - A tehetséggondozás és tudományos utánpótlás-nevelés múltja, jelene és jövője a hadtudományok területén, különös tekintettel a tudományos diákköri mozgalom szerepére II. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 25:(E-szám) p. 309

Felhasznált irodalom

[1] Alejandro Saucedo, Web 3.0 - The Internet of Things! (Videoanyag) Forrás: https://www.youtube.com/watch?v=F_nbUizGeEY, 2015.12.10

[2] Favaro, Sharon, Lisa Rose-Wiles and Darren Sweeper, Rethinking research guides: bringing the library to the user, National Széchényi Library of Hungary, 2009 Forrás: http://www.ki.oszk.hu/3k/news.php, 2015.12.10

[3] Matt Iannucci, Peter MacLeod - Meet Toronto's Hidden Experts, Joseph L. Rotman School of Management University of Toronto,Martin Prosperity Institute; Forrás: http://martinprosperity.org/media/Big%20Ideas_Hidden%20Experts_14-05-28.pdf, 2015.12.10

[4] Lengyelné Molnár Tünde - Kutatástervezés, Eger, 2013 http://mek.oszk.hu/14400/14492/pdf/14492.pdf

[5] Bodonyi Ilona, A rendészettudomány kutatás-módszertana, Budapest, 2008 (Jegyzet) Forrás: http://rtk.uni-nke.hu/uploads/media_items/a-rendeszettudomany-kutatas-modszertana.original.pdf 2015.12.10

[6] Dr. Hornyacsek Júlia, A tudományos kutatás elmélete és módszertana, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Budapest, 2014, ISBN: 978-615-5491-36-8; Forrás: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9973/Teljes%20sz%C3%B6veg!?sequence=1&isAllowed=y 2015.12.10

[7] Dr. Gőcze István, A tudományelmélet és kutatásmódszertan alapjai, ZMNE, Elektronikus Tanulmány, Budapest, 2010
Forrás: http://www.lib.pte.hu/csomag/FEEK/MA-Lev/01felev/Kocsis_M-Tudomanyelmelet/GOCZETUDELM_KUTMODSZT_TANULMANY.PDF
2015.12.10

[8] Dr. Majoros Pál, A kutatásmódszertan alapjai, 2004, ISBN 963 394 584 4

[9] Csermely Péter, Gergely Pál, Koltay Tibor és Tóth János, Kutatás és közlés a természettudományokban, Osiris kiadó, 1999. ISBN: 9789633795286 http://www.linkgroup.hu/docs/Kutatas-kozles-termtud.pdf 2016.01.18

[10] Csatai Rózsa - NYME MÉK Kutatásmódszertan I., elméleti ismeretek a társadalomtudományi kutatásokhoz (segédlet), Mosonmagyaróvár, 2012.; Forrás: www.mtk.nyme.hu/fileadmin/user_upload/gazdasag/Letoeltesek/CSRKUTMODjegyzet2012.doc 2015.12.10

[11] Amazon, Lend or Borrow Kindle Books Forrás: Forrás: http://www.amazon.com/gp/help/customer/display.html/ref=hp_rel_topic?ie=UTF8&nodeId=200549320, 2015.12.10

[12] Don Tapscott, Anthony D. Williams Wikinómai, Hogyan változtat meg mindent a tömeges együttműködés, ISBN 978-963-9686-22-9, 2006, p. 178

[13] Virtual Obeya Demonstrációs video anyag https://www.youtube.com/watch?v=Z6814WqigNA 2016.09.24.

[14] Terenghi, F., Kristensen, K. ; Cassina, J. ; Terzi, S. - Virtual obeya: A new collaborative web application for running lean management workshops
Forrás:
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6871554&abstractAccess=no&userType=inst, 2015.12.10

[15] Németh András - A tehetséggondozás és tudományos utánpótlás-nevelés múltja, jelene és jövője a hadtudományok területén, különös tekintettel a tudományos diákköri mozgalom szerepére I. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 25:(E-szám) pp. 296-308. (2015)(Magyar Hadtudományi Társaság);
http://mhtt.eu/hadtudomany/2015/2015_elektronikus/25_NEMETH_ANDRAS.pdf
2016.02.21

[16] Németh András - A tehetséggondozás és tudományos utánpótlás-nevelés múltja, jelene és jövője a hadtudományok területén, különös tekintettel a tudományos diákköri mozgalom szerepére II. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 25:(E-szám) pp. 309-322. (2015)(Magyar Hadtudományi Társaság);
http://mhtt.eu/hadtudomany/2015/2015_elektronikus/26_NEMETH_ANDRAS_2.pdf
2016.02.21

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Szádeczky Tamás
szadeczky.tamas@uni-nke.hu

KRIPTOGRÁFIAI PROTOKOLLOK MEGFELELŐSÉGE

Absztrakt

Az informatikában a biztonságos kommunikációt kriptográfiai algoritmusokkal és rájuk épülő protokollokkal tudjuk megvalósítani. Ahogy az elmúlt két évben kiderült, a biztonsági szoftverek – hasonlóan minden más PC alkalmazáshoz – tartalmaznak szoftverhibákat. A cikk a hibák kezelésének műszaki és üzleti oldalát elemzi, a szabványalkotó, a jogalkalmazó és az üzleti gyakorlat szempontjából, így különös tekintettel a kriptográfiai protokollok elavulásának a szabványalkotó általi kezelésére. 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.

Secure IT-based communication is achievable with the application of cryptographic algorithms and protocols. As it became clear in the last two years, security software, similarly to any other PC software, contains bugs. The article analyses the technical and business sides of treating those bugs from the aspects of the standardizing body, the regulating authority and the business practice. The focus is the treatment of the aging of cryptographic protocols by standardization bodies.

Kulcsszavak: *kriptográfia, SSL, TLS, PCI DSS, Java, böngésző, szabvány-megfelelőség ~ cryptography, SSL, TLS, PCI DSS, Java, browser, standard compliance*

BEVEZETÉS

A 2000-es évek óta megnövekedett a nyomás a szoftverfejlesztőkön, hogy a termék minél előbb a piacra kerülhessen, így az üzleti igény kielégítésre kerüljön. Ez nyilván rövidebb fejlesztési időt és sajnos kevesebb tesztelést jelent. Ezt az üzleti hozzáállásbeli változást lekövette a fejlesztési módszertan is és a korábbi vízesés modellt felváltotta az agilis szoftverfejlesztés. [1] Ez azt jelenti, hogy szemben a korábbi specifikáció – fejlesztés – tesztelés folyamattal, maga a specifikáció sem készül el a munka megkezdése előtt, hanem az is folyamatosan változik az üzleti igényeknek megfelelően. Ehhez átalakult a tesztelés módszertana is, de sajnos az nem megfelelően hatékony a hibák kiszűrésére. Ebből kifolyólag a fejlesztett szoftverek túlnyomó többsége hibákat hordoz magában, amelyek a felhasználó számára jobb esetben csak a nagyszámú rendszeres frissítés megjelenésével válik láthatóvá. Az informatika felhasználójaként természetessé vált, hogy például havi rendszerességgel kapunk operációs rendszerünkhöz és felhasználói szoftvereinkhez kritikus biztonsági frissítéseket. Súlyosabb esetben ez oda is vezet, – mint az Adobe Flash Player esetében – hogy egyes szoftver beszállítók letiltják ezen túlzottan sérülékeny szoftverek alkalmazását. [2] Ezekhez a problémákhoz sajnálatosan hozzászoktunk, de alapjaiban rengeti meg az információbiztonsági szakmát, ha pont a sérülékenységekből fakadó kockázatok minimalizálásra létrehozott biztonsági szoftverekben találnak kritikus sérülékenységeket.

A TECHNIKAI PROBLÉMA

A 2014-es év több ilyen kritikus sérülékenységet hozott és azóta is több probléma került napvilágra. 2014 áprilisában került nyilvánosságra a HeartBleed bug, amely az OpenSSL kriptográfiai függvénykönyvtárában lévő hiba, ami harmadik fél részére lehetőséget biztosít a RAM-ban tárolt adatokhoz való hozzáféréshez, így akár a felhasznált kriptográfiai kulcsokhoz, jelszavakhoz. [3] Így a kommunikáció titkosítására használt program nyitva hagyta a támadók előtt az egyébként elvileg megfelelő titkosítási algoritmussal kommunikáló felek rendszereit. Ezzel, mint kiderült, egy lavina indult el és újabb és újabb sérülékenységekre derül fény. Ez a helyzet technikai oldalról egyértelműen kezelhető, az adott szoftverkomponenst újabb, javított verzióra kell frissíteni, vagy ahogy a Linux rendszereknél jellemző, a korábbi verziót javítják és a teljes alkalmazás frissítése nélkül az adott hiba orvoslásra kerül (backporting). Nem olyan egyszerű viszont a kérdés a biztonsági megfelelőség (compliance) illetve az üzleti követelmények szempontjából.

A fentiekhez hasonló problémakör a kriptográfiai algoritmusok és protokollok elavulása. Minden jelenleg alkalmazott negyedik generációs titkosítás tökéletlen (kivéve a szervezési okokból hatékonyan nem használható One Time Pad algoritmust), tehát feltörhető, viszont ez jó esetben időben lehetetlen feladat. Megfelelő algoritmusnak tekintjük például azt, ami a Föld összes számítógépének együttes számítási kapacitásával évezredek-évmilliók alatt törhető fel. Ezek a nagy számok kifejezetten hangzatosak, de valójában – a számítási kapacitás Moore-törvény szerinti növekedése és kódtörési feladatok többezer magos grafikai processzorokra való áthelyezése miatt – már az eredmény, hogyha évtizedekig megfelelő védelmet nyújt az adott algoritmus az adatainknak. Így folyamatosan avulnak el a régebben biztonságosnak tekintett algoritmusok, mint ahogyan az a DES és az RC4 szimmetrikus algoritmusokkal történt. A probléma megoldása mindössze annyi, hogy a korábbi algoritmusokat a kor színvonalának megfelelő jobb algoritmussal helyettesítjük, az adatokat újrakódoljuk. Külön kihívást jelent a speciális célú kriptográfiai algoritmusok – mint a katonai szenzorhálózatokban alkalmazott MINISEC algoritmus – jóságának megítélése, hiszen ezek alkalmazása csak nagyon szűk területen történik, így az azt tesztelő hackerek is kevesen vannak. [4] Mindemellett a védelmi rendszer kialakításakor figyelembe kell venni, hogy a

kriptográfiai eljárások kijátszhatóak a rejtjelezés előtt történő kompromittálással, például a billentyűzet közvetlen rádiófrekvenciás lehallgatásával. [5] Hasonló a probléma a lenyomatképző (hash) függvények esetében is, ahol a képzett lenyomat elveszíti az egyediségét. A lenyomatképző függvények alkalmazásának célja az, hogy egy tetszőleges hosszúságú bemenet egy állandó hosszúságú kimenetre (például 128-256 bitre) kerül leképzésre. Magától értetődő, hogy minden tetszőleges hosszúságú bemenetet nem lehet párszáz biten ábrázolni úgy, hogy minden hash érték egyedi legyen. Szükségszerűen lennie kell ütközésnek, tehát két különböző bemenet egyszer csak ugyanazt a kimenetet fogja produkálni. Egy lenyomatképző algoritmust addig tekintünk megfelelőnek, amíg nem találnak valamilyen ütközést. [6] Ez történt az MD4, MD5 és az SHA-1 algoritmusok esetében is. A megoldás itt is az algoritmus leváltása.

Technikai szempontból tehát a megoldás az alkalmazott kriptográfiai algoritmusok és az azt alkalmazó protokollok avulásának és sérülékenységeinek nyomon követése és szükség esetén azok leváltása egy korszerű megoldásra. Maga a leváltás a tárolt adatok esetében azok dekódolását, majd az új megoldás szerinti rejtjelzését jelenti. Adatátvitel esetében pedig mindössze az alkalmazott kriptográfiai algoritmust, illetve protokollt kell lecserélni.

AZ ÜZLETI PROBLÉMA

Ami technikai szempontból egy „egyszerű” frissítéssel, vagy cserével megoldható lenne, az az üzleti valóságban sajnos nehezen kivitelezhető. A szabályozó, normaalkotó szervek jobb esetben előremutatóan megkövetelik a gyenge kriptográfia cseréjét, majd az érdekelt felek kérésére gyakran kénytelenek meghosszabbítani a határidőket, mint ahogy azt a Payment Card Industry Security Standards Council (PCI SSC) is tette. A bankkártyás fizetések biztonságát a Visa Inc., MasterCard, American Express, Discover Financial Services, és JCB International által alapított PCI SSC több, általa kiadott szabványban határozza meg. Ezek közül a legszélesebb körben ismert és alkalmazott Payment Card Industry Data Security Standard (PCI DSS) szabvány határozza meg a bankkártya elfogadók által alkalmazandó biztonsági szabályokat. Ennek alkalmazása minden bankkártyás fizetést elfogadó és az annak lebonyolításában résztvevő szervezet számára kötelező. A szabvány – szemben más információbiztonsági szabványokkal, mint az ISO 27001 – egy bizonyos részterületre koncentrálva különösen részletes technikai szabályokat határoz meg. Az egyik ilyen szabálycsoport a bankkártya adatok nyilvános hálózatokon való átküldésének szabályait rögzíti. A 4.1. pontban meghatározottak szerint csak megfelelő kriptográfiai algoritmussal és azt alkalmazó protokollal szabad bankkártya-adatokat nyilvános hálózatokon átküldeni. A 2013 novemberében kiadott 3.0 szabványban az SSL és TLS protokollok még jó példaként szerepeltek. A 2015 áprilisában megjelent 3.1-es verzióban éppen a fent leírt OpenSSL sérülékenységek miatt már az SSL és a korai TLS protokollokat nem tekintik biztonságosnak és az új alkalmazások esetében nem is használhatóak. Annak ellenére, hogy a PCI DSS szerint csak a szabványnak leírtak tekinthetők normatív leírásnak a PCI SSC a szabvány átírásának mellőzésével több dokumentumot is kibocsátott, amelyek az átállás időpontját és módját határozzák meg. [7] Mindemellett viszont sehol nem definiálják a korai TLS verzió fogalmát, kételyek közt hagyva az azt alkalmazó szakembert. Amerikai szervezet lévén a PCI SSC elsősorban a National Institute of Standards and Technology (NIST) szabványaira hivatkozik. Az NIST SP 800-52 Rev.1-ben részletesen foglalkoznak a TLS protokoll különböző verzióinak biztonságos paraméter beállításaival, így ebből kiderül, hogy a TLS 1.0 egyáltalán nem tekinthető biztonságosnak, a TLS 1.1 megfelelő paraméterezéssel biztonságosnak tekinthető és a TLS 1.2 jelenleg feltétel nélkül biztonságos. A TLS 1.1 esetében le kell tiltani a már nem biztonságos kriptográfiai algoritmusok alkalmazását, valamint ki kell kapcsolni a visszafele kompatibilitást engedélyező paramétereket. Annak ellenére, hogy az átállás végső

határidejére a PCI SSC a 2016. június 30-at irányozta elő, szembesülnie kellett azzal, hogy egyre növekvő ellenállásba ütközik az alkalmazói oldalról. [7] Az a probléma ugyanis, – amit a szerző maga is, egy webportál biztonsági konfigurálásakor is tapasztalt – hogy egyes, széles körben elterjedt alkalmazások a TLS 1.2 bevezetése után nyolc évvel még mindig nem támogatják azt. A probléma tehát nem az, hogy az üzemeltető ne tudna frissíteni egy függvénykönyvtárat, vagy telepíteni egy új alkalmazást, hanem jelentős beruházást igénylő új fejlesztések, adatmigrálások és szerkezeti átalakítások válhatnak szükségessé. A pénzügyi világ alapvetően törekszik a biztonságos megoldások alkalmazására, viszont előtérben mégiscsak a fizetések lebonyolítása, a tranzakciók lefuttatása áll. Nem engedhető meg a rendszerek kiesése és minden fejlesztés elég komoly tesztelésen kell, hogy túlessen. Megértve az üzleti oldal nehézségeit a PCI SSC az átállás határidejét 2018. június 30-ra tolta ki, de hogy megakadályozza az alkalmazói oldal esetleges passzív, elodázó hozzáállását, rendszeres kockázatértékelési és jelentési kötelezettséget írt elő a meghosszabbított határidő mellé.[1] Így tehát az átállást elodázó alkalmazók megnövekedett adminisztratív terhekkel néznek szembe és minden auditon magyarázkodásra szorulnak. Különleges helyzetben vannak a kártyával történő fizetést biztosító POS terminálok. Itt is széles körben alkalmazott az SSL és TLS protokollok teljes köre, viszont mivel itt – honlapok, webalkalmazások és háttéradatbázisok híján – a sérülékenységek kisebb valószínűséggel használhatók ki, ezért a szabályok is megengedőbbek. Tekintettel arra, hogy az OpenSSL eddig ismert sérülékenységei csak webalkalmazások esetén használható ki, a POS terminálok ennek hiányában eddig nem veszélyeztetettek.

Ebben az esetben is szükséges viszont a rendszeres kockázatértékelés elvégzése, amelynek keretében a gyártó vagy üzemeltető felméri, hogy valóban nem áll-e fent a POS terminál veszélyeztetettsége. Ebben az esetben a szabványalkotó nem is írt elő átállási határidőt. Fontos viszont, hogy mindez csak a jelenlegi kockázati környezetre és az eddig ismert sérülékenységekre igaz, így mindig követni kell az aktuális iparági riasztásokat, sérülékenységi listákat.

GYAKORLAT ÉS KITEKINTÉS

A szerző egy multinacionális cég megbízásából több nyugat európai szolgáltató és kereskedő PCI DSS auditját is elvégezte. A 2016-ban végzett auditok jelentős hányadánál már az átállás a TLS 1.2-re megtörtént, a PCI SSC által eredetileg kitűzött határidőre. Jellemzően problémás viszont a szerveroldali Java alkalmazásokat futtató webszolgáltatások átalakítása, ugyanis a Java csak a Java Development Kit (JDK) 7 verziótól kezdődően támogatja a TLS 1.2 alkalmazását és a JDK 8 használja azt alapértelmezetten. [8]

1. táblázat: Java Development Kit SSL/TLS titkosítási protokoll-támogatása [8]

Verzió	**JDK 6**	**JDK 7**	**JDK 8**
Megjelenés	2006	2011	2014
Alapértelmezett protokoll	TLS 1.0	TLS 1.0	TLS 1.2
Támogatott protokollok	TLS 1.1 (csak JDK 6 update 111 és újabb) TLS 1.0 SSL 3.0	TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.0	TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.0

[1] lásd PCI DSS 3.2 Appendix A2

A legfontosabb PC böngészők piacán a helyzet hasonló, itt a 2006 áprilisában megjelent TLS 1.1-et és a 2008 augusztusában megjelent TLS 1.2-t a böngészők 7 évvel később kezdték teljes körűen támogatni. Ami nehezen érthető, hogy mind a Firefox-ban, mind az Internet Explorer-ben ezek alapértelmezetten ki voltak kapcsolva, így a felhasználók csak a részletes technikai beállítások megváltoztatásakor tudhatták volna használni azt. Jelentős különbség a JDE és a böngészők között, hogy amíg a böngészők gyakorlatilag automatikusan frissülnek, a fejlesztési keretrendszerek közötti váltásra migrációs folyamatot kell végrehajtani. Tehát amíg elavult Chrome és Firefox böngésző gyakorlatilag elenyésző számban, elavult Internet Explorer a régi Windows-verziókon van, addig Java 6-ot futtató szerverek még nagy számban vannak, attól függetlenül is, hogy a támogatása már a Java 7-esnek is véget ért.

2. táblázat: Asztali böngészők SSL/TLS titkosítási protokoll-támogatása [11] [12] [13]

Állapot	**Chrome**		**Firefox**		**Internet Explorer/Edge**	
	ver	év	ver	év	ver	év
TLS 1.0 támogatás	1	2008.12	1.0	2004.11	4 (letiltva) 7	1997.09 2006.10
TLS 1.1 támogatás	22	2012.09	23 (letiltva) 27	2013.08. 2014.02	8 (letiltva) 11	2009.03 2013.10
TLS 1.2 támogatás	30	2013.09	24 (letiltva) 27	2013.09 2014.02	8 (letiltva) 11	2009.03 2013.10
SSL 3.0 letiltva	40	2015.01	34	2014.12	IE 11 (security update 3038314)	2015.04
Aktuális verzió	52	2016.07	48	2016.08	IE 11 Edge 14	2013.10 2016.08

Emellett meglepően nagy számban tapasztalható a POS terminálok elavult verzióval való csatlakozása. Így akár egy több tízezres POS terminál hálózat is SSL 3.0-val kapcsolódik az elfogadó bankhoz. Itt a legnagyobb problémát a kiterjedt helyszíni szoftverfrissítés szükségessége vagy akár a teljes hardver csere jelenti. Ez egy fizetési szolgáltató (payment service provider) esetében akár milliárdos költséget is jelenthet a teljes infrastruktúra tekintetében. Itt tehát nagyon lassú változásra kell számítanunk. Maga a szabványalkotó sem merte feltenni a kérdést, hogy mi történik akkor, ha a POS terminálokat is érintő SSL/TLS sérülékenység kerül napvilágra.

Szemben a PCI DSS-ben meghatározott, viszonylag részletes követelményekkel és határidőkkel más normákban nem találunk ilyen előírást. A méltán népszerű és széles körben alkalmazott ISO27001 mindössze azt írja elő, hogy az alkalmazott kriptográfiai kontrollokról szabályzatot kell alkotni, szabályozni kell a kulcsok használatát, védelmét és az életciklusát, de konkrét algoritmust nem említ meg, így az esetleges átállást is az alkalmazóra bízza. Áttételesen tehát, de a kockázatértékelés és elemzés keretében írja elő az elavult algoritmusok kockázatának kezelését.

A hatósági gyakorlatban szintén kevéssé jellemző a fenti problémakör kezelése, de üdítő kivételként meg kell említeni a Nemzeti Média és Hírközlési Hatóság elektronikus aláírásokra vonatkozó határozatait, amelynek keretében például az EF/26838-x/2011 sz. határozatokkal kötelezővé tette a hitelesítés-szolgáltatók átállását az SHA-256 lenyomatképző algoritmusra. [9] Ezzel lekövetve az European Telecommunications Standards Institute (ETSI), a távközlés területén működő regionális szabványügyi testület vonatkozó ajánlását és meghonosítva a jó nemzetközi gyakorlatot hazánkban is. [10]

ÖSSZEGZÉS

Összefoglalásként elmondható, hogy a kriptográfiai algoritmusok és protokollok sérüléseiből illetve elavulásából adódó átállási feladatokat – amelyek egyébként minden informatikai üzemeltetőre és alkalmazóra feladatot rónak – a szabványalkotók és hatóságok mindössze kis hányada kezeli. Ennek oka egyrészről a szabályozásban általában elvárt technológiai függetlenség, másrészről a technikai változások üzleti szempontból történő lekövetésének gyakorlati nehézségei, ahogy azt a PCI DSS SSL és korai TLS verzióváltással kapcsolatos felhasználói ellenállása és az átállási idő módosítása is mutatja. Az auditálási tapasztalatok azt mutatják, hogy az új átállási idő tartható és a felhasználók többségénél a problémát már megoldották, de vannak még kivételek.

Felhasznált irodalom

[1] Indira Nurdiani, Jürgen Börstlera, Samuel A. Frickera, The impacts of agile and lean practices on project constraints: A tertiary study, Journal of Systems and Software, Volume 119, September 2016, Pages 162–183

[2] Matt Burgess: Google Chrome will start blocking Flash by default, Wired, 16 May 2016 [2016.08.01.] http://www.wired.co.uk/article/google-chrome-adobe-flash-html5

[3] CVE-2014-0160, CVE-2014-0346

[4] Nagy Dániel: Kriptográfiai kihívások a vezeték nélküli szenzorhálózatokban, Hadmérnök, XI. évf. 2016/1. sz.

[5] Szabó Tibor: Kormányzati informatikai hálózati infrastruktúrák védelmi rendszereinek új kihívásai a vezeték nélküli kommunikáció tükrében, Bolyai Szemle, 2015/3. sz.

[6] Dario Forte, The death of MD5, Network Security, Volume 2009, Issue 2, February 2009, Pages 18-20

[7] PCI SSC: Bulletin on Migrating from SSL and Early TLS https://www.pcisecuritystandards.org/pdfs/Migrating_from_SSL_and_Early_TLS_-v12.pdf [2016.08.05.]

[8] Erik Costlow: Diagnosing TLS, SSL, and HTTPS https://blogs.oracle.com/java-platform-group/entry/diagnosing_tls_ssl_and_https

[9] NMHH: Algoritmusokkal kapcsolatos határozatok http://nmhh.hu/tart/index/1442/Algoritmusokkal_kapcsolatos_hatarozatok

[10] ETSI TS 102 176-1 v 2.1.1 (2011-07) „Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”

[11] Mozilla: Firefox Releases https://www.mozilla.org/en-US/firefox/releases/ [2016.08.21.]

[12] Chrome Releases http://googlechromereleases.blogspot.hu/ [2016.08.21.]

[13] Transport Layer Security https://en.wikipedia.org/wiki/Transport_Layer_Security [2016.08.21.]

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Andras TÓTH
toth.hir.andras@uni-nke.hu

AUTHORIZED RADIO SYSTEMS TEST IN URBAN AREA

Absztrakt

Because of hybrid warfare and migration there are emerging new requirements for communication networks. Nowadays many military activities are carried out in urban areas, where the interference and shielding bring difficulties in radio networks. In this paper, there will be presented three different radio systems test to install network centric communication to support commanders' military decision making

A hibrid hadviselés és a migráció új követelményeket támaszt a kommunikációs hálózatokkal szemben. A városi körülmények között végrehajtott katonai műveletek számára nehézséget jelent a rádió hálózatokat érő interferencia és visszaverődés. Az alábbiakban három rádiórendszer kerül bemutatásra, amelyek a parancsnoki döntéshozatalt hivatottak elősegíteni a hálózatközpontú kommunikáció során.

Keywords: *very high frequency radio; cellular radio system; ultra-wideband radio; network centric communication system; decision making process; situational awareness ~ magas frekvenciájú rádió, cellás rádió rendszer, ultra szélessávú rádió, hálózatközpontú kommunikációs rendszer, döntéshozatal, helyzetismeret*

INTRODUCTION

After analyzing the ongoing military operations all over the world we can argue, that the military environment has been changed in the 21st century. Based on these there is one theory, which deals with generations of warfare. Some experts are expressing that nowadays we are in the era of the so called Fourth Generation Warfare (4GW). In parallel with this there are described the so called "hybrid warfare" activities too. "Hybrid threats are – any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battle space to obtain their political objectives" [1]. In the main military hotspot areas (Afghanistan, Iraq) these hybrid warfare activities are the most specific operations. Usually the countering military missions are carried out in urban environment, which can cause huge difficulties for our communication systems, and the internet and mobile networks are influenced also by hybrid challenges. [2]

In our days, the other important security issue, which is needed to be mentioned, is the migration. There are strong governmental and social expectations in Hungary that we must control our borders and especially to recon terrorists aiming to enter to the European Union. Of course, when migrants entering our territories they find cities, villages and other objects, which can influence our communication networks.

The above mentioned threats and challenges are influencing the military application too. Dedicated experts are arguing, that next generation of commanders should be ready for them and it is expected that they must lead their units in a very proper way. [3]

In May 2016, the Faculty of Military Sciences and Officer Training (National University of Public Service, Budapest, Hungary) conducted an exercise focusing on urban combat. The signal soldiers have had to provide a network centric communication system to support the commander with almost real life information. It means that after the soldiers get the information, they have had to transmit and process it to build up the best situational awareness. [4] At the lowest level (company, platoon) there were just radios available to establish the subnetworks.

This paper presents the problems and the solutions of the radio communication with different devices in urban district.

THE RADIO SYSTEMS OF THE EXERCISE

In the beginning of the exercise we had to realize which our possibilities are. For this we had to know our capabilities such as:

- tasks to be carried out;
- system of activity and deployment;
- number and nature of partakers,
- organizations;
- info-communication capabilities of professional control;
- tasks of the subordinate staff, system of activity;
- environment of the execution;
- available tools and infrastructure at hand [5].

We used three different types of radios on the exercise. First of all, we tried to communicate via our VHF military radios, then we used a civil cellular radio system, and the last version was the ultra-wideband radios.

Military VHF Radio

The military radios were multi-role radios with modern transmission techniques provides long reach- and noise resistant communication. The system is developed to meet the demands in modern tactical communication, and have a wide range of roles: combat net radio (CNR), combat net radio relay, data transmission, text message terminal, single channel radio access. The technical data of the radios:

–Frequency band:	30,000–87,975 Hz
–Channel bandwith:	45 kHz
–RF modulation type:	GMSK (Gaussian minimum shift keying)
–Modulation data:	Orthogonal M-ary
–Channel spacing:	25 kHz
–Output power:	10 mW; 500 mW; 5 W or 50 W
–Interfaces	Eurocom J (multiwire – modified RS-232) compatible with V.24/V.28 Eurocom K and K+ (2-wire) 2 audio interfaces (also for parameter loading

During the exercise we used the frequency hopping mode to avoid enemy jamming and interception. The audio and data signal was encrypted, and the signal was encoded with spread spectrum technique and modulated with Gaussian Filtered Minimum Shift Keying (GMSK) modulation. The radios used frequency hopping by constantly changing the carrier frequency. In this case the transmitter and receiver had to follow the same hopping pattern. Our main problam was with the hopping network, that for the communication it was required very exact time synchronization (among the radios $\Delta t<300$ ms in the same network). We used the radio for voice and data networks in combat net radio and Autonomous Packet Radio (APR) mode. Both communications had an issue with the reflection and the shielding. When we had direct line of sight (LOS) the network worked fine, but it was just among few of the soldiers, not among all of them. For that the better solution was the APR, where the operators have the possibility to do direct adressed calls to other radio operators. In this case the radios, which have LOS, forward the call to the next radio till the signal reaches the receiver. The communication channel is this signalway among the radios.

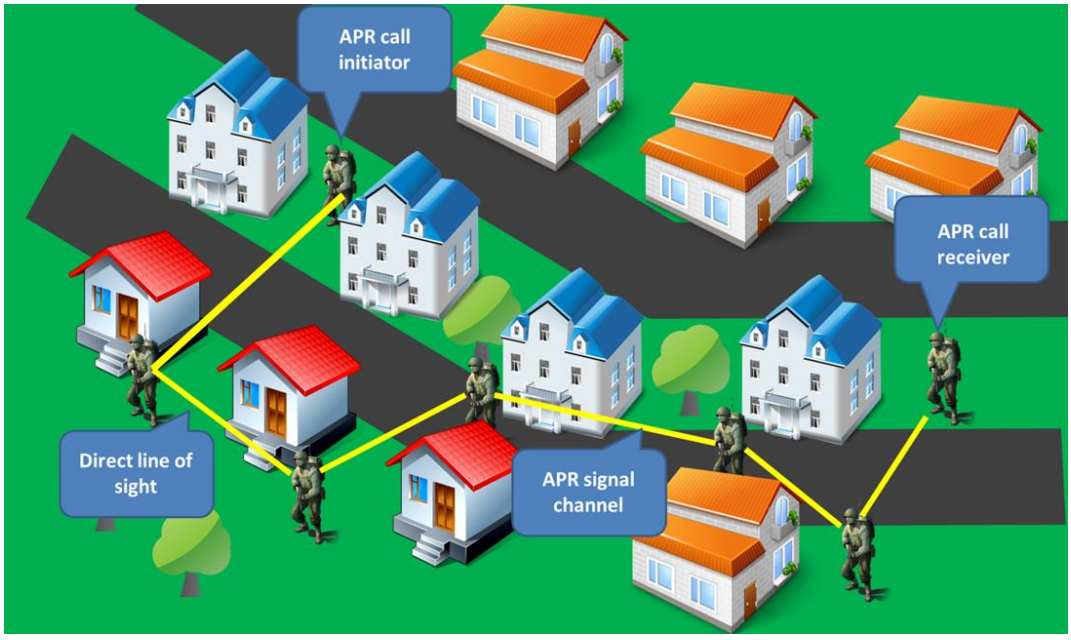


Fig. 1. The autonomous packet radio (APR) mode in urban area.

We were able to provide voice, data and message terminal functions for the soldiers. The voice and message terminals worked well in these solutions but the datarange was too low, so we could not send real life pictures for the commanders. In data transmission services the maximum data rate was in asynchronous transfer mode 19,200 bit/s. Because of this, and the long distance among the troops and headquarters the situational awareness was not granted so we had to use other services. Another disadvantage of the radio that it is not a Ground-Air-Ground (GAG) radio, so we did not have the possibility to communicate to the aircrafts during the exercise.

The Civil Cellular Radio System

We tried to use a civilian system, so called unified digital radio system, with which we are able to make direct push-to-talk (PTT) communication to groups and with priority setting; centralized call control, for priority and queuing; direct mode, portable to portable without central radio coverage; relay mode, one portable can use another mobile device to link to the central radio; and data networks. A huge advantage of the system is, that we can coopeerate with police, disaster management, fire departments, ambulance and other services, which use the same devices. The network based on terrestrial trunked radio (TETRA) technology. It provides secure speech and data transfer, and on the management side we can follow our troops via the built GPS in the devices. If we have no GPS in our radio the system can also show our near position with triangulation from the base stations. We are able to send pictures and videos on the system, because the available data rate can manage it continously. [6] The data rate can reach the 700 kbit/s with 64-QAM and the bandwidths of 150 kHz with direct LOS, so we could help the commander's decision making with real information.

Table 1. The Most Important System Parameters for TETRA [7];

Parameter	Value
Frequency	380-385 MHz (mobile station) / 390-395 MHz (base station)
Carrier Spacing	25 kHz
Access Method	TDMA, 4 Timeslots / Carrier
Uplink / Downlink Spacing	10 MHz
Modulation	π/4 DQPSK
Carrier Data Rate	36 kbit/s
Voice Coder Rate	7.2 kbit/s gross

The problem is with the system, that at least one base station is needed for the communication. At the exercise area, we had one of it, where the companies and platoons acted. They could communicate directly with this station, or reached it with relay mode. Someone, who can not connect to the base station directly, can use another mobile device to get connected to the radio network. Because we had just one node at the area sometimes it happened, that some of the soldiers were dropped off the network, because it was overloaded, when many of the wanted to communicate at the same time. The battalion headquarters was about 20 km far away from them, and there we had our own base station. The commander and the members of the staff had their own private mobile radio, and at the communication and information section we had a public access mobile radio. It was a huge advantage, because with it we were able to connect the radio system to the local area network (to share data with the subunits) and to the Private Automated Branch Exchange (PABX) and the Public

Switched Telephone Network (PSTN). This povided for us the possibility to make calls from the radios to the telephone system and we could reach from the desks of the staff the troops on the exercise field. It helped to make a faster communication and better information sharing from the lowest levels. The system can be connected to the GSM network as well, and we are able to make direct call to mobile phones if it is necessary.

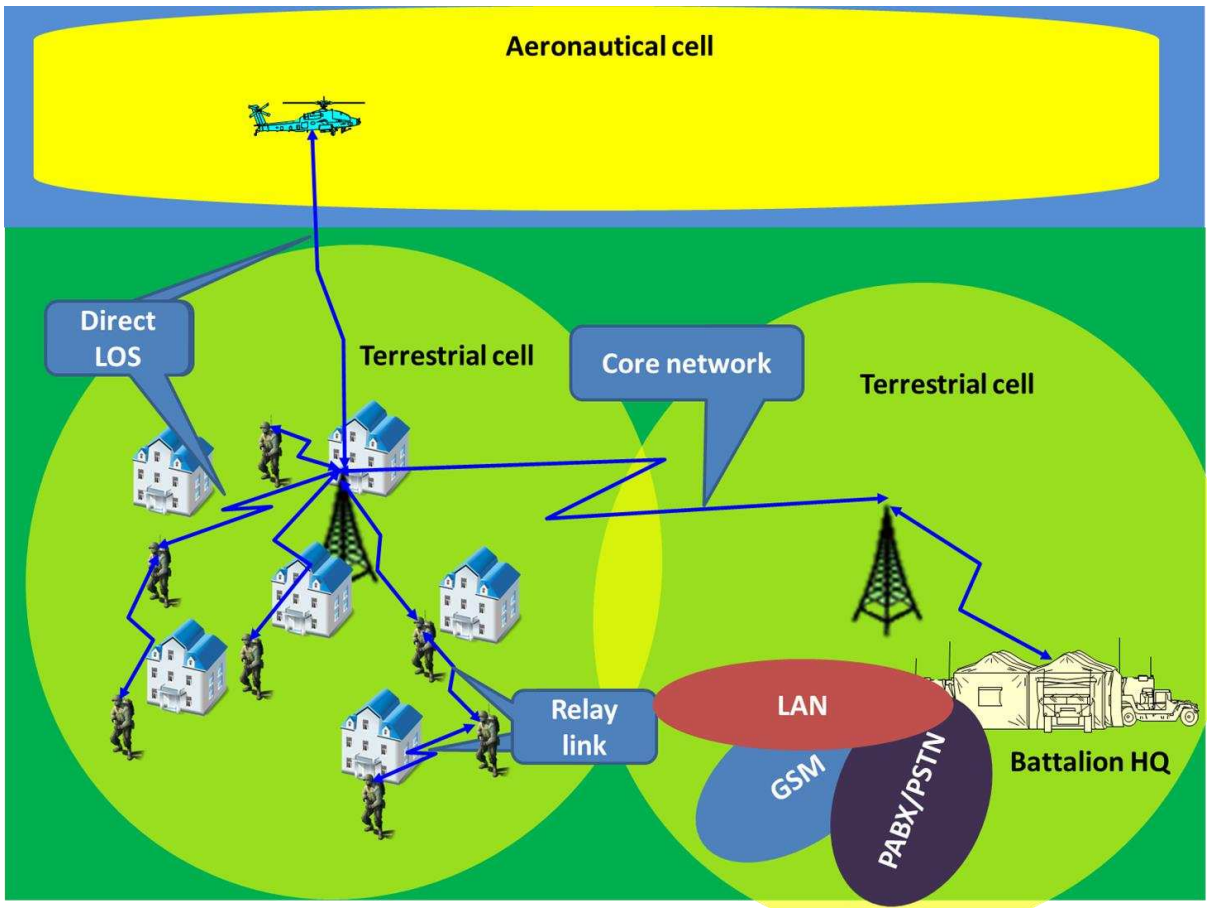


Fig. 2. Terrestrial and Air-Ground-Air network of unified digital radio system [8].

Another advanatge of the system is that it has Air-Ground-Air (AGA) capability, so we had the possibility to communicate with aircrafts like helicopters and airplanes. It helped to ask close air support (CAS) and medical evacuation (MEDEVAC), or just to keep the contact with the aircrafts during the missions.

Due to the cellular technology, the long distance among the troops and headquarters was not an issue, because we could send our data on the established core network between the two base stations. The voice, the data and the video signals were separeted from each other with virtual private network, and the management helped to reach the best quality of service.

Our communication networks operated very well with this solution, we could provide real life information (data, picture and video) for the commander and the subunits to support situational awareness. The problem with it is that most of the services do not work without base station. Because of this reason we can use this system inside the country, where the core network is built, but this solution can not operate for instance in peacekeeping missions.

Ultra-Wideband Radios

We tried on the exercise an ultra-wideband (UWB) radio as well to build a network centric operational area. It was a high-speed, short-range wireless communication network to share information on situational awareness and tactical instructions for the commanders. It was a wireless mobile network to forward high-speed communication (voice and data) within a cluttered urban warfare environment. The ultra-wideband systems have some benefits such as:

- provide high data rates;
- have very good time domain resolution allowing for ranging and communication at the same time;
- have immunity to multipath and interference [9].

The UWB is an air interface technology that provides adequate bandwidth, and with it we can establish an optimal operational environment, which is effectively maintain a low probability of detection and intercept.

We used devices with standard IEEE 802.15.3 and we reached the maximum data rates of 50 Mbps in short range (about 10 meters). We had several short distance wireless personal area networks (WPANs), and the information sharing was acted on them. The data rates decreased exponentially; above 30 meters the signal loss was so high, that we used the devices just on the maximum range of 25-30 meters. The platoon commanders could follow their troops among the buildings very well from there command posts; they had real life pictures from the activities. Due to the reflections and the short distance of the soldiers everybody was reachable, and there was just a very few point of the shielded territories.

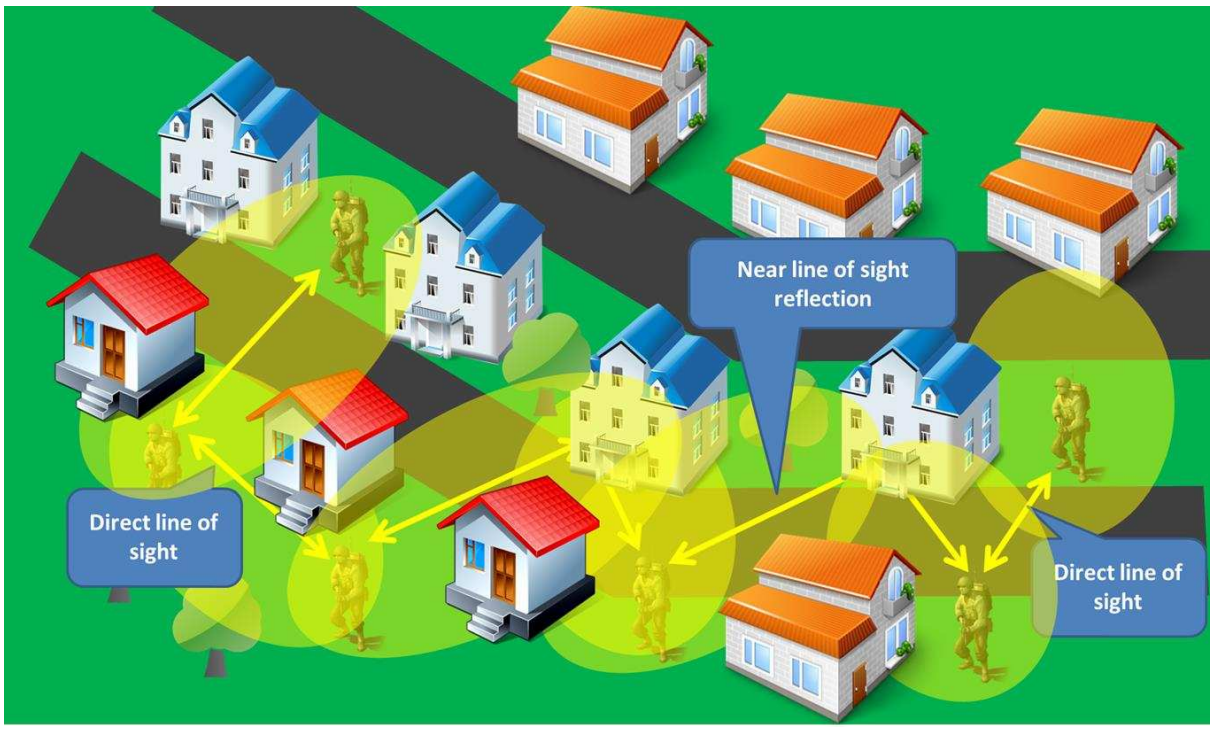


Fig. 3. The ultra-wideband radio usage on urban warfare environment.

According to our experiences the UWB radios could work very well in urban area on short range communication, but the problem was, that we could not send the information to the higher headquarters. We had to establish a node close to the command posts of the executors. There was a mobile microwave link to be installed between the node and the battalion headquarters. The radio was a flexible software defined radio microwave radio with the

frequency band 7-8 GHz, and the interface was configured to transmit four 2 Mbit/s channels. Another disadvantage of the system, that we had no connection with aircrafts, commanders had to use also the devices of the node to communicate with helicopters and close air support airplanes.

CONCLUSIONS

On the exercise we used three different systems to support commanders' military decision making in urban area. Nowadays the main activities of military and non-military (peacekeeping, humanitarian, and boarder guard) operations are executed in villages, cities or populated areas. As signal soldiers we have to provide the best communication links for the commander and units to get in touch and to share information to make situational awareness.

The first system was an authorized military VHF system in the Hungarian Defence Forces. We realized that these radios are not able to provide the necessary capability for a network centric communication system. In urban areas the radios can not communicate among each others because of the interference and shielding. In open areas the systems provided reliable voice communication in over 20 kilometers range, but the data rate was so slow that we could not provide real life information. The only one possibility was, to send data via this system, the short text message, but it was not enough to share all the necessary information. Other disadvantage was that the soldiers could not get in touch with aircraft, because these radios are not interoperable with our airforce radios.

The second system was a civilian cellular radio network, which worked very well on the exercise area; we could share information in near-real life (voice, data, video etc.). The main conclusion was that we can use this network at our boarders, because it is needed base stations for the system. With mobile base station we could install this complex in abroad as well, and then it can support for instance the peacekkeping missions too. It is able to work together with aircrafts and cooperate with other services such as police, fire departments, ambulance. According to the system's management methods we can carry out multinational networks, and it provides secure communication links among allied troops, and helps the information sharing for the commanders via data transfer links.

The third system was an ultra-wideband radio network, which was able to provide high-speed communication links in a short-range territory. In small units it was the best solution to share information inmediatelly, but a huge issue of the system was that we could not send data from the units to the headquarters with it. It was needed to install an other communication link to share information with the commanders on the exercise area.

To summarize the three systems have separeted capabilities and possibilities. They can be integrated in one system and with this solution we are able to build a network centric communication system, where the commanders can share information among each others. The VHF and UWB devices can be used by the subunits, and the cellular network can support the communication links with the higher headquarters.

References

[1] G. Mgaloblishvili, B. Kutelia, I. Guruli, and N. Evgenidze, "Hybrid warfare and the changing security landscape in the euro-atlantic area", Economic Policy Research Center (EPRC), Tbilisi, Georgia, 2016, p. 10

[2] Balog Fatime, Fekete Csanád, Németh András, Németh József Lajos: A hibrid hadviselés különös tekintettel a mobil kommunikációra, in: HADMÉRNÖK X:(4) pp. 120-131. (2015)

[3] Németh József Lajos: „Korszerű hadviselés, korszerű vezetői felfogás” I.: Összefoglaló Dr. Porkoláb Imre dandártábornok előadásáról az MH ÖHP-n, in: http://biztonsagpolitika.hu/cikkek/korszeru-hadviseles-korszeru-vezetoi-felfogas-i-osszefoglalo-dr-porkolab-imre-dandartabornok-eloadasarol-az-mh-ohp-n, 2016:(02.10) pp. 1-4. (2016)

[4] Farkas Tibor, “Questions and tasks of communication in disaster and crisis situations in Hungary”, Communications 2015, pp. 117-126

[5] Farkas Tibor, and Hronyecz Erika, “Basic information needs in disaster situations (capabilities and requirements)”, Proceedings of the XXI-th International Scientific Conference of Young Engineers], Cluj-Napoca, Romania, 2016, pp. 153-156

[6] Farkas Tibor: A katasztrófavédelmi és válságkezelési tevékenységek általános elemzése az irányítás és az infokommunikációs támogatás tükrében; in: HADMÉRNÖK XI:(3) pp. 135-148. (2016)

[7] Rohde & Schwarz, “TETRA Measurements, Application Note”, München, Germany, p. 4

[8] Terrestrial Trunked Radio (TETRA), Voice plus Data (V+D), Designers' guide, Part 6, Air-Ground-Air, European Telecommunications Standards Institute, 2011, p. 9

[9] Simon L. Cotton, and William G. Scanlon, “Millimeter-wave soldier –to-soldier communications for covert battlefield operations”, IEEE Communication Magazine, Vol. 47 No. 10, October 2009, pp. 72-81.

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Végvári Zsolt
vegvari.zsolt@hm.gov.hu

A HIBRID VILLAMOS ENERGIAELLÁTÓ RENDSZEREK VEZÉRLÉSÉNEK TEREPI MEGVALÓSÍTÁSA

Absztrakt

Napjainkban a katonai táborok működése elképzelhetetlen a villamos áram nélkül. Ezt mostanáig szinte kizárólag fosszilis üzemanyagok elégetésével biztosították, ami nemcsak költséges és környezetszennyező, de az ellátás biztosítása is nagyon kockázatos. A hagyományos és a megújuló energiaforrásokra épülő technológiák kombinációját jelentő hibrid rendszerek ötvözik a generátorok megbízhatóságát a megújuló források olcsóságával és tisztaságával, de csak abban az esetben, ha a rendszert alkotó elemek vezérlése képes minden pillanatban optimalizálni a működést. Mivel a katonai hibrid berendezéseknek a legzordabb terepi körülmények között is megbízhatóan ki kell szolgálni a fogyasztókat, a vezérlést végző rendszerelemekkel szemben is rendkívül szigorúak az elvárások. Természetesen az eltérő tervezési elvek miatt számos módon lehetséges a vezérlés terepi kivitelű megvalósítása.

Nowadays, the operation of military camps would be impossible without electricity. Until now it was provided almost exclusively by burning fossil fuels, which is not only costly and polluting, but secure of its logistics is also very risky. As the combination of traditional and renewable energy technologies, hybrid systems connate the reliability of generators with the cheapness and clearness of renewable sources, but just in case, if the system control is able to optimize the operation of the components every moment. As the military hybrid devices must be reliably serve consumers even in the toughest field conditions, system control elements are called on to meet extremely high expectations. Of course, because of the different design principles it is possible to achieve the design of the controller according to field conditions in several ways.

Kulcsszavak: *hibrid villamos energia, mikrogridek, műveleti terület, vezérlő egység ~ hybrid electricity, microgrids, operational area, controller unit*

BEVEZETÉS

A villamosság felfedezése óta az emberiség évről-évre egyre jobban támaszkodik erre az energiaformára. Nincs ez másként a hadseregek esetében sem. Mind a gyalogos katonák felszerelésében, mind a gép- és harcjárművek fedélzetén egyre több a villamos működésű eszköz [1, 42 o.] és külön fejezet a katonai létesítmények villamos energiával történő ellátása. A védelmi szféra állandó települési helyű, avagy „béke" létesítményei az esetek döntő többségében a polgári villamos hálózatra kapcsolódnak, hiszen ennél gazdaságosabb megoldás aligha kínálkozik, de egészen más a helyzet a haderők ideiglenesen települt egységeivel. A gyakorlatok, a békemissziós küldetések illetve a tényleges fegyveres konfliktusok idején komoly logisztikai és technikai kihívás a táborok villamossággal történő ellátása ott, ahol nincs megbízható villamos infrastruktúra.

A második világháború idején a táborokban a világítást, a főzést és a fűtést is fosszilis tüzelőanyagok vagy fa elégetésével oldották meg, még a legkorszerűbb hadseregek is, és a villamosságra csupán a kommunikációs eszközök működtetéséhez volt szükség. Erre a célra akkoriban kisebb aggregátorokat1 rendszeresítettek [2, 258 o.], jobbára az adott eszközökhöz külön-külön. Ezzel szemben napjainkban gyakorlatilag a katonai táborok csaknem kizárólag villamossággal működnek. A világítás, a már alapkövetelménynek számító klímaberendezések, a tábori konyhák és a teljes vezetési rendszer villamos energiával üzemel. A nagyszámú, hálózatba kötött villamos fogyasztó kiszolgálására pedig nagyteljesítményű, egész táborok vagy táborrészek ellátására alkalmas aggregátorok használatosak.

A katonai aggregátorok jelenleg többnyire a polgári berendezésekhez hasonlóan gázolajjal üzemelnek, aminek oka a dízelmotorok viszonylag nagy hatásfoka, de a NATO egységesítési törekvéseinek következtében az üzemanyag módosulhat[2]. A folyamatos működéshez szükséges üzemanyag biztosítása annak fajtájától függetlenül mindenképpen jelentős logisztikai kihívás. Fegyveres konfliktusok alatt, békemissziók idején legalább részben megsemmisült, megbízható működésre képtelen polgári infrastruktúrával kell számolni, vagyis a táborok működtetéséhez szükséges üzemanyagokat, a hadseregeknek maguknak kell biztosítani. A gyakorlatban üzemanyag-szállító konvojokat szerveznek, amelyek nyilvánvalóan elsőszámú célpontjai az ellenségnek. Ez annyira igaz, hogy közelmúlt iraki és afganisztáni megszállása alatt az egyik legveszélyesebb, legtöbb áldozatot követelő tevékenység is a konvojok kísérete volt [4].

[1] A magyar szakirodalom aggregátornak nevezi a villamos energiát előállító generátor és az azt meghajtó hőerőgép (többnyire dízelmotor) komplexumát. Az angolszász szakirodalom nem ismeri az aggregátor kifejezést és csak, mint „diesel generator"-t említik az ilyen berendezéseket, amely szokás a magyar hivatkozásokban is terjed. Jelen cikkben ragaszkodom a magyar kifejezéshez.

[2] A közelmúlt háborús eseményei igazolták, hogy szárazföldi haderők béke lehelyezésen kívüli üzemanyag-ellátása a számos használatos tüzelőanyag miatt tarthatatlanul bonyolult, ezért az új doktrína [3, 1512. pont] értelmében a jövő harceszközei és hadfelszerelései már csupán egyetlen üzemanyagot, a kerozint használhatják, ami várhatóan lényegesen leegyszerűsíti az ellátási lánc kiépítését.

1. ábra: egy holland gyártmányú, konténeres „nagy” hibrid rendszer működés közben a CL15 gyakorlaton (a szerző fotója)

Mivel a katonai táborok villamos energia iránti igénye a közeljövőben aligha fog csökkenni, a villamosság előállításához szükséges fosszilis energiahordozóktól való – legalább részbeni – függetlenedés kiemelt kutatási terület mind a nemzeti és nemzetközi,[3] mind a NATO[4] fejlesztési célkitűzéseiben. A megújuló energiaforrások felhasználása kézenfekvő megoldás a katonai tevékenységek során is, de azok megbízhatatlansága miatt egyelőre nem mondhatunk le a hagyományos aggregátorokról sem [1, 53 o.]. A két technológia házasságából születtek az ún. hibrid rendszerek. A cikk írásának idején még egyetlen európai haderő sem tart rendszerben ilyen berendezést,[5] de miután a nemrégiben Magyarországon megrendezett CL15 logisztikai gyakorlaton[6] több ilyen eszköz is demonstrálta a technika életképességét, várható, hogy a közeli jövőben szép számmal megjelennek majd a hadfelszerelések között.

Mivel a hibrid rendszerek összetett algoritmusokkal biztosítják az optimális működést, a katonai változatoknál kiemelt fontosságú a vezérlésre alkalmazott elektronika olyan robosztus kivitelezése, ami alkalmassá teszi őket, hogy a terepen való fokozott igénybevételnek kitéve is el tudják látni feladatukat. Mivel a témának újszerűsége miatt még nagyon csekély irodalma van, elsősorban saját gyakorlati tapasztalatokra építve kívánom ismertetni ezt a modern technológiát, külön figyelmet fordítva a vezérlő elektronika terepi működést lehetővé tevő elméleti és gyakorlati megoldásokra.

[3] Az Európai Védelmi Ügynökség (European Defence Agency – EDA) Energia és Környezet Munkacsoportja foglalkozik a vonatkozó nemzeti fejlesztések összehangolásával.

[4] A NATO szervezetén belül a brüsszeli székhelyű Újszerű Biztonsági Kihívások Osztálya (Emerging Security Challenges Division – ESCD) valamint a vilniusi székhelyű Energiabiztonsági Kiválósági Központ (Energy Security Center of Excellence – ENSEC COE) végez ilyen jellegű kutatásokat.

[5] Az EDA már közel egy éve üzemeltet kísérleti jelleggel egy ilyen berendezést Maliban, a NATO ENSEC COE pedig nemrégiben vásárolt szintén a tapasztalatok gyűjtése céljából egy hibrid komplexumot [5].

[6] A Capable Logistician 2015 Nemzetközi Logisztikai Együttműködési Gyakorlat 2015 júniusában került megrendezésre az MH Bakony Harckiképző Központjában a várpalotai lőtéren [6, 30 o.].

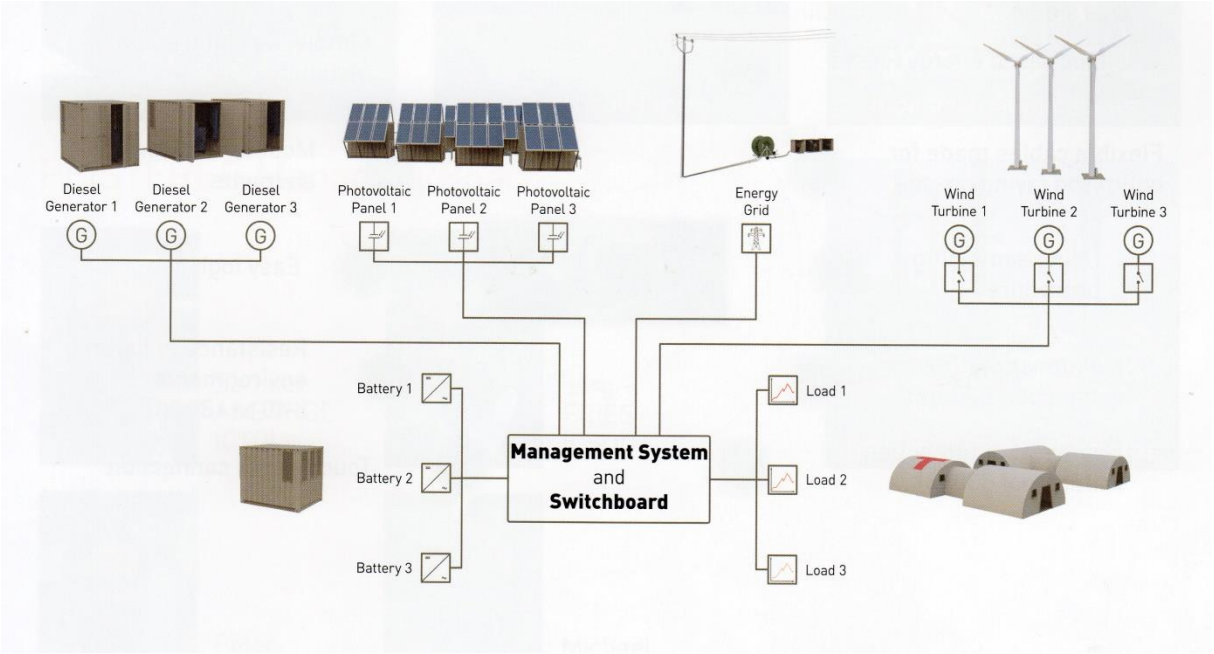
A HIBRID VILLAMOS RENDSZEREK

A hibrid villamos rendszerek felépítése és működése

A hibrid villamos energia ellátó berendezések alapvető célja, amint azt már említettem, a fosszilis tüzelőanyagok felhasználásának csökkentése. Az első ilyen jellegű eszközöket polgári céllal hozták létre még a XX. század végén, az energiatakarékosság és a környezetvédelem jegyében. Amennyiben egy lokális villamos energiatermelő berendezés illetve a lokális fogyasztók egyetlen hálózatban üzemelnek, a nemzetközi szakirodalom a mikrogrid kifejezést használja, amelyet a katonai források is átvettek, bár itt még nem alakult ki az egységes terminológia.[7]

Az ilyen mikrogridek lehetséges elemei a következők:

- Megújuló energiaforrást használó villamos energiát előállító berendezések (jellemzően napelemek)
- Hagyományos dízelaggregátor
- Energiatároló egység
- Hálózati távvezeték interfész
- Vezérlő és menedzsment rendszer



2. ábra: egy teljes kiépítésű mikrogrid elvi vázlata (forrás: Pfisterer)

A polgári rendszerek az esetek többségében az eltérő célok és követelmények miatt nem teljes kiépítésűek, vagyis nem tartalmazzák az igen költséges energiatároló egységet és a dízelaggregátort sem. A működés során a többlet energiamennyiséget, amit a helyi fogyasztók pillanatnyilag nem használnak fel, visszatáplálják a hálózatba, és ha a helyi termelés nem képes kielégíteni a helyi fogyasztást, akkor a hálózatból fedezik a különbözetet. Amint látható, a helyi energiabiztonság növelése nem elsődleges kívánalom az ilyen megoldásoknál, de a sok összekötött mikrogriddel megerősített hálózat mégis jelentősen megnöveli a teljes villamos rendszer hibatűrő képességét [6, 32 o.].

[7] A NATO-n belül a „microgrid”, az EDA-nál inkább a „smart grid” kifejezés használatos.

A katonai rendszerek gyökeresen más koncepció szerint épülnek fel. Mivel a szükséges energiamennyiséget bármikor, bármilyen körülmények között biztosítani kell a fogyasztók felé, a hagyományos aggregátor itt kötelező elem. Ugyanakkor a villamos távvezetékhez való csatlakoztathatóság lehetőségét sok esetben nem teremtik meg, mert ahová ezeket a berendezéseket szánják, ott valószínűleg úgysincs vezetékes áramszolgáltatás. Ez azt is magával vonja viszont, hogy meg kell oldani a helyi többlet tárolását és a kisebb hiányok, az aggregátorok indítása nélküli áthidalását is, amit többnyire masszív lítium-alapú akkumulátorcsoportokkal érnek el [6, 32 o.], illetve újabban vizsgálják a hidrogéncellás működés lehetőségét is.

Ugyan a katonai mikrogrideknél nem annyira a gazdasági, mint inkább a taktikai előnyök megszerzése motiválja a fosszilis üzemanyagok felhasználásának mérséklését, azért az aggregátorok által meg nem termelt energiát még valahonnan fedezni kell. Erre szolgálnak a megújuló energiaforrásokon alapuló technológiák, amelyek igen sokfélék lehetnek, de többségük sajnos nem alkalmas a katonai felhasználásra. Az erőművi technikák túlnyomó része már a méreténél fogva sem jöhet szóba, így pl. a tükrös naperőművek sem. Vízerőművek elvben egész apró méretben is kivitelezhetőek, és bár a hatékonyságuk is alacsony, elsősorban azért nem használhatók, mert a műveleti területek jelentős részén egyszerűen nincs olyan vízfolyás, amelyre rá lehetne építeni őket. A biomassza és a geotermikus energia pedig olyan méretű kiszolgáló infrastruktúrát igényel, aminek a mobilitása gyakorlatilag nulla. A gyakorlatban tehát a lehetséges alternatívák száma mindössze kettőre csökken, a szélenergiára és a fotovillamos elven alapuló[8] napelemekre [1, 47 o.; 50 o.].

A szél a kontinentális éghajlaton (így Magyarországon is) többnyire csak a talajszinttől mért nagyobb magasságokban számottevő és megbízható [10, 24. p.]. Ráadásul a szélgenerátorok telepítése nehézkes, könnyen elárulják a felhasználás helyét (a magas árbocok jól láthatóak, zajosak és nagy a radarkeresztmetszetük is), így az alkalmazásuk csak nagy körültekintés mellett javasolt. A napelemek főbb hátrányai, azon nyilvánvaló tényen túl, hogy éjszaka nem működnek, hogy hatékonyságuk radikálisan csökken, ha a napfény szűrten, vagy nem merőlegesen éri őket, a csillogásuk is árulkodó lehet. Mindezeken túl villamos egyenfeszültséget állítanak elő, ami ugyan az akkumulátoros tárolás szempontjából ugyan kedvező, de mivel a tábori hálózatok a polgári szabványú váltakozó feszültséget használják, a teljes rendszerben több átalakítás is szükséges. Ugyanakkor tagadhatatlan előnyük, hogy kisebb vagy nagyobb mértékben szinte minden égöv alatt elérhetőek (sőt még a világűrben is tökéletesen működnek), továbbá nagyon egyszerűen, gyorsan telepíthetőek [6, 48 o.].

A hibrid villamos rendszerek előnyei és hátrányai

A CL15 nemzetközi gyakorlat számos európai szintű újdonsággal szolgált a résztvevő nemzeteknek. Ezek közül is kiemelkedik, hogy soha nem látott mennyiségben vonultak fel korszerű katonai energetikai berendezések. Ennek nyomán – szintén első alkalommal – a villamosságért felelős erők és eszközök önálló logisztikai egységet alkotva, saját parancsnokság alatt tevékenykedtek[9]. A számos egyéb berendezés mellett a gyakorlat során négy önálló, viszonylag nagyméretű hibrid áramellátó rendszer került telepítésre. Ezek – jogi és technikai okok miatt – nem mikrogridként, hanem sziget üzemben,[10] azaz önállóan, a

[8] Nem a napfény hőhatásával forralt vízgőz segítségével hajtanak meg turbinákat és generátorokat, hanem a beeső fotonok egy félvezetőrétegben direkt módon hoznak létre elektron-áramot, mindenféle kísérőjelenség, pl. zaj nélkül.

[9] Annak ellenére, hogy a gyakorlaton résztvevő korszerű energetikai rendszereket kivétel nélkül külföldi polgári cégek szállították, jelentősen emelte Magyarország elismertségét, hogy az egység parancsnokságát egy magyar katona, a HM Védelemgazdasági Hivatal állományába tartozó Illés Attila ezredes látta el. E cikk szerzője a gyakorlat alatt az egység technikai tanácsadójaként és összekötőként dolgozott.

[10] Az angol szakirodalom az ilyen jellegű működést off-gridnek nevezi.

gyakorlatot kiszolgáló villamos hálózattól függetlenül látták el árammal a hozzájuk rendelt katonai egységeket. A gyakorlat két hete alatt valamennyi rendszer hibátlanul, kiesés nélkül működött, ami már önmagában is igazolja, hogy a hibrid rendszerek legalább akkora vagy még nagyobb üzembiztonságot kínálnak, mint az egyszerű aggregátorok, de ez természetesen még nem elég annak alátámasztására, hogy célszerű a hagyományos rendszerek kiváltása.

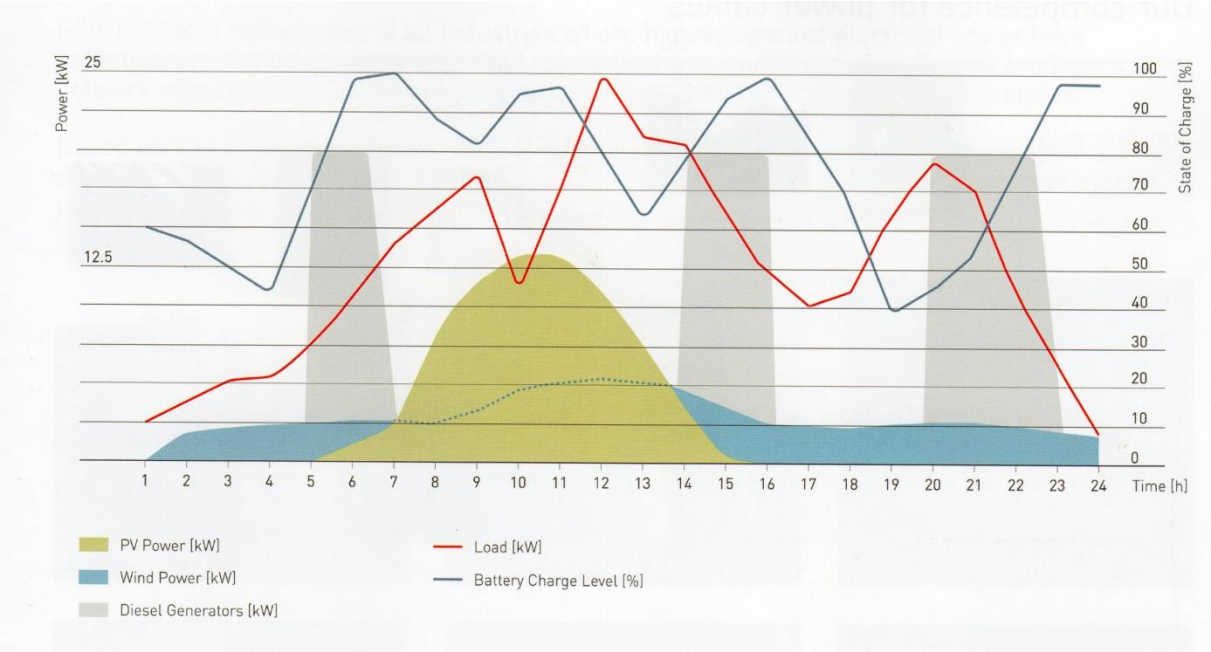
Az már sokkal többet árul el az ilyen rendszerek képességeiről, hogy a hozzájuk tartozó mintegy 800 m^2-nyi napelem a júniusi napsütésben naponta átlagosan 1 MWó tiszta energiával látta el a gyakorlat résztvevőit. A rendszerek gyártói előzetesen úgy kalkuláltak, hogy kb. 40-50 %-os üzemanyag-megtakarítást lesznek képesek felmutatni a gyakorlat végére, de részben a napos időnek köszönhetően több mint 60 %-ot értek el. Ez egyben alátámasztja azt is, hogy éves szinten nagyon is elképzelhető a magyarországi klíma mellett, a mintegy iparági szabványnak tekintett 40 %-os üzemanyag-megtakarítás. Azt is fontos viszont hangsúlyozni, hogy a 40 %-os elvárt érték egy jól kiegyensúlyozott rendszerre igaz, ahol a rendszerelemek skálázása arányos.

Szintén a gyakorlat alatt derült ki, hogy az egyik hibrid rendszer a tényleges fogyasztáshoz képest jelentősen túlméretezett PV és akkumulátor kapacitással lett felszerelve, így annak aggregátorát a második naptól már átvezényelték egy másik helyszínre, mivel egyáltalán nem volt rá szükség. Ez rámutat arra, hogy ha akkora akkumulátorkapacitást integrálunk egy hibrid rendszerbe, ami több napra is elég tartalékot jelent, elvben teljesen kiváltható az aggregátor (és már nem is hibrid a rendszer). De ez sajnos csak elvi lehetőség, mert a korszerű lítium-polimer akkumulátorok rendkívül drágák, így jelenleg csak egy hibrid rendszer lehet igazán gazdaságos, mert az nem hoz létre számottevő ritkán kihasznált tartalékot.[11]

Kevéssé ismert tény, hogy a hibrid rendszerek gazdaságosságához jelentős mértékben hozzájárul a beléjük integrált aggregátorok különleges működési módja. A hagyományos rendszereknél a dízelmotornak folyamatosan működni kell, akkor is, ha épp nincs fogyasztás, a hatásfok pedig mindvégig erősen függ a fogyasztó rendszerek pillanatnyi áramfelvételétől. A hatásfok kb. a névleges megengedett terhelés 80 %-nál maximális, kisebb terhelésnél ez drasztikusan romlik. Ezzel szemben a hibrid rendszerekben az aggregátorok csak az akkumulátorok töltésére szolgálnak, arra is csak akkor, ha a napelemek nem termelnek elégséges mennyiségű villamosságot. Ez annyit tesz, hogy csak ritkán, jellemzően egy-két alkalommal kapcsolódnak be egy nap, de akkor végig maximális hatásfokkal üzemelnek (ez az aggregátorok élettartama szempontjából is kedvező).

Ennél a pontnál érkeztünk el a hibrid rendszerek legnagyobb hátrányaihoz. Bár az általuk szolgáltatott villamos energia mintegy fele ingyen van, és az előállítás nem jár környezeti terheléssel sem, ezért cserében lényegesen bonyolultabbak, mint a hagyományos aggregátorok. Mivel a hibrid rendszerek több forrásból is állítanak elő energiát, megbízhatóbbak és hibatűrőbbek egy szimpla aggregátornál, de a számos kiegészítő berendezés sokkal szerteágazóbb üzemeltetési gyakorlatot és karbantartást kíván, jelentősen megnő általuk a rendszer mérete és tömege továbbá természetesen jelentős költséggel is jár az integrálásuk. A jelenleg létező katonai rendszerek nem sorozatgyártásúak, csupán még prototípusok, így elég nehéz kérdés azok árát megállapítani, de a gyártó cégekkel való konzultáció alapján a bekerülési költségük 3-5-szöröse lehet egy hasonló teljesítményű konvencionális aggregátornak.

[11] Amennyiben a gazdaságosság nem elsődleges szempont, reális alternatívája lehet az akkumulátoroknak a hidrogén üzemanyagcella és a vízbontó készülék kettőse, a témával bővebben foglalkozik Gregory Hoogers könyve [7]. A hidrogén energiasűrűsége sokkal nagyobb az akkumulátoroknál, és a napelemek áramával felbontva a vizet, folyamatosan állítható elő hidrogén. Katonai hibrid rendszerekben még nem használatos, de számos polgári megvalósítása már működik. Az üzemanyagcellák tömeges elterjedésének fő akadályai a katalizátorként használt platina drágasága és a rendkívül illékony és a levegővel igen robbanásveszélyes elegyet alkotó hidrogén megbízható tárolása [8, 97. o.].



3. ábra: egy mikrogrid 24 órás működésének sémája (forrás: Pfisterer)

Miután hibrid áramellátó rendszerek katonai környezetben történő üzemeltetésével kapcsolatban még csak minimális hiteles információ áll rendelkezésre a megtérülési időre vonatkozó számítások nem tekinthetők hitelesnek, de nagyságrendileg jó támpontnak tekinthetők [9]. Az egyik cég literenkénti 3 eurós üzemanyagár mellett[12] a rendszert folyamatosan használva mintegy 3-4 éves megtérüléssel kalkulál [9], ami igen kedvezőnek tekinthető. Ne feledjük viszont, hogy a gazdaságosság és a környezet védelme nem lehet elsődleges szempont ott, ahol katonák élete forog veszélyben. A hibrid rendszerek katonai alkalmazásának legfontosabb előnye, hogy általuk csökken a szállító karavánok támadásoknak való kitettsége, illetve azonos készletezett üzemanyag-mennyiség mellett mintegy kétszeresére nő a műveleti területen települt táborok önálló alkalmazási ideje.

A hibrid villamos rendszerek katonai alkalmazhatósága

Ahogy az előző részből kiderült, megfelelő alkalmazás mellett nem elhanyagolhatóak a hibrid rendszerek gazdasági és környezetvédelmi előnyei, a katonai felhasználást mégis az általuk biztosított kiterjesztett túlélőképesség indokolja. Az tény, hogy a hibrid áramellátó berendezések jelenleg még annyira újszerűek, hogy eddig egyetlen hadseregnél sem kerültek rendszeresítésre, de az általuk biztosított műveleti előny és a gazdaságosság miatt a védelmi szektor komolyan érdeklődik a technika iránt. Nem lebecsülendő indok a haderők a környezet védelme melletti elkötelezettségének demonstrálása sem.

A régi időkben megszokott volt, hogy a hadseregek voltak a technológiai újítások úttörői, de ez a szerep mára az alkalmazott technikák komplexitása és költségessége miatt részben átkerült az iparhoz. Ennek ékes példái a hibrid rendszerek. A jelenleg már üzemelő prototípusok szinte mindegyike egy-egy polgári rendszerre épül, gyakorlatilag azok katonai igények szerint módosított, robosztusabb kivitelű változatai. Alig egy-két olyan példa van, ahol az eszköz eleve előre megfogalmazott hadműveleti követelmények teljesítésére lett tervezve, illetve gyakori a kettős, katonai-polgári használatra is alkalmassá tehető megvalósítás.

[12] Az ár nyilvánvalóan lényegesen magasabb, mint a hazai töltőállomásokon megszokott, de ne feledjük, hogy a példában katonai műveleti területről van szó. Az itt említett ár magában foglalja az üzemanyag készletezéséhez, szállításához és védelméhez szükséges összes képesség fenntartásának és működtetésének aggregált költségeit is.

Mivel még csak kísérleti eszközökről és prototípusokról van szó, talán még korai ezek csoportosítása, de két fő fejlesztési irányzat már most is jól elkülönül és ezek sok szempontból markánsan különböznek is egymástól. Az első csoportba tartoznak a jellemzően nagy teljesítményű, önálló alegységek, kisebb táborok vagy táborrészek ellátására alkalmas rendszerek. Ezek a méretüknél és tömegüknél fogva szinte kivétel nélkül egy vagy több szabványos konténerre épülve kerültek kialakításra, de a mobilitásuk így is korlátozott. Noha a polgári rendszerekhez képest az egy-két órás települési és bontási idő extrém gyorsnak számít, ez még mindig nem teszi lehetővé, hogy gyorsan mozgó katonai egységeket kísérjenek.

A kisebb mobilitásért cserébe ezek a berendezések rendkívül jól bővíthetőek és skálázhatóak. Jellemzően teljes kiépítésűek, azaz valamennyi mikrogrid elemet tartalmazzák, többnyire még a nagyfeszültségű távvezetékekhez való kapcsolódás is megoldott, vagy csekély átalakítással megoldható. A konténeres kialakítás egyébként is nagyfokú modularitást tesz lehetővé, a várható körülményeknek és az alkalmazói igényeknek megfelelően könnyen módosítható pl. az akkumulátorok mennyisége és kapacitása, vagy megoldható a többféle nemzeti tábori villamos hálózatokra (pl. 230 V / 50 Hz vs. 110 V / 60 Hz) történő, akár egyidejű táplálás is. Napjainkban a korszerűtlen nagyteljesítményű tábori aggregátorok leváltására szánják őket.

A másik jellemző megvalósítás a rendkívül mobil, percek alatt üzembe helyezhető és bontható, de kisebb teljesítményű eszközöké. Ezek tipikus implementációja az ún. szolár-utánfutó, ahol egy vontatható alvázra telepítik a napelemeket, az akkumulátorokat és a vezérlést, de az aggregátort nem. Itt arra a koncepcióra építenek, hogy a gyorsan mozgó kis katonai egységek (pl. egy híradó állomás) saját áramellátása gépjárműfedélzetről vagy kisméretű aggregátorról megoldott, de mivel az áramellátás része a komplex célrendszernek (pl. a híradó komplexumnak), nem annak cseréjére, hanem inkább kiegészítésére szánják őket, mintegy utólagosan hozzáadva a hibrid rendszerek előnyeit. Ennek jegyében az ilyen, nem teljes, hibrid rendszerek sokféle „külső” aggregátorral képesek együttműködni, de a villamos távvezetékekhez történő csatlakoztathatóság egyáltalán nem elvárás velük szemben. A tervezők természetesen itt is törekszenek a modularitásra, de az alváz mérete és terhelhetősége e tekintetben nyilvánvalóan komoly akadályt jelent pl. az akkumulátorok mennyiségének variációja szempontjából.

A HIBRID VILLAMOS RENDSZEREK VEZÉRLÉSE

A hibrid rendszerek vezérlésének elvei

A hibrid rendszerek vezérlését hardveresen napjainkban minden esetben egy a feladathoz skálázott számítástechnikai eszköz, számítógép [12, 210 o.] valósítja meg. Ehhez kapcsolódnak az érzékelő elemek (szenzorok) és a beavatkozó elemek (kapcsolók), illetve rendkívül fontos a szoftver, vagyis az az algoritmus, amely megteremti az optimális termelés-felhasználás arányt.

Mind a polgári, mind a katonai hibrid rendszerek elsődleges célja a fosszilis tüzelőanyag felhasználás csökkentése, ezért a termelés során mindig a megújuló források használata élvez prioritást. A megújuló források által termelt villamosság polgári rendszereknél (napelemeket feltételezve egy inverteren[13] keresztül) közvetlenül a fogyasztói hálózatra kerül, míg katonai rendszereknél minden esetben az akkumulátorokat tölti. Ennek oka a folyamatos rendelkezésre állás biztosítása. Amíg az akkumulátorok és a fogyasztók közötti kapcsolat ép, a rendszer más elemeinek esetleges kiesésétől függetlenül mindaddig biztosított a folyamatos áramellátás, amíg az akkumulátorok teljesen le nem merülnek. Ez az idő egy jól megtervezett

[13] Villamos egyenfeszültségből váltakozó feszültséget előállító berendezés.

rendszernél több óra kell, legyen, így bőven adva lehetőséget az üzemeltetőknek a beavatkozásra.

Amennyiben a megújuló források tartósan nem képesek a fogyasztók által az akkumulátorokból kivett energiamennyiség pótlására, akkor szükséges elindítani a generátorokat. Ezt általában az akkumulátorok töltöttségének egy kritikus szint alá csökkenése váltja ki, ami az általam ismert rendszereknél 20 % körül van, de a konkrét konfigurációtól és a fogyasztóktól függően mindig a megkívánt minimális üzemidő tartalékhoz állítják be, sőt akár bizonyos paraméterek függvényében dinamikusan változhat is.

A vezérlés tervezési alapelveinél érdemes még megemlíteni a fogyasztók priorizálhatóságát. Ez annyit tesz, hogy túlterhelés esetén, vagy ha valamilyen meghibásodás miatt a rendszer nem képes teljes kapacitással működni, akkor a kevésbé fontos fogyasztói csoportok (pl. sátrak klimatizálása) leválasztásra kerülnek annak érdekében, hogy a létfontosságú alrendszerek (pl. kommunikáció) működőképesek maradhassanak. Ez egy olyan képesség, ami elvben egy egyszerű aggregátor esetében is megvalósítható lenne egy plusz berendezés hozzáadásával, de a hibrid rendszereknél elég csupán a meglévő szoftvert módosítani hozzá.

A fenti alapelvek csak egy adott konfiguráció optimális működését szabályozzák, vagyis a priorizált rendelkezésre állás követelménye mellett az aggregátorok üzemidejének minimalizálását. Ugyanakkor a vezérlésnek támogatnia kell az adott hibrid rendszer megvalósításának (konfigurációjának) teljes spektrumát. Ez annyit tesz, hogy ha a rendszer működhet különböző mennyiségű és teljesítményű akkumulátorok, napelemek és aggregátorok többféle összeállításában is, akkor azt a vezérlésnek is kezelnie kell. Ennek érdekében a vezérlést hardveresen több input és output csatornával kell ellátni, míg a szoftver oldaláról is lehetővé kell tenni az egyes konfigurációkhoz optimális algoritmus alkalmazását. Ez a jelenleg működő prototípusok esetén még kézzel történik, tehát a rendszerelemek megváltoztatása után módosított paraméterekkel újraindítják a vezérlést, de piacérett termékek esetén valószínűleg elvárás lesz a rendszerelemek „hot-swap”[14] variálhatósága.

Látható, hogy a hibrid rendszerek csak akkor képesek a tőlük elvárt működésre, ha a rendszerelemek megfelelő skálázása mellett a vezérlés is elég intelligens, mindamellett kellően gyors és pontos. A fejlődés trendjéhez tartozik az is, hogy míg a hagyományos katonai aggregátorok többsége úgy lett kialakítva, hogy folyamatosan igényli a kezelőszemélyzet jelenlétét, a hibrid rendszerek felépítéséből adódóan triviális a többé-kevésbé autonóm működés. Mivel a vezérlés mindenképpen része a rendszernek, bizonyos ergonómiai vagy a rendszer üzembiztonságát javító funkciók kialakítása lényegében nem jelent plusz hardverköltséget csak némi programozói munkát.

A vezérlésre alkalmazott informatikai megoldások

A hibrid villamos energia ellátó rendszerek vezérlése három főbb részre bontható, a rendszer állapotáról, működéséről információkat szolgáltató szenzorokra, a vezérlő algoritmust megvalósító informatikai eszközökre és a beavatkozó elemekre. A szenzorok villamos paramétereket (túlnyomóan feszültség és áramerősség) mérnek, illetve hőmérsékletet. Más érzékelő (pl. szélgenerátornál a fordulatszám-érzékelő) csak elvétve fordul elő az ilyen berendezéseken. A beavatkozó elemek szintén elég homogén képet mutatnak, lényegében csupán nagyszámú mágneskapcsolóról, néhány hőkioldóról van szó. Bár a kisebb teljesítményű szolár-utánfutókon félvezetős kapcsolókat is alkalmazhattak volna, talán az anyacégek[15] hagyományai miatt minden esetben ragaszkodtak a mágneskapcsolókhoz.

[14] Az elektronikus eszközök azon képessége, ami lehetővé teszi egyes részelemek működés közbeni cseréjét, anélkül, hogy a teljes rendszer működésében ez zavart okozna.

[15] A hibrid rendszereket fejlesztő cégek többségének nem ez a fő profilja. Az esetek többségében valamilyen hagyományos villamos energetikai cégnek a leányvállalata felelős az újszerű megoldások fejlesztéséért.

Egyértelmű tehát, hogy a vezérlés minden szempontból leginkább érdekes része az alkalmazott informatikai megoldás.

Miután a katonai hibrid rendszerek még csak prototípus szinten léteznek, nincs általánosan elfogadott „kvázi-szabvány” megoldás a vezérlő algoritmus implementálására. Erre a célra számos az informatikából ismert architektúra is alkalmas lehet. A rendszer összetettségétől és teljesítményétől függően egy 8 vagy 16 bites programozható kontroller ugyanúgy használható, mint egy mikroszámítógép (pl. Raspberry) vagy akár egy nagyteljesítményű PC. Ahogy a már működő rendszerek esetében viszonylag jól elkülöníthetőek a nagyobb teljesítményű konténeres rendszerek a mobil változatoktól, úgy a vezérlés kialakítása tekintetében is jól megfigyelhető két markánsan különböző eljárás.

A mobil szolár-utánfutók minden esetben valamilyen egyszerűbb programozható logikai vezérlőt (PLC)[16] alkalmaznak, amelyek kis méretek és tömeg mellett, számos változatban, igen szerteágazó képességekkel szerezhetőek be. Az általam megismert eszközökben Siemens, Omron és Wago gyártmányú PLC-k voltak megtalálhatók. Ennek a megoldásnak nagy előnye, hogy PLC-k szabványos ki- és bemenetekkel valamint szabványos programozási nyelvekkel rendelkeznek. A korszerűbb eszközök már időzítőt és számlálóáramköröket is tartalmaznak és a programnyelvük utasításkészletében olyan elemek is megtalálhatóak, mint a feltételes ugróutasítások vagy a szubrutinhívás. Ezekkel együtt a jelenleg akár már 100 euróért is beszerezhető PLC-k olyan feladatok megoldására is alkalmasak, amelyekhez néhány éve még komoly számítógépek voltak szükségesek.

A PLC-k a szerszámgépek vezérlésére használt félvezetős logikai áramkörökből jöttek létre, ezért az ipari környezetben való alkalmazásuk ma is triviális. Ennek köszönhetően igen sok PLC már eleve el van látva azokkal a védelmi megoldásokkal, amelyek alkalmassá teszik őket a terepi felhasználásra. Mivel hődisszipációjuk alacsony, nem igényelnek aktív hűtést és olcsón kialakíthatóak az IP65, IP67 védelmi szintnek megfelelő eszközök is.

A PLC-s megoldás hátrányai a korlátozott számítási teljesítmény, a rugalmatlanság és a korlátozott ergonómia. Annak ellenére, hogy a korszerű PLC-k is igen jelentős számítási teljesítményt nyújtanak, egy bizonyos szint felett a gyártók már áttérnek a teljes értékű folyamatirányításra is alkalmas számítógépek alkalmazására. Ennek oka nem abban keresendő, hogy a félvezetők mai integráltsági fokán nem lehetne erősebb processzorokat alkalmazni, hanem a bonyolultabb logikai modellek már nem követhetőek a PLC-k programozására használt gépközeli programnyelvekkel. Ahol a logikai modell már csak magasabb absztrakciós szintű programnyelvvel hozható létre, az már a számítógépek világa.

A PLC-k programját szinte minden esetben egy PC-n futó, igen egyszerű fejlesztői környezetben hozzák létre és többnyire még ma is soros porton, ritkábban USB-t vagy hálózati interfészt használva töltik fel az eszközre. Ez egyben azt is jelenti, hogy a terepi viszonyok közötti programmódosításuk nem igazán életszerű. A korlátozott ergonómia azt jelenti, hogy a PLC-k manapság megszokott megjelenítő funkciókkal és beavatkozási lehetőségekkel nem rendelkeznek. Állapot és státuszkijelzésre LED-eket, esetleg szegmensekből álló LCD panelt kapnak, amelyekkel és néhány gombbal egyszerűbb menürendszerek is kialakíthatóak, de ezek nem alkalmasak a teljes körű ellenőrzésre így a tesztelésre sem. Az utóbbi egy-két évben már kaphatóak 7-8 colos érintőkijelzővel szerelt PLC-k is, ám ezek inkább csak a kezelést teszik egyszerűbbé és látványosabbá, a PLC-k lehetőségeit nem terjesztik ki számottevően, ráadásul a legtöbb megjelenítő nem képes biztosítani a terepi katonai eszközöknél elengedhetetlen, minden időben való láthatóságot [12, 244 o.].

A nagyobb teljesítményű konténeres rendszerek vezérlése minden esetben számítógépen futó programmal megoldott. Ez egy fix konfiguráció esetében könnyedén megoldható lenne

[16] PLC – Programmable Logic Controller.

PLC-vel is, de a kivitelező cégeknek nincs végleges gyártmányuk illetve nem is terveznek ilyet, így nem tudnak lemondani a számítógépes megoldás nyújtotta rugalmasságról. Az ilyen nagy értékű berendezéseknél egyáltalán nem szokatlan, hogy nem egy uniformizált termék kis szériás sorozatgyártására rendezkednek be, hanem rendelésre, manufakturális jelleggel építik meg az egyes példányokat. A konténeres rendszerek egyik legfőbb vonzereje márpedig az, hogy az alkalmazók igényeinek (és pénzügyi lehetőségeinek) illetve a várható bevetési területeknek a függvényében számos konfiguráció kialakítható azonos bázison.

Az itt alkalmazott platform tekintetében manapság már igen nagy a választék. A szükséges számítási kapacitást, a könnyű bővíthetőséget és a képernyő-billentyűzet kombináció jelentette felhasználói ergonómiát akár Android-os alapon, vagy egy olcsó Raspberry-Pi miniszámítógéppel is lehetne biztosítani, de a gyakorlatban mégis a PC-s alap kínálja a legnagyobb lehetőségeket.

Az általam ismert valamennyi nagyobb teljesítményű katonai hibrid áramellátó berendezés egy Windows operációs rendszert futtató PC-t, egy esetben laptopot használ a rendszer vezérlésére. A szoftverek minden esetben egyedi fejlesztések, a gyártók legalább annyira titkolják a felépítésüket, mint a gyakran szintén egyedi akkumulátoraikét. Ezek a programok nyilvánvalóan sokkal részletesebb beállítási lehetőségeket tesznek lehetővé, és bár adott esetben még nem mentesek a hatásvadász marketingelemektől, valóban sok vizuális információt képesek nyújtani, amelyek segítségével tovább optimalizálható a rendszer működése.

Külön érdekesség, hogy a PC-s megoldások esetében mennyire eltérő buszrendszerekre fűzték fel a vezérléshez tartozó szenzorokat és beavatkozó elemeket a gyártók. Általában a legkézenfekvőbb megoldásként a PCI-E foglalatba illeszkedő bővítőkártyát preferálják a kivitelező cégek, de a laptopos megoldáshoz, USB-n keresztül vezérelt külön kapcsolódobozt konstruáltak. Az egyik gyártó pedig egy meg nem nevezett ipari buszrendszert alkalmazott, a masszív árnyékolt csavart érpáras kábelek alapján valószínűsíthetően a Profibus[17] egy verzióját, amit az anyacég profilja is sejtet.

A nyilvánvaló előnyök mellett a PC-k és kiegészítőik ára nem nevezhető igazi hátránynak, mivel a teljes rendszer bekerülési költségeihez képest eltörpülnek. A konténerekben az igen méretes és nem éppen könnyű akkumulátorok társaságában a kiterjedésük sem okozhat gondot. Igazából éppen a terepi működés követelményeinek való megfeleltetés jelent megoldandó konstrukciós problémát, így némi nehézséget.

HIBRID VILLAMOS RENDSZEREK VEZÉRLÉSE TEREPI KÖRÜLMÉNYEK KÖZÖTT

Informatikai eszközök terepi kivitele

A visszafogott üzemanyag fogyasztásból eredő műveleti előny biztosítása, mint fő célkitűzés, illetve számos egyéb elvárás is gyökeresen más megközelítést kíván a hibrid rendszerek tervezésekor és kivitelezésekor, amennyiben katonai felhasználásra készítenek fel egy ilyen eszközt. Ezt a fajta alkalmazói igényt számos paraméterben fel lehet fedezni, amelyek együttesen, mint „terepi kivitel” fogalmazódnak meg.

Fontos megjegyezni, hogy egy eszköz nem lesz terepi kivitelű attól, hogy katonák használják. Példának okáért a legtöbb manapság a katonák által használt PC egyszerű irodai eszköz. Katonai értelemben a terepi kivitel nem is egyfajta off-road képességet jelöl, hanem azt jelenti, hogy az adott eszköznek a hétköznapi infrastruktúrától távol, műveleti területen, „terepen” kell működnie. Ez a triviális környezeti viszonyok tűrésén kívül abban is jelentkezik, hogy ezek az eszközök nem számíthatnak a polgári megoldásokéhoz hasonló

[17] PROcess FIeld BUS. Európában kifejlesztett és elterjedt ipari automatizálási buszrendszer.

„gondos” bánásmódra, a használat során mindig alávetik őket a katonai célok teljesülésének. A terepi alkalmasságot meghatározó elvárások két fő részből állnak, a működés szempontjából káros külső tényezőkkel szembeni ellenálló-képességből, valamint a speciális igényeknek való megfelelésből.

A környezeti hatás szempontjából legfontosabb, általános követelmény-jellemzők, amelyekkel szemben egy eszköznek valamilyen szintű ellenállást kell tanúsítani, az alábbiak [12, 243-244 o.]:

- Víz, nedvesség
- Hőmérséklet
- Por, szilárd szennyeződések
- Légnyomás
- Vegyi anyagok
- Rázkódás
- Esés, ejtés, ütés, gyorsulás
- Kopás
- Elektromágneses sugárzás
- Extrém akusztikus hatások

Polgári alkalmazáskor ezek többségére nem is adnak meg tűrést, hiszen pl. a lakossági eszközöknél egyértelmű, hogy csak szobai környezetben vagy legalábbis az emberek komfortzónáján belül lesznek használva, míg az ipari berendezéseknél az adott feladatkörben kritikus paraméterekre adnak meg komolyabb elvárásokat. A terepi eszközöknél a terepi körülmények azt jelentik, hogy a bevetés valamennyi tervezett helyének klimatikus viszonyaival, a vétlen saját és az esetleges szándékos ellenséges tevékenységgel szemben is védelmet kell biztosítani – az ésszerű határokon belül.

A gyakorlatban általános terepi követelmény a minimum a fröccsenő víz elleni védelem, a teljes porvédelem, valamint a legalább -25 és + 50 °C fok közötti hőmérsékleten, tetszőleges relatív páratartalom melletti üzemképesség. A legtöbb terepi eszköznél elvárás a túlnyomás biztosítása nélküli légi szállíthatóság, illetve a terepjáró gépkocsin, harcjárművön történő szállítással járó rázkódás tartós elviselése is. A többi paramétert az eszköz jellegétől függően definiálják. Ruházati anyagoknál pl. igen fontos a kopás, a szakítószilárdság és a nyújthatóság, de nincs nagy jelentősége az elektromágneses sugárzásnak, ami viszont az elektronikus berendezéseknél, így a hibrid villamos rendszerek vezérlésénél is igen fontos, a működést befolyásolni képes tényező.

Az informatikai eszközöknél fontos követelmény, hogy burkolatuk legyen kopásálló és álljon ellen minden rendszeresített vegyi mentesítő anyagnak, valamint nyújtson mechanikai védelmet is. Többé-kevésbé szabvány követelmény, hogy a terepi informatikai eszköz maradjon működőképes három egymást követő 50 cm magasságból betonalapra történő ejtést követően, valamint extrém, akár 120 dB –t meghaladó akusztikus hatásnak kitéve is.

A környezeti hatások tekintetében a legtöbb alkalmazási környezetre vonatkozóan szabványok segítik a megfelelő tervezést és kivitelezés. A villamos működésű eszközök tokozására vonatkozóan a por-, a víz-, illetve a mechanikai védelem tekintetében közismert polgári besorolás az ún. IP védelem.[18] Egyszerűsége és ismertsége okán gyakorta alkalmazzák katonai területen is. Az „IP” jelölés utáni első szám a szilárd testek (por) szerkezetbe jutása elleni mechanikai védettség szinte, ahol a 0 védettség hiány, míg a 6 a tökéletes védettség. A második szám a vízállóságot jelöli, a 0 itt is a védettség hiánya, az 5, a kisnyomású vízsugár

[18] IP – International Protection Marking (Nemzetközi Védettség Jelölés). Leírását az USA Nemzeti Szabványügyi Intézete (ANSI) IEC 60529 szabvány tartalmazza, amelyet Magyarországon MSZ EN 60529.2001 jelzéssel honosítottak.

elleni védettség, a 8 az 1-3 méter mélységig a víz alatti használhatóság jelölése. A 9-es jelzésű készülékek nagy nyomású víztömeg alatt is működőképesek. Ritkábban használt a mechanikai szilárdságot jelölő harmadik szám 0-9, amelyet bizonyos tömegű tárgyak bizonyos magasságokból történő leejtésének energiáját adják meg, mint elviselendő esés-energiát [11, 31 o.], illetve a szabványhoz tartoznak még kiegészítő betűjelölések is.

Természetesen a többi környezeti tényező tekintetében is számos polgári szabványosítással foglalkozott testület adott ki mértékadó dokumentumokat, például az elektromágneses kompatibilitás (EMC) tekintetében is legalább 4-5 nagyobb szervezet gondoz több tucatnyi sztenderdet, ám ezeket katonai eszközöknél csak elvétve használják.

Magyarországon, ahogy sok más kisebb, szövetségi rendszerhez tartozó államnál, jelenleg nincsenek önálló katonai szabványok. Általában az ún. NATO STANAG[19]-eket honosítjuk és használjuk, ezek hiányában pedig gyakorta az USA MIL STD[20]-k jelenthetnek iránymutatást, amelyek egyébként is többnyire a STANAG-ek bázisát képezik. A hőmérsékleti viszonyokra és a páratartalomra vonatkozó ajánlásokat a STANAG 2895 tartalmazza, illetve jóval bővebben a MIL-STD-810 tárgyalja a klíma követelményeket. Az elektromágneses interferencia tekintetében nincs általános STANAG, az egyes eszközcsoportokra vonatkozó specifikációk tartalmazhatják ezeket, de az USA katonai szabványai közül a MIL-STD-461 általánosságban is felöleli ezt a kérdést. Mechanikus ellenállóságra szintén generális érvényű STANAG, az USA szabványok közül a MIL-STD-883 foglalkozik vele.

A nem környezeti viszonyokból fakadó terepi elvárásokat az eszköz jellege és az alkalmazás helye együttesen határozza meg, így igen sokfélék lehetnek. Villamos energiaellátó berendezések vezérlése esetében én az alábbiakat emelném ki:

- Egyszerű, ergonomikus kezelés, nagyfokú automatizáltság, a vétlen hibák elleni védelem
- Nagyfokú mobilitás, gyors telepíthetőség és bonthatóság, kompakt méretek és kis tömeg
- Minimális karbantartási igény, magas hibatűrés
- Vizuális álcázhatóság, minimális zaj, csekély kompromittáló kisugárzás
- Távvezérlés lehetősége

Ezek többségére nem léteznek szabványok, a katonai berendezések esetében a mindenkori alkalmazói igények alapján a megrendelők írják elő az eszköz harcászati-műszaki paramétereiben. Kivételt képez az álcázás, álcázhatóság követelménye. Minden tábori használatú haditechnikai eszköz esetében alapvető elvárás az álcafestés, ami Magyarországon a RAL 6031 jelzésű matt zöld színt jelenti. Mivel az áramellátó rendszereken érzékeny adatok nem találhatók, a felderítésük pedig vizuálisan jóval egyszerűbb, a kompromittáló kisugárzás megengedett mértékét nem tartom szükségesnek definiálni.

A hibrid rendszerek vezérlése terepi kivitelben

A CL15 gyakorlaton szereplő katonai hibrid villamos energia ellátó eszközök elég pontosan reprezentálták a jelenlegi európai technológiai színvonalat és a fejlesztés trendjeit. Az ott a vezérlésen alkalmazott védelmi megoldások is jó áttekintést adnak a létező és működő rendszereken fellelhető korszerű technikákról.

Ahogy maguk a berendezések is két nagyobb csoportba voltak sorolhatók, úgy a terepi körülményeknek való megfeleltetés tekintetében is elsősorban két eltérő elképzelés mentén kerültek kialakításra a vezérlés elemei. Annyiban mérettől és teljesítménytől függetlenül

[19] STANdardization AGreement. NATO szabványosítási megállapodás, amelyet jóváhagyás után valamennyi tagországnak alkalmaznia kell.
[20] MILitary STandarD – Katonai szabvány. Az USA védelmi minisztériuma által kiadott szabványok.

minden kivitelező megegyezett, hogy a szenzorok és mágneskapcsolók esetében nem alkalmaztak különleges védelmi megoldásokat. Az alkalmazott érzékelők minden esetben átlagos, kereskedelmi forgalomban kapható, de ipari kivitelű darabok voltak. Ezek valójában olyan egyszerű szerkezetek, hogy a megfelelő szerelés esetén semmilyen körülmények között nem képezhetik a vezérlés gyenge pontját. A felhasznált mágneskapcsolók is minden esetben kereskedelmi termékek voltak, nem egyszer az anyacég gyártmányai. Ezek a szerkezetek működési elvükből és a kiforrott technikából adódóan a környezeti hatások egy jelentős részére érzéketlenek. Egy erős ütés, a por vagy a víz természetesen tönkretehetné őket, de akár IP 685-ös tokozású kivitelben is viszonylag olcsón beszerezhetők, amelyek a megfelelő szerelés esetében önmagukban garantálják a terepi körülményeknek való megfelelést.

A hagyományos szolár-utánfutók egyikén sem alakítottak ki külön védett helyet a vezérlés számára. Egész egyszerűen a megfelelő IP védettséggel rendelkező PLC-t és mágneskapcsolókat használtak fel, amelyeket más tervezési elvek mentén helyeztek el az alvázon. A kábelek por és vízálló bevezetését a PLC-k és kapcsolók saját tömszelencés bevezetései biztosították. A kézi kapcsolók gumisapkás kivitelűek voltak. A PLC-k és a mágneskapcsolók annyira elnyűhetetlen eszközök, hogy néhány esetben közvetlenül a komoly rázkódásnak és vibrációnak kitett alvázra szerelték őket, mindössze egy vékony gumialátétet használtak a behatások csillapítására. Ahol a vezérlés elemei az alváz olyan helyére kerültek, ahol a ki voltak téve a felfröccsenő sárnak, ott a tisztíthatóság érdekben elhelyeztek egy fém vagy műanyag pajzsot, amelyek viszont hangsúlyozottan nem jelentettek önmagukban semmiféle védelmet, esetleg annyiban járultak hozzá a működés fenntartásához, hogy a passzív hűtések hatékonyságát a hűtőbordákra száradt sár nem volt képes lerontani.

A konténeres bázisú berendezések esetében a konténeren belül semmilyen víz- vagy por elleni védelmet nem alkalmaztak, azt maga a konténer biztosította. A konténerek ajtói erős gumiszigetelést kaptak és legalább 20 cm-es lábakon álltak, így azokba sem por, sem víz nem juthatott semmilyen körülmények között. A kábelátvezetések természetesen megfelelően méretezett tömszelencéken keresztül történnek. Az aktív elemek hűtésére sem alkalmaztak külön technikát, mivel valamennyi konténer légkondícionált volt. Ennek oka nem a kezelőszemélyzet kényelmének biztosítása volt, hiszen ezeket az eszközöket alapvetően teljesen automatikus működéshez tervezték, hanem az akkumulátorok hatékonyságát kívánták így biztosítani.

A CL15 gyakorlaton bemutatott hibrid eszközök mindegyike (még a szolár-utánfutók is) nagy energiasűrűségű lítium-polimer akkumulátorokat alkalmazott az energia tárolására. Ezek viszont a legtöbb ilyen eszközhöz hasonlóan nagy hidegben sokat veszítenek a kapacitásukból, -20 °C alatt akár a névleges töltésük 80-90 %-át is elveszíthetik [13, 638-639 o.]. A szolár-utánfutók esetében erre nem is találtak megoldást, extrém hidegben egyszerűen jobban hagyatkoznak az aggregátorokra. A táborok villamos ellátásának szívét jelentő nagyobb rendszereknél ez már komolyabb problémát jelentene, ezért a gyártók vállalták a klimatizálás extra energiaigényét, amely még mindig jóval szerényebb veszteséget jelent, mint amit az akkumulátorok drasztikus kapacitásvesztése okozna.

A fentiek okán a vezérlés algoritmusát adó PC-k védelme is jelentősen egyszerűsödött, hiszen lényegében már csak a mechanikus hatásoktól kell azokat óvni azokat. Csupán érdekesség, hogy az acél konténer igen jelentős, az épületekét jóval meghaladó védelmet képes biztosítani az elektromágneses hatások ellen is. A konténer, mint uniformizált bázis ellenére, mindegyik PC kialakítása egyedi volt. Az egyik gyártó a konténer belső falára rögzített konzolon egy erősített kivitelű ipari PC-t helyezett el. Egy másik csupán egy közönséges brand PC-t használt erre a célra, bár hangsúlyozták, hogy a vibrációra, ütődésekre érzékeny merevlemezt korszerű SSD-re cserélték, illetve ügyeltek a jó láthatóságot biztosító nagy fényerejű IPS kijelzőre. A harmadik megoldás egy egyszerű polgári kivitelű laptop volt. A cég jelezte, hogy a CL15-re összeállított konfigurációhoz akkor csupán ez állt a

rendelkezésükre, de a vezérlő szoftvere minden probléma nélkül telepíthető a katonai laptopokra is.

Két mobil és egy „köztes” berendezést külön is említek, mert tervezésüknek és kivitelezésüknek van néhány sajátossága, ami némileg eltér a két fő vonaltól, és ez a vezérlésben is tetten érhető. Egy osztrák cég gyártja a nagyon innovatív „okos virágot”. Ez tulajdonképpen egy négy ember által mozgatható műanyag doboz, amelyből gombnyomásra virágszerűen kiemelkedik, majd szirmokhoz hasonlóan kinyílik egy sor napelem. A mintegy 2,5 m^2-nyi PV felület ebben a kategóriában egyedülálló módon, egy GPS vevő segítségével követi a napot a pályáján, hogy a napsugarak mindig az optimális merőleges szögből érjék. A viszonylag kis alaphoz képest nagy felület erős szélben még a rögzítés ellenére is instabillá válhat, ezért a 70 km/h –át meghaladó szél esetén a virág automatikusan bezáródik.

Ezek a plusz képességek nem jelenthetnek igazán nagy megterhelést a vezérlés számára, de a rendszer kiegészül még néhány szenzorral, illetve számos szervomotorral is. Az osztrák mérnökök nem akarták elárulni, hogy milyen informatikai eszköz képezi a vezérlés központját, de szinte biztos, hogy nem egy egyszerű PLC, hanem egy mikroszámítógép, mivel egyetlen GPS helyadat alapján kell kiszámítani a PV felület mindenkori optimális beállítását két tengely mentén, ami egy viszonylag számításigényes feladat. Annyi tudható, hogy a vezérlés alkatelemei nem IP védettek, az egészet egy több csavarral és gumigyűrűvel lezárt üreg rejti. Mivel a rendszer működése alapesetben teljesen automatikus, csak néhány kapcsoló és visszajelző került védett kivitelben a burkolatra – de szállításkor, vagy telepített állapotban ezeket is fedél takarja.

Az egyik brit cég rendkívül ötletesen gondolta újra a szolár-utánfutót. Nem hagyományos merev üvegtáblákat[21] kell kihajtogatni az alvázról, hanem egy dobozszerű felépítményben szőnyegszerűen van felcsavarva a mintegy 70 méternyi flexibilis napelem.[22] A felépítmény biztosítja a PLC alapú vezérlés megfelelő védelmét is, ugyanakkor a kezelőszervek a szigetelt ajtók nyitása után könnyen, ergonomikusan hozzáférhetőek. Ez a koncepció jóval több lehetőséget hagy a különféle kiegészítők elhelyezésére, így a szolár-utánfutók között messze ez a megoldás volt a legjobban skálázható és modulokkal az igényekhez igazítható, amelyhez természetesen a vezérlést is adaptálták.

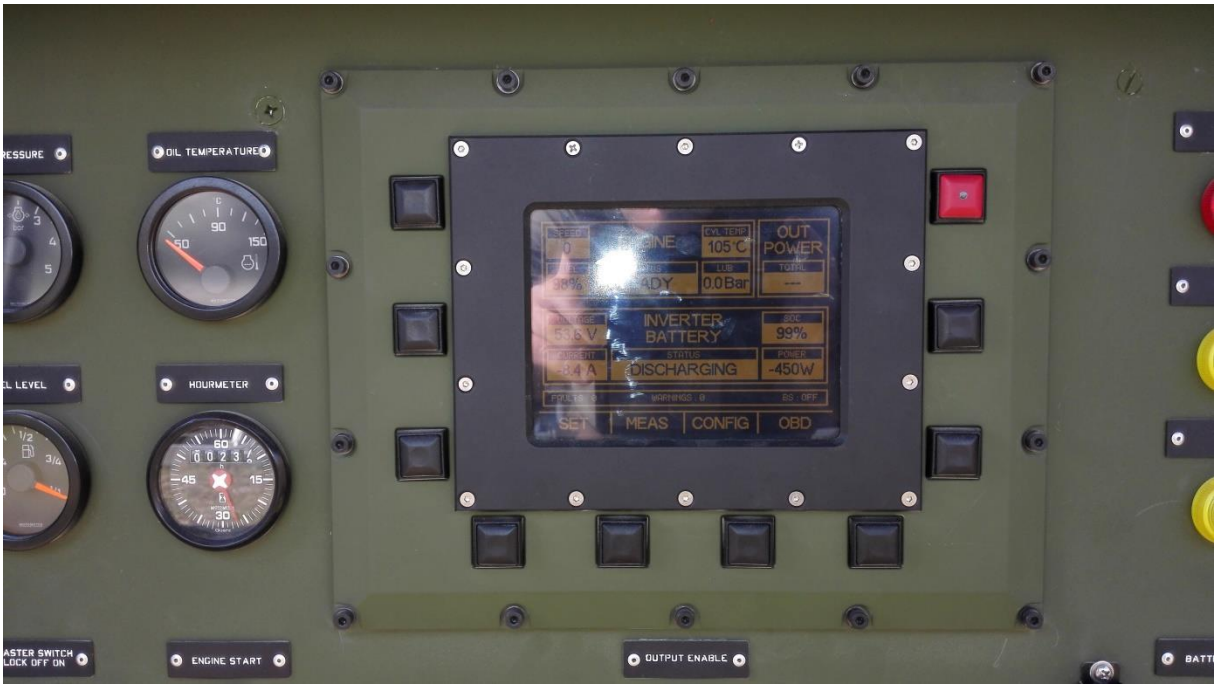
A gyakorlaton a Görögországot egyedül képviselő cég terméke minden szempontból egyedülálló volt. Lényegében ez volt az egyetlen megoldás, ami nem egy civil rendszer módosításával jött létre, hanem eleve katonai célra szánták, ami számos részletben megmutatkozott. Teljesítménye alapján inkább a szolár-utánfutók kategóriájába tartozott, de nem volt mobil, a kb. 1 m^3-es kompakt berendezés targoncás, darus és helikopteres emelésre is fel volt ugyanakkor készítve. A görög szakemberek elsősorban automatikusan működő létesítmények, pl. híradó állomások ellátásához optimalizálták. A rendszer szintén unikális módon nem egy külső aggregátort használt, hanem azt a kompakt egység tartalmazta, igazából csak a napelemek elhelyezése nem volt szabott. A tervezésnél semmilyen későbbi bővíthetőségnek nem hagytak helyet, viszont minden olyan módszert alkalmaztak, ami elősegítette a tartós üzemet. Az alkalmazott akkumulátorok az átlagosnál kisebb energiasűrűségű, de a szélsőséges hőmérsékleten jóval megbízhatóbb Lítium-ferrofoszfát típusba tartoztak [8, 95. o.].

A vezérlés lelke egy mikroszámítógép, amely önmagában is IP67-es védelmi szinttel büszkélkedhet és valamennyi többi rész szintén önmagában is IP67-es minősítéssel bír, mindezeken túl a legkritikusabb részeket még duplikálták is. Az energetikai folyamatok

[21] A szilícium poli-, illetve monokristályos napelemtáblák a legelterjedtebbek és a legolcsóbbak. A legkorszerűbb többátmenetes típusok hatásfoka megközelíti a 40 %-ot [1, 49 o.].

[22] Általában különleges félvezetőkből, pl. réz-indium-szelenidből készülnek. Hatásfokuk jelenleg még 20 % alatt van, de számos olyan előnyös tulajdonsággal bírnak, mint a kis tömeg és az olcsó gyártástechnológia, sőt még jelentős fejlesztési tartalékok is vannak a technológiában [1, 50 o.].

menedzselése nem kívánta volna meg a számítógép alkalmazását, de az algoritmus az átlagosnál sokkal több önellenőrző és konfigurációs, sőt önjavító rutint is tartalmaz. A rendszer kezelésére egy nagy fényerejű, akár direkt napsütésben is látható monokróm kijelző és néhány vízálló billentyű szolgál, amelyeket egy masszív fémajtó mögé rejtettek. A görög tervezők alapos munkát végeztek, a cég 5000 órát meghaladó MTBF[23]-et adtak meg a készülékre.



4. ábra: a görög hibrid rendszer vezérlőpanele

ÖSSZEGZÉS

Mivel a jelenleg ismert villamos áram termelésre alkalmas technológiák közül egyedül az aggregátoros megoldás az, ami minden időben képes terepi viszonyok között is ellátni a katonai egységeket, alkalmazásukról nem mondhatunk le. Ugyanakkor mind a várható műveleti, mind a gazdasági előny okán szükséges a terepi viszonyok között is kiaknázható megújuló energiaforrások bevonása a villamos energiatermelés rendszerébe. A két technológia integrációjából születő hibrid berendezések képesek a kétféle eljárás előnyös tulajdonságait egyesíteni, így hosszabb távon a nagyobb bonyolultság és a magasabb bekerülési költség ellenére is megtérülő (műveleti szempontból is) az alkalmazásuk. Az optimális működést a viszonylagos bonyolultság okán kizárólag korszerű, teljesítményében megfelelően skálázott informatikai eszközökkel lehet biztosítani. Az ilyen eszközöket mindenképpen úgy kell tervezni és alkalmazni, hogy képesek legyenek elviselni mindazt a környezeti illetve a katonai feladatrendszerből adódó romboló hatásokat, amelyeket a rendszer többi eleme is.

A kisebb méretű és teljesítményű hibrid berendezések jellegükből fakadóan kevesebb lehetőséget kínálnak a modularitás és a bővíthetőség terén, ezért vezérlésükhöz tökéletes megoldás a viszonylag olcsó, de megbízható PLC, míg a nagyobb rendszerek vezérléséhez szükséges a teljes értékű számítógépek teljesítménye és az általuk biztosított egyedi konfigurálhatóság. Mindkét csoport esetében járható út az informatikai eszközök a rendszer

[23] Mean Time Between Failures – Meghibásodások között eltelt átlagos idő. A készülékek megbízhatóságára vonatkozó általános mérőszám.

többi elemétől független, védelmének egyedi kialakítása, illetve az is, hogy a rendszer más elemeivel együtt, esetleg az általuk már biztosított megoldásokat használva alakítunk ki megfelelő védettséget.

Magyarország viszonylatában a teljes kiépítésű konténeres megoldások alkalmazásának jelenleg nincs realitása, mivel az ország valamennyi katonai objektumában, még a gyakorlótereken is elérhető a távvezetékes áramszolgáltatás, így nem használható ki a hibrid rendszerek által biztosított előnyök egyike sem. Tartós missziós szerepvállalás esetében pedig viszonylag ritka az önálló magyar jelenlét, szinte mindig nemzetközi kötelék részeként ténykednek a magyar katonák, így az önálló áramellátás igénye itt sem fogalmazódik meg. Mindebből az következik, hogy a konténeres megoldásokkal kapcsolatos terepi informatikai eszközök tekintetében Magyarországnak jelenleg nem kell követelményeket támasztani.

Lényegesen nagyobb az esélye annak, hogy autonóm működésű híradó állomások ellátásához, illetve a szakcsapatoknál rendszeresített tábori eszközökhöz kiegészítő lehetőségként merül fel a hibrid rendszerek alkalmazásának igénye. Ilyen jellegű berendezés konstruálására nem mellesleg a hazai ipar is képes lehet, míg a komplexebb konténeres megoldások valószínűleg meghaladják a magyar cégek lehetőségeit. A vezérlés elemeinek elosztott egyedi védelme, illetve a központosított elhelyezés és védelem kialakítása az ilyen mobil eszközökön terepi követelmények szempontjából egyenértékű, valószínűleg az egyik vagy másik preferálásával elérhető árelőny is eltörpül a teljes berendezés bekerülési költségéhez képest. Amennyiben más konstrukciós szempont ezt nem írja felül, én rendszertechnikai szempontból mégis a centralizált vezérlés és a hozzá tartozó védelem kialakítását tartom előnyösebbnek, mivel a kezelés így ergonomikusabb, a karbantartás és javítás némileg egyszerűbb.

Felhasznált irodalom

[1] Végvári Zsolt: A megújuló villamos-energiaforrások felhasználásának lehetőségei harctéri körülmények között, *Hadmérnök*, 1 (2016), 41-55

[2] Hegedűs Ernő, Fröhlich Dávid: Az R/7 rádióállomás és a Csonka áramfejlesztők gyártásának és alkalmazásának körülményei, különös tekintettel a sereglovasság híradó eszközeinek üzemeltetésére (1927-1945). *Katonai Logisztika*, 1 (2014), 258-266

[3] *Chapter 15: Fuels, Oils, Lubricants and Petroleum Handling Equipment – Military Fuels and the Single Fuel Conception,* NATO Logistic Handbook, 1997

[4] Christopher Helman: For U.S. Military, More Oil Means More Death*, Forbes*, November 12, 2009. http://www.forbes.com/2009/11/12/fuel-military-afghanistan-iraq-business-energy-military.html (a letöltés ideje: 2015. 11. 23)

[5] Nanette Cazaubon: A german engineering system brings NATO closer to smart energy targets, *The European Security and Defence Union*, 23 (2016), 56-57

[6] Végvári Zsolt: A Smart Energy koncepció és eszközei a CL15 logisztikai gyakorlaton, *Haditechnika*, 6 (2015), 30-34

[7] Gregor Hoogers (Eds): *Fuel Cell Technology Handbook*, CRC Press, London, 2003

[8] Végvári Zsolt: Akkumulátorok a gyalogos lövészkatonák felszerelésében, a fejlesztés lehetséges irányai, *Katonai Műszaki Közlöny*, 2 (2016), 85-101

[9] Pfisterer GmbH expo és konferencia nyomtatványai

[10] Tóth Péter, Bulla Miklós, Nagy Géza: Energetika, *Digitális Tankönyvtár*, 2011

[11] ANSI/IEC 60529-2004 Degrees of Protection Provided by Enclosures (IP Code), *National Electrical Manufacturers Association*, Rosslyn, 2004

[12] Munk Sándor: Katonai informatika a XXI. század elején, Zrínyi, Budapest, 2007

[13] Yan Ji, Yancheng Zhang, Chao-Yang Wang: Li-Ion Cell Operation at Low Temperatures, *Journal of The Electrochemical Society*, 4 (2013), 636-649

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Holicza Péter
holicza.peter@rh.uni-obuda.hu

CIVILIZÁCIÓS TÖRÉSVONALAK EURÓPÁBAN: MAGYARORSZÁG ÉS SZOMSZÉDAI A HOFSTEDE-DIMENZIÓK TÜKRÉBE

Absztrakt

Samuel P. Huntington szerint a következő időszakot a világ civilizációs törésvonalai mentén kirobbanó konfliktusok jellemzik majd, aminek a nyugat is elszenvedője lesz. A világ fő civilizációinak térképén a nyugat keleti határa megegyezik Magyarország, illetve a magyarlakta területek keleti határaival. A teória alapján a kelet-közép és kelet-európai kulturális, vallási határvonal (is) jövőbeni összecsapások helyszíne lehet. A Huntingtoni elmélet, a közelmúlt európai eseményei és a Közel-Keleten zajló folyamatok tükrében a téma igen nagy aktualitással bír. Magyarország és szomszédos országainak további elemzése a Hofstede 6-D modell segítségével, új ismeretekkel szolgál az említett törésvonal létének vitatására vagy megerősítésére a Kárpát-medence térségében.

According to Samuel P. Huntington, the biggest threat to Western civilization is a coming period that will be characterized by conflicts erupting as the world's civilizations reach their breaking points. The conflicts of the future will occur along the cultural lines separating civilizations. Huntington drew the Eastern Boundary of Western Civilization around Hungary in Central Eastern Europe. Neighbouring countries from the South-East belong to the other side of the map of civilizations. It also might be a battle line of the future (according to the theory), necessary to emphasize the importance of cultural awareness and review of different views about the region. This paper intends to link Huntington's theory with Hofstede's measurements on the Hungarian and neighbouring countries' culture in order to find out possible correlations and differences that could confirm or doubt the existence of such fault line in the Carpathian Basin.

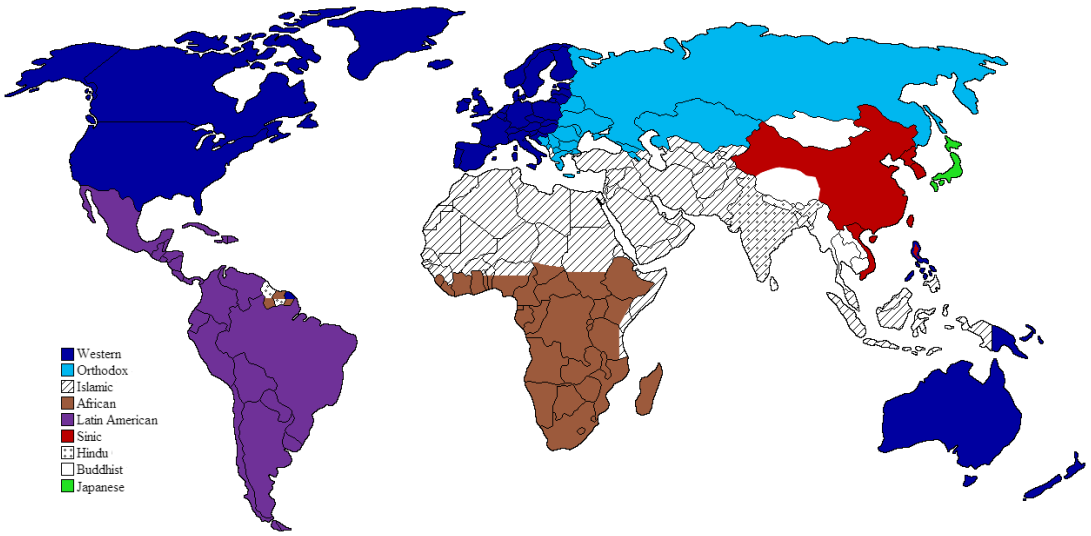
Kulcsszavak: *Huntington, Hofstede, Magyarország, kulturális elemzés, civilizációk ~ Huntington, Hofstede, Hungary, cultural analysis, civilizaitons*

A HUNTINGTONI CIVILIZÁCIÓK

Az emberi evolúció egy pontján a kölcsönös megértés, egymástól való függőség és társas együttélés rendkívül hasznos életmóddá vált. Kisebb elkülönült csoportokból közösségek, majd társadalmak és civilizációk alakultak. Az emberi pszichológia fejlődésének e szakasza még ma is rengeteg történészt, antropológust és társadalomtudományi szakértőt foglalkoztat.

A civilizáció szót említve leggyakrabban a régmúlt nagy civilizációira gondolunk, melyek mindmáig lenyűgöznek bennünket látványos teljesítményeikkel, pl.: inka, azték. római, perzsa, ókori görög, kínai, maja, egyiptomi, Indus-völgyi, stb. civilizációk. Maga a szó valószínűleg a latin civis szóból származik, jelentése: polgár. Európában a kultúra fogalom előtt már a XIV-XV. században előfordult a civilitas kifejezés, miszerint az emberek politikai, szociális, gazdasági, vallási nézeteik, illetve helyzetük szerint önként csoportosultak [1]. Az Oxford English Dictionary a civilizációt az emberi társadalom már egy fejlett szintjével azonosítja [2]. Huntington civilizáció alatt a legmagasabb kulturális csoportosulás, a kulturális identitás legtágabb szintjét érti, ez alapján 9 civilizációt különböztet meg a közös célok, nyelv, történelem, vallás, szokások, intézmények és öntudat szerint, melyek határvonala nem mindig követi az országhatárokét [3].

A XVI-tól a XIX. századig a birodalmi terjeszkedés mellett az európai civilizáció is nagyobb teret nyert, melynek során gyakran régebbi és meghatározó helyi kultúrák is áldozatul estek. A XX. században már más erők dolgoztak, az ideológia került főszerepbe, ami két különböző koncepció kiterjesztését jelentette: az amerikai kapitalizmus és az orosz kommunizmusét. A hidegháború alatt alakult ki a három világ: Első világ (kapitalizmus); Második világ (kommunizmus) és a Harmadik világ azokkal az országokkal melyek sem a nyugati hatalmak, sem az egykori keleti blokk országaival nem kötöttek szövetséget. Az ezzel egy időben történő tömeges tájékoztatás és propaganda (rádió, televízió, mozi) lehetővé tette az egyes régiókban népszerű nézetek és kultúra exportálását a világ többi tájára.



1. ábra: A világ civilizációi 1990 után „The World of Civilizations: Post-1990". Forrás: [3]

A hidegháború végével megszűnt a vasfüggöny, ami Európát politikailag és ideológiailag megosztotta. Mivel ezek a divíziók többé már nem relevánsak, Huntington az országokat azok politikai és gazdasági rendszerük, fejlettségük helyett a civilizációs és kulturális szempontrendszer szerint kategorizálta. Az 1. térkép szerint a következő világrégiókat különbözteti meg egymástól, mint fő civilizációk: nyugati (keresztény), ortodox (keresztény) iszlám, hindu, afrikai, latin-amerikai, kínai, buddhista és japán [4].

A civilizációk közti törésvonalak látszólag a hidegháború politikai és ideológiai határait helyettesítik. Európa a nyugati és az ortodox kereszténység között válik megosztottá, valamint napjainkban már az iszlám is nagy szerepet játszik. A civilizációs különbségek nem csupán valósak, azok alapvetőek. Huntington szerint a civilizációs öntudat egyre fontosabbá válik a jövőben, és a világot a fő civilizációk interakciói formálják majd. Előrejelzi: A jövőbeni konfliktusok a civilizációs törésvonalak mentén alakulnak majd ki [5].

A NYUGAT KELETI HATÁRA

Európára fókuszálva, a legfontosabb választóvonal a nyugati kereszténység keleti határa lehet, ahogy William Wallace meghatározta (2. térkép) [6]. Ez a határvonal választja el Finnországot és a balti államokat Oroszországtól, valamint két részre osztja Belorussziát és Ukrajnát azok nyugati keresztény és keleti ortodox lakossága szerint. Említésre méltó, hogy Ukrajna egyéni elemzése során Huntington előre jelezte egy háború valószínűségét az említett törésvonal mentén: Míg az etatista megközelítés egy orosz-ukrán háború lehetőségére hívja fel a figyelmet, a civilizációs szempont ezt minimalizálja, és inkább egy belső konfliktust, szétválást jelez, ami erőszakosabban megy majd végbe, mint Csehszlovákiában, de közel sem annyira véresen, mint Jugoszláviában [7]; [8].

Az európai törésvonallal folytatva, Wallace térképén látható, hogy a főleg magyarlakta Erdély szintén le van választva Románia keleti területéről, így a nyugati civilizáció részét képezi. Dél-Európában a törésvonal elválasztja Szlovéniát és Horvátországot a többi balkáni államtól. Felfedezhető, hogy ez megegyezik a Habsburg és az Ottomán Birodalom történelmi határával. Bosznia és Szarajevó, Szerbia és Albánia példáin láthattuk az ortodox és muszlim országok északi határainál kirobbanó konfliktusokat, csakúgy, mint az oroszok és muszlimok esetében Közép-Ázsiában.

Az északi és nyugati területeken élő népek főleg katolikusok vagy protestánsok, osztoznak a közös európai történelmen, mint például a reformáció, polgári és ipari forradalmak, stb. Ezek az országok gazdaságilag jobban teljesítenek, és nagyobb valószínűséggel építenek, tartanak fent egy stabil demokratikus politikai rendszert, mint a törésvonal keleti és déli vonzásában élő (ortodox és muszlim) népek. Huntington szerint az ideológia vasfüggönyét a kultúra bársonyfüggönye helyettesíti, ami a legmeghatározóbb választóvonalat jelenti napjainkban [9]; [10].

Magyarország és egykori területei, déli és keleti szomszédjai Huntington civilizációs törésvonala mentén helyezkednek el. Ahogy az 1. ábrán is látható, a hét szomszédos országból három teljesen, vagy részlegesen (2. ábrán) elválasztott a törésvonal által. Mivel a történelmi tradíciók, kulturális értékek és az idealizált jövőkép eltérőek, a civilizációk összecsapása-elmélet alapján e területek jövőbeni konfliktusok színterei lehetnek [11].

A hipotézis és a konfrontáció valószínűségének igazolására az aktuálpolitikai helyzettől függetlenül, további kulturális elemzést javaslok egy eltérő szempontrendszer segítségével. A szóban forgó országok kulturális személyiségjegyeinek összehasonlításához Geert Hofstede 6-D modelljét használom.

2. ábra: A nyugati kereszténység keleti határa. Forrás: [6]

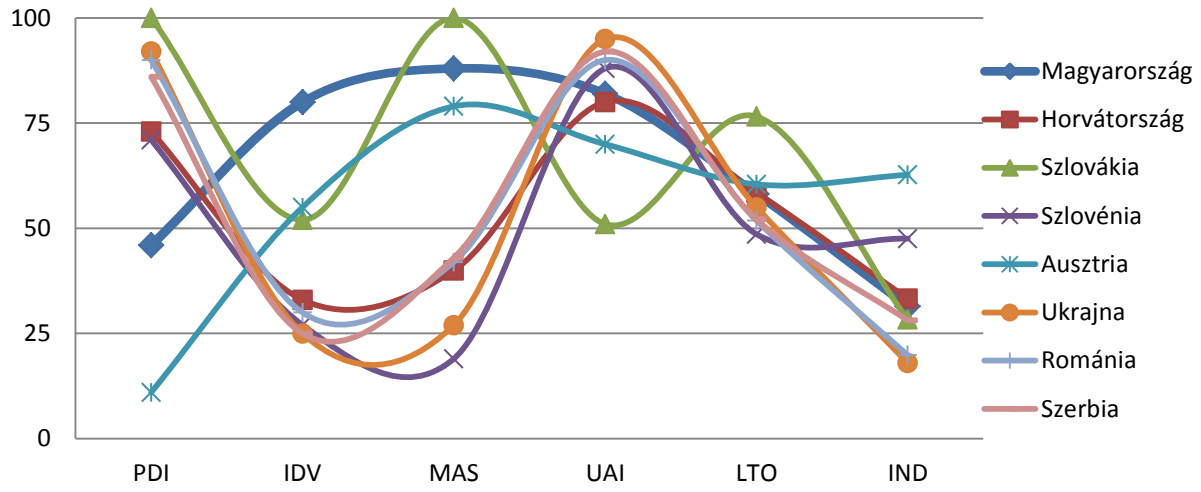
HOFSTEDE KULTÚRÁLIS DIMENZIÓI

A kultúra egy rendkívül összetett fogalom, amelynek elemzése során már az 1952-es kutatások több mint 100 definíciót írtak össze, ám egységes és mindenki által elfogadott meghatározása a mai napig nem létezik. A kulturális elemzés terén Professzor Geert Hofstede folytatta az egyik legátfogóbb kutatást. Szerinte a kultúra "a gondolkodás kollektív programozása, amely megkülönbözteti egy csoport vagy egy kategória tagjait másoktól… a környezet változásaira adott emberi válaszokat befolyásoló közös jellemzők összessége". Kultúra mindaz, amit az emberek tesznek, gondolnak, és amivel rendelkeznek, mint a társadalom tagjai [12].

A Hofstede féle 6-D modell a nemzeti kultúrákat teszi mérhetővé és összehasonlíthatóvá hat dimenzió segítségével:

- Hatalmi távolság (Power Distance Index – PDI): Az emberek közötti egyenlőtlenség olyan mértéke, melyet még elfogadhatónak tartanak. Az alacsony hatalmi távolságot viszonylag kis egyenlőtlenség, konzultatív vezetési stílus jellemzi, még a nagyobb hatalmi távolság komolyabb egyenlőtlenséget mutat, mely társadalmak vezetői gyakran autokraták, beosztottjaik pedig kevésbé mernek ellentmondani (egzisztenciális egyenlőtlenség).
- Individualizmus - kollektivizmus (Individualism vs. Collectivism - IDC): A különálló egyén, vagy a csoport tagjaként folytatott tevékenység előnyben részesítése. A kollektivista társadalmakban fontos a közösség, egymás segítése, az egyén alárendeli magát a csoportérdeknek, ezzel szemben az individualista társadalom az egyént, a „saját lábán is megállót" preferálja [13].
- Férfiasság - nőiesség (Masculinity vs. Femininity - MAS): A nemi szerepekhez társított magatartás alapján számított index. Elkülönülnek a férfias jegyek, mint a teljesítmény, siker, versengés, kitartás, illetve a nőies, mint a gyengédség, szolidaritás, támogatás, az emberi kapcsolatok. A férfias társadalmakban ezek a szerepek jobban elkülönülnek, mint a nőiesben, ahol több átfedés fedezhető fel.
- Bizonytalanság kerülés (Uncertainty Avoidance Index - UAI): Megmutatja, hogy egy társadalomban mennyire tekintik fenyegetésnek a kétes, illetve ismeretlen helyzeteket, mennyire igénylik a strukturált rendszereket, írott vagy íratlan szabályokat.
- Jövőorientáció (Long Term Orientation vs. Short Term Normative Orientation - LTO): a társadalom időorientációját a hosszú vagy a rövid távú gondolkodás határozza meg. Alacsony értéknél a társadalmak a jelenre, vagy a közeljövőre koncentrálnak, jellemző a megszokott gyakorlatok alkalmazása, a változásoktól való félelem. A hosszú távon gondolkodók inkább a jövőre koncentrálnak, kevésbé ragaszkodnak a múlthoz, és vállalkozó szelleműek.
- Engedékenység - korlátozás (Indulgence vs. Restraint - IND): Mennyire próbálják meg kontrollálni vágyaikat, impulzivitásukat. A relatíve kis kontroll irányába hajló un. megengedő és a relatíve erős kontrollal jellemezhető korlátozó kultúrák jelentik [14]; [15].

Az 3. ábrán Magyarország és szomszédos országainak kulturális mérőszámai rajzolódnak ki a fenti dimenziók alapján.



3. ábra: Magyarország és szomszédos országainak 6-D modellje. Forrás: saját szerkesztés, adatok: [16]

Ahogy az 3. ábra mutatja, a vastagított sötétkék vonal rajzolja ki a magyar értékeket, ami a Huntingtoni teória szerint a nyugati civilizáció része Ausztriával, Horvátországgal, Szlovákiával és Szlovéniával egyetemben. Románia, Ukrajna és Szerbia a törésvonal másik oldalán helyezkednek el, azok ortodox és részben iszlám (a szerbiai albán és bosnyák kisebbség) lakosságának okán. Az elmélet teljes körű igazolásához, a nyugati és az ortodox civilizációkhoz tartozó országoknak hasonló trendvonalakat kell mutatniuk, azonban Hofstede modellje (részben) újraosztotta ezeket a csoportokat.

A hat kulturális dimenzió közül a hatalmi távolság (PDI), az individualizmus (IDV) és a férfiasság (MAS) mutatják a legnagyobb eltéréseket. Ezek az értékek egyértelműen elválasztják Ausztriát, Magyarországot és Szlovákiát a többi országtól. Horvátország, Románia, Ukrajna, Szerbia és Szlovénia rendkívül hasonló értékeket mutat mind a hat index tekintetében. Részletesebb bontásban látható, hogy az új, kisebb (nyugati) csoportot képviselő országok között is eltérést mutatnak a szlovák értékek. Egyezőség csupán az individualizmus terén lép fel Ausztriával, valamint az engedékenység – korlátozás (IND) együtthatója alapján Magyarországgal. A teljes régiót vizsgálva, a legnagyobb eltérést a hatalmi távolság indexe (Ausztria- minimális, Szlovákia- maximális), és a maszkulinitás (Szlovénia- minimális, Szlovákia- maximális) mutatja. A legegyenletesebb értékekkel a bizonytalanság kerülés (UAI) és a jövőorientáció (LTO) indexei rendelkeznek az ábrán látható országok között. A magyar függvénygörbe által felvett értékek alapján, Magyarország kultúrája az ausztriai és a horvát jellemzőkhöz áll a legközelebb.

ÖSSZEGZÉS

Figyelemre méltó, hogy a nyugati civilizáció csoportjába sorolt országok (Ausztria, Horvátország, Magyarország, Szlovákia és Szlovénia) között egyértelmű kulturális különbségek fedezhetőek fel. A 6-D elemzés értekei alapján kirajzolódó trendvonalak Horvátországot és Szlovéniát a Huntingtoni törésvonal ortodox oldalához tartozó Romániához, Ukrajnához és Szerbiához csatolják. Szlovákia különbözik a leginkább a régiós átlagértékektől, amit Ausztria reprezentál.

Magyarországra fókuszálva, a hatból mindössze három index (PDI, IDC, MAS) mutat szignifikáns eltérést a déli és keleti oldalról szomszédos országoktól. A további mutatók

(UAI, LTO, IND) közel azonosak a törésvonal mindkét oldalán. Hofstede 6-D modellje hozzávetőlegesen 50%-os eltérést mutatott Magyarország és az ortodox civilizációhoz tartozó szomszédjai között. Ennek értelmében a Közép-Európát keletről határoló törésvonal léte bizonyítást nyert, azonban az eredmények vegyesek. Kijelenthető, hogy számos érv alapján, pl.: közös kulturális értékek, környező országok magyarlakta területei, keresztény vallás, migrációs hatás, stb. a kárpát-medencei törésvonal áthidalható. Keleti fenyegetettség esetén is kisebb a valószínűsége egy nyugati keresztény – ortodox keresztény konfliktusnak, mint az ortodox – iszlámnak, ami leginkább a balkáni államokat érinti [17].

Felhasznált irodalom

[1] Latin Dictionary, http://www.latin-dictionary.org/civilis 2016.10.10.

[2] Oxford Dictionary, http://www.oxforddictionaries.com/definition/english/civilization 2016.10.10.

[3] The World of Civilizations: POST-1990 Archived 12.03.2007, Wayback Machine.

[4] Huntington, P.S., (1993) Foreign Affairs, Vol. 72, No. 3. pp. 23-24.

[5] Huntington, P.S., (1993) Foreign Affairs, Vol. 72, No. 3. p. 25.

[6] W. Wallace, THE TRANSFORMATION OF WESTERN EUROPE. London: Pinter, 1990. Map by Ib Ohlsson for POHHON AFFAIRS.

[7] Huntington, P. S. (1996) The Clash of Civilizations? Simon & Schuster, p. 166., ISBN 0-684-84441-9

[8] Testing Huntington in Ukraine". European Tribune.

[9] Huntington, P.S., (1993) Foreign Affairs, Vol. 72, No. 3. p. 30.

[10] Huntington, P. S. (1996) The Clash of Civilizations? Simon & Schuster, Map 1.3. p. 27. ISBN 0-684-84441-9

[11] Lazányi, K., (2014) A biztonsági kultúra, Taylor IV. Vezetéstudományi Konferencia

[12] Hofstede, G., (2001) Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations. Second Edition, Thousand Oaks CA: Sage Publications

[13] Lazányi, K., (2012) A társas támogatás szerepe egy individualista társadalomban, A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI 4:(2) pp. 51-58.

[14] Hofstede, G., (2011). Dimensionalizing Cultures: The Hofstede Model in Context. Online Readings in Psychology and Culture, 2 (1). http://dx.doi.org/10.9707/2307-0919.1014

[15] Hofstede, G., Hofstede, G.J., and Minkov, M. (2010). Cultures and Organizations, McGraw-Hill Publishing: New York, NY. p. 281.

[16] Hofstede, G., Country Comparison Tool, Available online: https://geert-hofstede.com/hungary.html, downloaded: 28.08.2016

[17] Huntington, P. S. (1996) The Clash of Civilizations? Simon & Schuster, p. 245. ISBN 0-684-84441-9

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Szűcs Endre
szucs.endre@bgk.uni-obuda.hu

AZ ŐSEMBER „BIZTONSÁGTECHNIKAI" ESZKÖZE

Absztrakt

A biztonság minden ember számára elengedhetetlen szükséglet. A biztonság fenntartására törekszünk felnőttként, illetve erre tanítjuk a gyermekeinket. A biztonság fenntartása folyamatos odafigyelést, körültekintést, óvintézkedések tételét igényli. Az ősember is azért cselekedet, hogy saját és a csoportja biztonságát fenntarthassa. Készített számos eszközt, amelynek köszönhetően a napi élelmét könnyebben megszerezhette és védekező eszközként is használhatta. Támaszkodott az érzékszerveire (látására, hallására stb.), hogy a bizotnságban legyen. Az ember és természetesen az ősember érzékszerveinél is vannak fejlettebb érzékszervek, amelyekkel az állatok rendelkeznek. A publkációm célja, hogy röviden ismertessem az ősember „biztonságtechnikai" eszközét a kutyát. Rámutassak a kutya „biztonságtechnikai" eszközként történő alkalmazhatóságára az ősember esetében.

Security is an indispensable necessity for every human being. As adults, we strive to maintain security, and we teach our children to do so as well. This requires constant attention, caution and taking precautions. The cave men already acted in order to provide and maintain security for their group. They created many tools that helped in obtaining the daily food and which could also be used in self defense as weapons. They used their senses (vision, hearing) to detect dangers. Naturally, there are more advanced sensory organs in the animal kingdom, than what a modern or a cave man had. The aim of my publication is to introduce the dog, as the "security system of the cave men" and elaborate on the possible usages of said "system".

Kulcsszavak: *biztonság, kutya, ősember, érzékszervek ~ security, dog, cave man, sensory organs*

BEVEZETÉS

Az ember akkor érzi magát biztonságban, ha számára minden olyan feltétel meg van, amely a veszélytől megvédi őt. A veszély előre jelzése mindig fontos, ahhoz, hogy az elhárítására megfelelő idő álljon rendelkezésre. A veszély jelzésének többféle módja is rendelkezésre állhat. Az ember odafigyel a tevékenysége során a környezetére. A környezet számos veszélyt hordoz magában, amelyek észlelése az érzékszerveink (látásunk, hallásunk, szaglásunk, tapintásunk) utján jut el a tudatunkig, ahonnan a megfelelő cselekvéseink kiindulnak a veszély elhárítása érdekében. Nem minden érzékszervünk működik kellő mértékben. Szükségünk van például arra, hogy a hallásunk segítsen bennünket abban, hogy melyik irányból érhet bennünket veszély, de a hallásunk nem elég jó.

Az ősember is törekedett arra, hogy biztonságban legyen. A biztonság elérése érdekében támaszkodott az érzékszerveire, készített eszközöket, illetve használta fel a környezetében lévő élőlényeket. Az első ilyen előlény a kutya őse volt, amelyet háziasított és ezzel növelte a veszélyek elhárítására rendelkezésre álló idejét és eszközét.

Jelen publikáció azt tárja fel, hogy az ősmber milyen viszonyban volt a kutyákkal, hogyan használta fel a kutyák tulajdonságait, képességeit a biztonsága érdekében.

AZ ŐSEMBER ÉS A KUTYA KAPCSOLATÁNAK KIALAKULÁSA

Az ősember közösségben élt, hogy annak erejét felhasználva biztonságban legyen, azaz életben maradhasson. A biztonságához hozzátartozott a megfelelő mennyiségű táplálék (élelem) előteremtése, a biztonságos szálláshely (lahely) kialakítása és fenntartása (főként a földművelésre való áttérés után).

A megfelelő mennyiségű élelem megszerzése érdekében a férfiak vadásztak, a nők és a gyerekek gyűjtögettek. A szálláshelyeket barlangokban alakították ki és a megszerzett élelmet a férfiak, a nők és a gyerekek odavitték és ott fogyasztották el. Az élelem elfogyasztása során maradék is keletkezett, melyet a lahely közelében szórtak szét. A vadállatok az érzékszerveik segítségével észlelték a kidobott ételmaradékot és odajártak azokért. Az ételmaradék megszerzése során a vadállatok mind közelebb kerültek az emberhez. A vadászatok során is előfordult, hogy az ősemberek hagytak maradékot az elejtett állatokból, melyeket a vadállatok fogyasztottak el. A vadállat is a könnyebb táplálékszerzést keresi és valószínű, hogy a vadászó ősembereket követték, hogy élelemhez jussanak. Az ősember szálláshelye és a vadászat helye körül az előzőeket figyelembe véve valószínűleg a sakál, vagy a farkas lehett jelen.

Az ősember a vadászat, illetve a gyűjtögetés során találhatott magára maradt farkas-, sakálkölyköt, melyet a szálláshelyén felnevelt és az(ok) a közösségnél maradtak és ott szaporodtak. A közösségnél született állatok már nem olyan körülmények között nőttek fel, mint a szüleik.

Az 1. számú képen az a kiskutya tetem látható, amelyet tamuti kutyának nevezetek el. A tamuti kiskutyát 2011-ben a Kelet-szibériai tenger partvidékén, Uszty-Janszki járás (Oroszország) Tamut falujától 42 kilométerre a Sziallah-folyó partján találtak meg. A kiskutya tetemét egy őskori tábor közelében találták meg, ahol az ősember által készített eszközöket (kőszerszámokat, nyílhegyeket) tártak fel. [1; p. 1]

1. ábra. A tamuti kiskutya [1; p. 2]

A kiskutya mumifálódott tetemét nemzetközi tudós csoport vizsgálja, akik között a Belga Királyi Természettudományi Intézet paleontológusa Mietje Germonpre az alábbiakat fogalmazta meg.

„.Két fő elmélet van a kutyák háziasítására” - mondta a belga szakértő. „Az egyik szerint az állat az emberek által lakott terület közelében ólálkodott, eleinte a maradékot kezdte el elfogyasztani, majd fokozatosan hozzászokott az emberi jelenléthez. Egy másik elmélet szerint pedig az ember volt a kapcsolat kezdeményezője, amikor fiatal állatkölyköket nevelt fel, és tanított be. Ez utóbbi hipotézist erősítheti meg a szibériai kutyakölyök léte is” - tette hozzá.”[1; p. 4]

A paleontológus véleményével egyetértek, mert azt napjaink kutatásai is alátámasztják. Több nemzetközi kutatást is végezetek arra vonatkozóan, hogy farkas kölyköket emberek neveltek fel. Ilyen kutatást folytattak magyarok is, akik napi 24 órában a közelükben tartották a farkaskölyköket.[2; p. 2] A farkaskölykök ilyen mérvű emberhez szoktatása bizonyította, hogy a háziasítás a kölyök állatokkal kezdődött.

A publikációban nem írok a kutya háziasítására vonatkozó konkrét időpontokat, mert azok sokfélék még a kutya háziasításával foglalkozó kutatók álláspontjai is más és más az időmeghatározást illetően.

Miért háziasította az ősember a kutyát? A kérdésre a választ a kutya érzékszervei, illetve alkalmazkodó és tanuló képessége adja meg. A kutya érzékszervei az alábbiak:

- szem,
- fül,
- orr.

Az érzékszervek közül az orr a legfejlettebb a kutyák esetében. A kutya szaglása sokkal jobb az ember szaglásánál, melyet alátámaszt az, hogy a kutya orrnyálkahártyája nagyobb, mint az emberé. A kutya orrnyálkahártyája 100 és 220 millió szaglósejtet foglal magába, míg az ember orrnyálkahártyája csak 5 millió szaglósejtet foglal magába. A kutya a szagok alapján

tájékozódik, illetve azok alapján különbözteti meg a körülötte lévő teret. A szagok alapján képes más állatok és az emberek nyomát követni és ennek következtében azt megtalálni.

A kutya másik fontos érzékszerve a füle és ennek következtében a hallása. „A kutya nagy pontossággal lokalizálja azt az irányt, ahonnan a hang származik. A hangforrás felé fordítja a fejét, mégpedig úgy, hogy a hang azonos erővel érje mindkét fülét, pillantását pedig arra felé szegezi, amerről a hang érkezik. Amennyiben nem sikerül megpillantania a hangot adó dolgot, és nem tudja legyőzni kíváncsiságát sem, ide-oda billenti fejét, s ily módon pontosan tájékozódik a hang eredetéről. A hangforrás meghatározásában a kutya magasan túlszárnyal minket, embereket. Ha az eb körül képzeletbeli kört rajzolunk, és azt beosztjuk 360 fokra, 5 foknyi pontossággal képes lokalizálni a hangot, vagyis ötször-tízszer pontosabban, mint mi.”[5] Az idézet alapján is állítom, hogy a kutya hallása jobb, mint az emberé. A kutya tehát hamarabb jelezte az ősember számára a veszélyt.

A kutya harmadik érzékszerve, ami az ősember szempontjából fontos a szem. „A kutyák szeme sokkal érzékenyebb a fényre és a mozgásra, mint az emberi szem, de kevéssé képes érzékelni a tárgyak körvonalait. A szem felülete jóval laposabb az emberénél, és bár a kutya is képes a lencse formájának megváltoztatásával a fókusztávolságot szabályozni, de nem tudja olyan hatékonyan, mint az ember.”[6] A kutyák sokkal jobban látnak éjjel, mint az emberek.

Az ősember is megtapasztalta ezeknek az érzékszerveknek a hatékonyságát és ezért tartotta magánál a kutyát. A kutya tanuló képességét is felhasználta a biztonsága érdekében, mert megtanította neki a vadászaton mit végezzen el, a szálláshely őrzésekor mikor jelezzen, mikor támadjon a betolakodóra. A kutya képes jelzésekre feladatot végrehajtani, amelyet tanulással érhet el. A kutya tehát bevált, mint „biztonságtechnkiai” eszköz.

A háziasított kutya fajtái

Az őskort a történészek több időszakra osztották fel, amely a kutya háziasításának folyamatában is jelen van.

Az őskor korszakokra bontása alapján a neolitkum időszakában már letelepedett az ősember, de a vadászatot természetesen nem hagyta abba. Tehát a közösség a maga biztonsága érdekében nevelte, tanította a kölyköket, amelyek azért még inkább voltak vadállatok, mint kutyák. A tanítás eredményeként vadászaton a vadak felhajtását esetleg elejtését végezték, illetve a vadállatok támadásától védték az ősembereket. A vadászzsákmány szállításában segédkezhettek, azaz jelen lehettek a vadászaton, mint teherhordók. A 2. számú képen a vadászaton alkalmazott kutyák ábrázolása látható.

2. ábra. A kutya alkalmazása vadászaton [3]

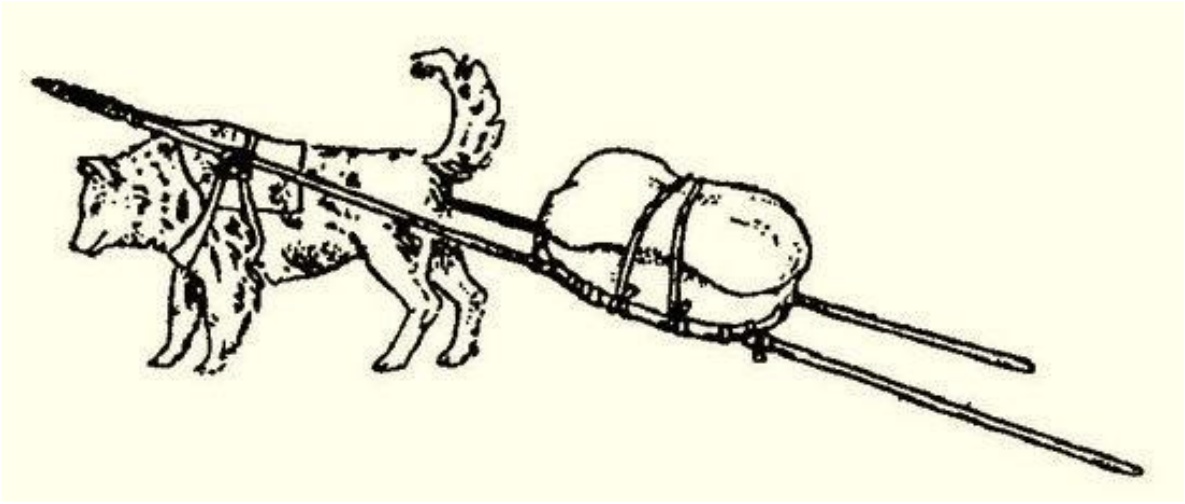
A képen látható, hogy a kutyák körbe veszik a szarvast, amelyet a bal szarva mellett látható emberalak a vadász leteríti. A kép felső részén egy szánon lévő kutyák vannak ábrázolva. A kép alapján látható, hogy kutyák több féle feladatot hajtottak végre. Az egyik kutya fajta a vádászatot segítette, míg a másik az elejtett vad lakhelyre szállítását végezte. [3]

A letelepedett ősember szállásának őrzésében és védelmében fontos szerepet töltöttek be a kutyák. A védelem kiterjedhetett a „házi állatokra" is nappal legeltetéskor, illetve éjszaka az őrzésükkor. A legeltetés során megakadályozták az állatok szétszéledését, elkóborlását. Védelmezték a „házi állatokat" a ragadozóktól. A „házi állatok" védelme biztosította az ősember számára az élelem tartalékot.

3. ábra. A házi állatok terelésében résztvevő kutya [4]

A különböző feladatok elvégzéséhez különböző fajták alakultak ki a háziasítás hosszú folyamata során. A feltárt kutya maradványok alapján a fajták az alábbiak.

- a vadász,
- a terelő,
- az őrző,
- a szánhúzó.



4. ábra. Terhet húzó kutya [7]

A kutya szánhúzásra természetesen a hóval borított területeken volt jelen. Vannak olyan vidékek, ahol a kutyák nem csak a havon húznak szánt, hanem a földön is, mint a 4. számú képen látható.

A kutyák tehát számos területen hasznos segítői voltak az ősembernek, melynek köszönhetően a biztonságosabb lett az élete.

ÖSSZEGZÉS

Az ősember környezete, amelyben élt tele volt veszéllyel, melyek alapvetően meghatározták a biztonságát. A biztonság elérése érdekében az ősember is megtett mindent. A veszélyek észlelése és az elhárításukra való cselekvés a mindennapjai részét képezték. A biztonságának növelése érdekében olyan eszközre volt szüksége, amely időben jelzi a veszélyt. A veszély időben történő jelzésére a kutya ősének a háziasítása hozta meg az eredményt. A publikációmban röviden ismertettem, hogyan alakulhatott ki az ember és a kutya kapcsolata. Kiemelem a kutya azon érzékszerveit, amelyek a leginkább alkalmassá tették az ember biztonságának magasabb szintre emelést. Rámutatok arra, hogy a milyen területeken alkalmazta a kutyát az ősember, mint „biztonságtechnikai" eszközt.

A további kutatási területnek tekintem az ókorban és a középkorban megvizsgálni a kutya szerepét az ember biztonságát illetően.

Felhasznált irodalom

[1] Így néz ki a világ legidősebb kutyája, amelyet a jég mumifikált. http://mult-kor.blog.hu/2015/06/30/igy_nez_ki_a_vilag_legidosebb_kutyaja_amelyet_a_jeg_mumifikalt, Letöltve: 2016. október 03.

[2] Richard W. Byrne. Állati kommunikáció evolúciója: hogyan képes a kutya megérteni a gazdáját? Magyar Tudomány 2006/2, http://www.matud.iif.hu/06feb/05.html, Letöltve: 2016. október 13.

[3] Barba Rafael Péter, A prehisztorikus kezdetek. http://kutya.hu/Cikk.aspx?id=4003 Letöltve: 2016. október 10.

[4] A kutya és az ember kapcsolata. http://kutya.yolasite.com/akutyahaziasitasa.php Letöltve: 2016. október 10.

[5] Kutya kisokos cikk. Fül. http://e-kutyak.hu/kutya-kisokos-cikk/ful/234, Letöltve: 2016. október 08.

[6] Kutya kisokos cikk. Szem. http://e-kutyak.hu/kutya-kisokos-cikk/szem/236, Letöltve: 2016. október 10.

[7] Bodrogi Tibor: Mesterségek, Társadalmak születése. Budapest, Neumann Kht., 2005. http://mek.niif.hu/04600/04682/html/index.htm, Letöltve: 2016. október 07

HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Kovács Zoltán
zkovacs.24@gmail.com

BIZTONSÁG VS. TÖRVÉNYES ELLENŐRZÉS AZ INTERNET ALAPÚ KOMMUNIKÁCIÓBAN - ELLENTÉTES VAGY EGYMÁSSAL MEGFÉRŐ KÖVETELMÉNYEK? II.

Absztrakt

A cikksorozat első része összefoglalta a kommunikáció változását, a változások hatását a szolgáltatói modellre és a törvényes ellenőrzésre. Rámutatott azokra a jogi hiányosságokra, problémákra, amelyek hatással vannak az internet alapú kommunikáció törvényes ellenőrzésének hatékony ellátására, majd nemzetközi kitekintéssel bemutatta az ellenőrzésére jelenleg rendelkezésre álló, jellemző technikai eszközöket és azok főbb tulajdonságait. A második rész rávilágított a hazánkban újonnan hatályba lépett jogszabályok adta lehetőségekre, pontosítva annak kereteit, valamint ismerteti, hogy milyen hatásai lehetnek a kommunikáció biztonságára.

The first part of this article series has summarized the changes of communication and the effects of these changes on the service-provider model and on the lawful monitoring. That article has pointed out the insufficiencies and problems of the current laws which affect the lawful monitoring of the internet-based communication, then described the currently and typically used possible technical solutions of lawful monitoring, and their major characteristics with an international view. The second part of this article series is highlighting the possibilities given by the Hungarian law that entered into force nowadays, on lawful monitoring of the application service providers, specifying its frames, and describing its effects on the security and privacy of communication.

Kulcsszavak: *hírközlés, kommunikáció, alkalmazásszolgáltató, törvényes ellenőrzés ~ electronic communication, communication, application service provider, lawful monitoring*

BEVEZETÉS

A cikksorozat első része, elsősorban a „Felhő alapú rendszerek törvényes ellenőrzési problémái”, a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. – II.”, valamint az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből” című cikkek alapján összefoglalta a kommunikáció, és ezáltal a szolgáltatói modell változását, bemutatta az internet alapú kommunikációs rendszerek törvényes ellenőrzésére alkalmazható jellemző módszereket, azok főbb előnyeit, hátrányait. Mindezt úgy, hogy erre alapozva bemutathatók legyenek a hazánkban 2016-ban elfogadott új szabályozás keretei és hatásai. Jelen cikk ezt teszi meg, megvizsgálva, hogy az új jogszabály milyen kötelezettségeket ró a felhasználókra, a gyártókra/fejlesztőkre, valamint az alkalmazásszolgáltatókra, bemutatja az általa biztosított jogi garanciákat, de körül járja a betarthatósággal kapcsolatos kérdéseket is.

A MAGYARORSZÁGI TV. SZABÁLYOZÁS ÉS ANNAK HATÁSAI

Az internet alapú szolgáltatások – ezek közül is kiemelten a kommunikációt lehetővé tevők – törvényes ellenőrzésében mérföldkőnek tekinthető a hazánkban 2016-ban hatályba lépett szabályozás. A terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény [1] ugyanis többek között módosította az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényt (Ekertv.). [2] Ennek keretében bevezette az alkalmazásszolgáltató fogalmát, definiálta a Magyarország területére irányuló szolgáltatásokat, valamint előírta a titkosított kommunikációt biztosító alkalmazásszolgáltatóknak, hogy megkeresés esetén tegyék lehetővé az erre feljogosított szervezetek számára a kommunikáció tartalmához és az annak kapcsán keletkező vagy kezelt meta adatokhoz való hozzáférést. Kötelezővé tette számukra továbbá a továbbított küldeményekkel, közlésekkel kapcsolatosan keletkező vagy kezelt meta adatok, azok keletkezésétől számított 1 éven át történő megőrzését is. Az ehhez szorosan kapcsolódó, a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Korm. rendelet [3] pedig rögzíti a szolgáltatók és a törvényes ellenőrzést végzők közötti együttműködésének részletszabályait.

A szabályozás keretei és hatásai

A sajtóban a jogszabályok kihirdetése előtt számos találgatás látott napvilágot, majd a kihirdetés után is lehetett olvasni kissé félreértelmezett interpretálásokat a szolgáltatók, de akár a felhasználók szerepéről, kötelezettségeiről, sőt az ellenőrzés kialakítása okán a kommunikáció biztonságának csökkenéséről is. Éppen ezért érdemes áttekinteni mire ad pontosan lehetőséget ez a szabályozás, mit tesz lehetővé és mit nem, valamint, hogy miben jelent előrelépést a korábbiakhoz képest.

Először is az említett szabályozás nem vonatkozik a titkosított kommunikáció felhasználóira, azaz irányukba semmilyen kötelezettséget vagy büntetést nem eszközöl. Másodszor pedig a titkosított kommunikáció kapcsán is csupán a szolgáltatókkal – és nem a gyártókkal, fejlesztőkkel vagy eladókkal (!) – foglalkozik, azaz azokra érvényes akik a kommunikáció felépítése és/vagy végrehajtása során érdemi tevékenységet látnak el. Így nem vonatkozik olyan gyártó és/vagy fejlesztő és/vagy értékesítő cégekre sem, akik csupán végpont-végpont titkosítást biztosító szoftver és/vagy hardver termékeket biztosítanak a felhasználók részére. Ez utóbbi esetben ugyanis mindkét kommunikáló félnek ugyanazt a titkosító eszközt kell alkalmaznia és ugyanazt – vagy legalábbis kompatibilis – harmadik fél

által nyújtott kommunikációs csatornát kell igénybe vennie, a tikosított kommunikáció kapcsán pedig nincs központi azonosítás, azaz így a kommunikáció kizárólag úgy tud megvalósulni, hogy a felek azt előre egymással egyeztették.

Ugyanakkor ez a szabályozás vonatkozik minden olyan kommunikációs szolgáltatóra, amelyik központilag biztosítja a titkosított kommunikáció lehetőségét minden oda beregisztrált felhasználó számára, a felhasználáshoz pedig megfelelő azonosítás szükséges.

A kötelezettség ilyetén történő meghatározásának a logikája megegyezik a jelenlegi hírközlési szolgáltatóknál alkalmazottal, amely előírja egyrészt a törvényes ellenőrzés biztosításának kötelezettségét, másrészt tiltja olyan új szolgáltatás bevezetését vagy a meglévők olyan átalakítását, amely azt ellehetetleníti, ugyanakkor engedi az egyedi, a felhasználó által alkalmazott végpont-végpont titkosítás használatát.

Ez az előírás viszont azt is jelenti, hogy azok a szolgáltatók, akik ma úgy nyújtanak titkosított kommunikációs szolgáltatást, hogy jelenleg nem biztosítják a kommunikáció tartalmához való hozzáférést, vagy át kell, hogy alakítsák működési struktúrájukat, vagy hazánkban nem nyújthatják szolgáltatásukat. Ez pedig amellett, hogy a hazánkban infrastruktúrával is jelenlévő hírközlési szolgáltatókkal e tekintetben versenyegyenlőséget teremt, lehetővé teszi a törvényes ellenőrzést az arra feljogosított szervek számára.

Érdemes ugyanakkor azt is megvizsgálni, hogy okozhatja-e ez a fajta új jogi szabályozás a kommunikáció biztonságának romlását a felhasználó szemszögéből. Ehhez először is elemezni kell az említett jogszabályok hatásait a kommunikációra biztonságára, majd ezeket össze kell vetni azoknak az egyéb technikai lehetőségeknek a hatásaival, amelyek adott esetben a törvényes ellenőrzést végzők rendelkezésére áll(hat)nak.

A szabályozás hatása a kommunikáció biztonságára

Tekintsük egy példát a klasszikus hírközlés világából. A rádiótelefonok hazai elterjedésekor az első telepített rendszer az NMT 450 volt. Ez a hangátvitelre titkosítás nélküli FM modulált jelet használt, [4] amely egy megfelelő vevő segítségével bárki által lehallgatható volt. Ilyen vevővel bármelyik rádióamatőr rendelkezhetett, de néhány tízezer forintnak megfelelő összegért ezeket bárki engedély nélkül megvásárolhatta, akár hazánkban is. Ehhez képes a mai GSM hálózatok ma már erős (jobbára A5.1 vagy A5.3) titkosítást alkalmaznak a levegőinterfész lehallgatás elleni védelmére. [5] Ezeket ma sokkal biztonságosabbnak tekintjük, mint a régi NMT rendszert, pedig azzal is tisztában vagyunk, hogy a GSM rendszerek esetében is biztosított a törvényes ellenőrzés lehetősége. Ez azt mutatja, hogy úgy lehetett növelni a kommunikáció biztonságát a felhasználó szempontjából, hogy ugyanakkor nem csorbult a törvényes ellenőrzéshez fűződő érdek sem.

Természetesen felmerülhet a kérdés, hogy a hazánkban bevezetett jogi szabályozásnak vannak-e negatív hatásai, azaz a felhasználó szemszögéből a kommunikáció továbbra is elég biztonságosnak tekinthető-e.

A felhő alapú rendszerek, így a kommunikációt (is) biztosítók esetében az egyik kiemelten kezelt probléma a szolgáltató kémkedése, valamint harmadik felek (pl. szolgáltató beszállítói, partnerei) hozzáférése a felhasználó adataihoz, [6] információihoz. Sőt, ennek a kérdésnek a vizsgálata kapcsán arra is külön is érdemes kitérni, hogy – az általában külföldi – felhőszolgáltató hogyan és melyik ország szervei számára biztosítja még az ellenőrzés lehetőségét. Nézzük meg például a Gmail esetét. A Gmail-t biztonságosnak tekintjük, hiszen már bejelentkezéstől erős SSL titkosítást használ, és több eszközt is biztosít (pl. ki mikor milyen IP címről, eszközről stb. fért hozzá utoljára a fiókunkhoz, figyelmeztető emailt küld, ha szokatlan bejelentkezést észlel pl. új mobil eszközről stb.), amellyel támogatja kommunikációnk biztonságát. [7] Ugyanakkor már a Google-al kötött szerződésben is szerepel, hogy hozzáfér leveleinkhez, azokat – persze csupán a szolgáltatás fejlesztése érdekében – elemzi és felhasználja. [8] Ráadásul a Snowden által közzétett anyagokból azt is

tudjuk, hogy 2009-ben a Google is csatlakozott az ún. „Prism” programhoz, amelynek keretében – több más szolgáltatóval, pl. Microsoft, Facebook, Apple stb.) együtt biztosították az Egyesült Államok szolgálatai részére a hozzáférést a rendszereiken tárolt és azokon átfolyó adatokhoz (pl. beszélgetések, video-chat, fényképek stb.). [9] [10] Joggal merülhet fel akkor a kérdés: a felhasználó szemszögéből nézve ez így mennyire biztonságos szolgáltatás? De úgy is feltehetjük a kérdést: ront-e bármit is a biztonságon az, ha az arra illetékes hazai szolgálat egyértelmű és szigorúan betartott és betartatott törvényi előírásoknak megfelelően fér hozzá az általa jogosan igényelt információkhoz?

Ehhez érdemes tovább vizsgálni a szolgáltatói együttműködés adta kereteket. Az egyik ilyen kitétel, hogy a hazai jogszabályok által előírtak mellett nincs szükség az átviteli út titkosításának kikényszerített gyengítésére. Ez azt jelenti, hogy nem kell olyan hátsó kaput, mesterkulcsot vagy gyengített titkosítást alkalmazni, amelyek lehetővé tehetik a szolgálatok számára a szolgáltatók bevonása nélkül is az információkhoz való hozzáférést. Ez a megoldás ugyanis valóban adna egyfajta technikai megoldást az ellenőrzésre[1], de ez azzal a veszéllyel is járna, hogy más, illetéktelen titkosszolgálatok, bűnözők, konkurens cégek stb. is könnyebben hozzáférhetnének a felhasználó adataihoz, információihoz, amely valóban jelentősen gyengíthetné a biztonságot.

A másik ilyen kitétel, hogy így nincs szükség a felhasználó által használt hardver eszközök (pl. okostelefon, notebook stb.) kikényszerített gyengítésére, hátsó kapu beépítésére. Ez szintén adhatna egyfajta technikai megoldást[2] a törvényes ellenőrzésre feljogosított szolgálatok részére, sőt nem csak a kommunikáció tartalmához, hanem akár az eszközön tárolt egyéb adatokhoz is hozzáférést biztosítana, ugyanakkor ugyanúgy rendelkezne azokkal a hátrányokkal, mint a fenti megoldás. Azaz az eszköz elvesztése, ellopása, de akár távoli hozzáférése esetén mások is könnyen hozzájuthatnának ezekhez az információkhoz, vagy telepíthetnének rá kémprogramokat. [11]

A szolgáltató együttműködése így talán a legkisebb veszélyforrásnak tekinthető, mindazok ellenére, hogy ily módon fennáll a veszélye a szolgáltató kémkedésének, vagy egy partnere illetéktelen hozzáférésének. Ez ugyanis jogi és adminisztratív úton kezelhető, azaz előírhatók a szolgáltató számára olyan rendelkezések, amelyek ennek kizárását szolgálják. Ráadásul ezek betartása, valamint a betartás bizonyítása a szolgáltatóknak is érdeke. Azok a szolgáltatók ugyanis, akik elvégeztetnek egy erre vonatkozó auditot, tanúsítással rendelkeznek arról, hogy náluk szabályozott és ellenőrzött módon zárták ki a fent említett problémát, és annak eredményeit közzé is teszik, versenyelőnyt szereznek azokkal szemben, akik nem tudnak hasonlót felmutatni. Ez a metódus a felhő alapú rendszerek esetében már elfogadottnak tekinthető, erre bevált formák és eljárások vannak, az auditorok pedig rendelkeznek a kellő tudással egy ilyen típusú átfogó vizsgálat elvégzéséhez. Ezért a szolgáltatók – a biztonság szem elé kerülésével – érdekeltek lesznek abban, hogy így járjanak el.

Arra, hogy a felhasználók számára valóban a szolgáltatók és a törvényes ellenőrzést végző szervezetek közötti együttműködés biztosítja a legkisebb kockázatot, további érvek is felsorakoztathatók.

---

[1] lásd „Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban – ellentétes vagy egymással megférő követelmények? I”.: pl. mély csomagvizsgálat (DPI), közbeékelődéses ellenőrzés (MitM)

[2] lásd feljebb: pl. aktív ellenőrző eszközök (kémprogramok), valamint pl. FBI-Apple vita. Ez utóbbi esetében két, az Iszlám Állammal szimpatizáló terrorista 14 embert ölt meg egy egészségklinikán az egyesült államokbeli San Bernandinóban. A rendőrség által begyűjtött bizonyítékok között volt az egyik támadó jelkódos zárral védett iPhone 5C típusú mobiltelefonja, amelynek feltörését kérte az FBI az Apple-től. A cég ezt megtagadta, majd egy, az ügyön túlnövő vita alakult ki az adatvédelemről. Bár bírósági végzés is született arról, hogy az Apple-nek segítenie kell, végül egy – vélhetőleg – izraeli cég törte fel a telefont és tette a rajta lévő adatokat elérhetővé az FBI számára. [22]

Az első, hogy a felhasználó számára így ismert és tudott az együttműködés ténye, amely ráadásul a hírközlési szolgáltatók viszonylatában már elfogadott gyakorlat is. Korábban éppen a Snowden botrány kapcsán derült fény arra, hogy például a legjelentősebb alkalmazásszolgáltatók tagadták, vagy kerülték a válaszadást az egyesült államokbeli nemzetbiztonsági szolgálatokkal és rendvédelmi szervekkel való együttműködésre, mégis lehetőséget biztosítottak számukra a felhasználók adataihoz való hozzáférésre. [12]

A második, hogy azok a szolgáltatók, akik a korábban már jelzett auditot végrehajtják, és annak eredményeit közzéteszik, azt is bizonyítják a felhasználóknak, hogy csak azokkal az ellenőrzést végző szolgálatokkal állnak kapcsolatban, akikről a felhasználó is tud. A felhő alapú szolgáltatások esetében ugyanis mindig is kiemelten kezelendő kockázat volt, hogy a szolgáltató kivel osztja, oszthatja meg a felhasználó adatait, így például a szolgáltató honos országában, vagy akár az adatközpontjainak országában is. [13] Amennyiben ez nem tisztázott a felhasználó számára, akkor ez is csökkentheti a kommunikációja biztonságát.

A harmadik, hogy arra egyébiránt sincs garancia, hogy egy szolgáltató vagy gyártó nem épít-e be tudatosan valamilyen hátsó kaput, amellyel akár saját maga, akár egy harmadik fél számára biztosíthatja a hozzáférést a felhasználó adataihoz. Erre több alkalommal is felmerült a gyanú olyan neves gyártók esetében, akik biztonságosnak hirdették termékeiket. [14] [15] [16]

Kikényszeríthetőség

A hazai szabályozás kapcsán felmerült már a kérdés, hogy ki lehet-e egyáltalán kényszeríteni az alkalmazásszolgáltatók együttműködését. Erre talán az adózással és a szerencsejátékok szabályozásával kapcsolatos példákat érdemes megemlíteni. Az alkalmazásszolgáltatók adóztatására már 2014-ben T/264 számon javaslat érkezett, [17] amelyet az Országgyűlés még abban az évben el is fogadott. [18] Az így hatályosított törvényben megfogalmazottak alapot és precedenst teremtettek az internet-technológiára épülő szolgáltatások, így az alkalmazásszolgáltatók „bekényszerítésére” a magyar jogrendbe. Ugyanakkor az adóztatás szempontjából is érdekes – és a későbbiekben megoldandó – feladatként jelentkezik a szankcionálás kérdése. Nagy kérdés ugyanis, hogy milyen eszközökkel lehet kikényszeríteni az együttműködést, vagy hogyan lehet büntetni az az alól kibújókat. Erre lehet példa az interneten nyújtott sportfogadások, szerencsejátékok esete. Itt a NAV[3] már blokkoltatja azokat az online fogadási szolgáltatást nyújtó oldalakat, amelyek nem tesznek eleget a magyar jogszabályokban megfogalmazottaknak. [19] Megjegyzendő azonban, hogy az itt egyébként működő szankcionálási rendszert is meg kívánták erősíteni az illetékesek, amelynek érdekében törvényjavaslatot terjesztettek be, [20] amelyet azóta az Országgyűlés el is fogadott, a rendelkezési pedig már hatályba is léptek. Ennek főbb elemei, hogy a kiszabható pénzbírságot a tízszeresére emelték, valamint bevezették a pénzügyi blokkolást is. Ez utóbbi azt akadályozza meg, hogy az illegális szerencsejáték szervező bankszámlájára megérkezzen a játékos által átutalt összeg, az átutalást ebben az esetben ugyanis a pénzforgalmi szolgáltató nem teljesítheti.

A szankcionálásra a törvényes ellenőrzés kapcsán jelenleg az Ekertv. – ismételhető módon – pénzbírság kiszabását biztosítja. Ennek gyakorlati betarthatósága, esetlegesen más elemekkel pl. a szerencsejátékokhoz hasonló módon blokkolással, történő kiegészítése még a jövő zenéje. Ugyanakkor meg kell jegyezni, hogy a szankcionálás kérdése az adózás esetében sem kristályosodott még ki teljesen, és ez ugyanúgy kérdéseket vet fel a törvényes ellenőrzés kapcsán is. Mindazok mellett, hogy az interneten nyújtott sportfogadások, szerencsejátékok esetében Magyarországon már kialakult egyfajta működő megoldás, célszerű egyrészt

[3] NAV: Nemzeti Adó- és Vámhivatal

megvizsgálni a külföldi ilyen célú megoldásokat, másrészt egyeztetéseket folytatni arról, hogy magasabb pl. EU szinten hogyan lehet a kérdésben egységesen fellépni.

Jogi garanciák

További kérdésként merülhet fel, hogyan lehet, vagy lehet-e bármilyen garanciát adni arra, hogy a törvényes ellenőrzést végző szolgálatok csak ahhoz az információhoz férnek hozzá, amelyekre engedélyt kaptak? Erre jogi garanciát nyújt a nagyon szigorú hazai szabályozás. Ez már a hírközlési szolgáltatók esetében is kizárólag ún. külső, azaz bírói vagy igazságügy miniszteri engedély megléte esetén tette lehetővé a kommunikáció tartalmához való hozzáférést, valamint kizárta a szűrő-kutató jellegű ellenőrzés lehetőségét. A jelenlegi szabályozás ezt konzekvensen fenntartja. Ráadásul a 185/2016. (VII. 13.) Korm. rendelet lehetőséget biztosít a szolgáltató számára, hogy jogi képviselőjével megvizsgáltassa az adatigénylés jogszabályok szerinti megfelelőségét. Ezek pedig megfelelő garanciális elemek mind a felhasználó, mind a szolgáltató számára.

ÖSSZEGZÉS

Összességében megállapítható, hogy a kommunikáció változása a szolgáltatói modell és a törvényes ellenőrzés változását is magával hozta. Az is megállapítható, hogy jelenleg több féle technikai megoldás létezik a törvényes ellenőrzés végrehajtására, ám a szolgáltatóval való együttműködés megkerülhetetlen. A Magyarországon 2016-ban életbe lépett jogi szabályozás mindenképpen előremutató, mondhatni példaértékű, hiszen mások csak most keresik a problémára a megfelelő megoldást. Jól mutatja ezt a német és a francia belügyminiszter által kiadott közös közlemény is, amelyben deklarálják, hogy a terrorizmus elleni küzdelem okán olyan megoldást kell találni a titkosított kommunikáció lehallgatására, amelyik biztosítja az adatokhoz való hozzáférést a felhasználók magánszférájának védelme mellett. Mindezt úgy, hogy a szabályozás minden szolgáltatóra egyforma kötelezettségekkel, egyforma feltételekkel terjedjen ki, függetlenül azok székhelyétől. [21] Azaz egyfajta, a magyar szabályozásnak megfelelő megoldást javasolnak, ám ennek tényleges megvalósításától még messze vannak.

Megállapítható az is, hogy az új hazai szabályozás teremtette lehetőség mindamellett, hogy a felhasználó szempontjából nézve a kommunikáció biztonságára a legkisebb veszélyforrásnak tekinthető, költséghatékonyan képes biztosítani a törvényes ellenőrzést. Ráadásul oly módon, hogy ahhoz megfelelő jogi garanciákat is csatol.

Ugyanakkor megállapítható az is, hogy a kikényszeríthetőség további megoldandó kérdéseket vet fel, amelyek hatékony megoldásához célszerű megvizsgálni egyrészt a hazai és a külföldi már kialakult és működő megoldásokat, másrészt egy magasabb pl. EU szintű egységesen fellépés lehetőségét.

Felhasznált irodalom

[1] 2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600069.TV&timeshift=fffffff4&txtreferer=00000001.TXT Letöltés ideje: 2016. 09. 25.

[2] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0100108.tv Letöltés ideje: 2016. 09. 25.

[3] 185/2016. (VII. 13.) Korm. rendelet a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600185.KOR Letöltés ideje: 2016. 09. 25.

[4] Ketterling, Hans-Peter A.: Introduction to Digital Professional Mobile Radio. Artech House. Norwood. 2004. ISBN 1-58053-173-3 https://books.google.hu/books?id=nZ5ISTkagOQC&pg=PA85&dq=nmt+450+modulation&hl=hu&sa=X&ved=0ahUKEwjPktaQuazPAhVI0xoKHY84APEQ6AEIVjAG#v=onepage&q=nmt%20450%20modulation&f=false Letöltés ideje: 2016. 09. 25.

[5] GSM Association Specification for A5/3. http://www.3gpp.org/ftp/tsg_sa/wg3_security/tsgs3_13_yokohama/docs/pdf/s3-000362.pdf Letöltés ideje: 2016. 09. 25.

[6] Chow, Richard – Golle, Philippe – Jakobsson, Markus – Shi, Elaine – Staddon, Jessica – Masuoka, Ryusuke – Molina, Jesus: Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security ACM. New York, NY, USA 2009. pp. 85-90. ISBN: 978-1-60558-784-4 http://www.parc.com/publication/2335/controlling-data-in-the-cloud.html. Letöltés ideje: 2011. 11. 05.

[7] Biztonsági tippek a Gmail használatával kapcsolatban. https://support.google.com/mail/answer/7036019?co=GENIE.Platform%3DDesktop&hl=hu Letöltés ideje: 2016. 09. 25.

[8] Google Általános Szerződési Feltételek (Utolsó módosítás: 2014. április 14.) https://www.google.com/intl/hu/policies/terms/ Letöltés ideje: 2016. 09. 25.

[9] Poitras, Laura – Gellman, Barton: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. 2013. 06. 07. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Letöltés ideje: 2013. 06. 28.

[10] NSA slides explain the PRISM data-collection program. 2013. 06. 06. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Letöltés ideje: 2013. 06 28.

[11] Yadron, Danny: Government keeping its method to crack San Bernardino iPhone 'classified'. https://www.theguardian.com/technology/2016/mar/22/apple-fbi-san-bernardino-iphone-method-for-cracking Letöltés ideje: 2016. 09. 25.

[12] Gyurkity Péter: Mindenki a megfigyelt felhőbe igyekszik. 2013. 06. 10. https://sg.hu/cikkek/97838/mindenki-a-megfigyelt-felhobe-igyekszik. Letöltés ideje: 2016. 09. 25.

[13] Cloud Computing: Benefits, risks and recommendations for information security. 2009. 11. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment. Letöltés ideje: 2014. 11. 12.

[14] Sullivan, Nick: How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer. 2014. 01. 06. http://arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/ Letöltés ideje: 2016. 09. 27.

[15] Zetter, Kim: Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors 2012. 12. 18. https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ Letöltés ideje: 2016. 09. 27.

[16] Afonin, Oleg: iOS 10: Security Weakness Discovered, Backup Passwords Much Easier to Break. 2016. 09. 23. http://blog.elcomsoft.com/2016/09/ios-10-security-weakness-discovered-backup-passwords-much-easier-to-break/ Letöltés ideje: 2016. 09. 27.

[17] http://www.parlament.hu/irom40/00264/00264.pdf. Letöltés ideje: 2014. 07. 01.

[18] 2014. évi XXXIII. törvény az egyes pénzügyi tárgyú törvények módosításáról. http://www.complex.hu/kzldat/t1400033.htm/t1400033.htm#kagy1. Letöltés ideje: 2015. 03. 29.

[19] Ezeket a szerencsejáték-oldalakat kapcsolta le a NAV. 2014. 06. 28. http://www.napi.hu/ado/ezeket_a_szerencsejatek-oldalakat_kapcsolta_le_a_nav.583212.html. Letöltés ideje: 2014. 07. 01.

[20] T/12250. számú törvényjavaslat egyes törvényeknek a tiltott szerencsejáték megakadályozásával összefüggő módosításáról. http://www.parlament.hu/irom40/12250/12250.pdf Letöltés ideje: 2016. 09. 27.

[21] Ein Beitrag zur Erhöhung der inneren Sicherheit in Europa http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/eckpunkte-der-europaeischen-zusammenarbeit-innere-sicherheit.pdf?__blob=publicationFile Letöltés ideje: 2016. 08. 25.

[22] Nakashima, Ellen: FBI paid professional hackers one-time fee to crack San Bernardino iPhone 2016. 04. 12. https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html Letöltés ideje: 2016. 09. 25.