HADMÉRNÖK

Kiemelt közlemények

16. évf. (2021)
4. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919 (elektronikus)

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
Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Gergely Zsuzsánna, Resofszki Ágnes

Tartalom

Fórum

HADMÉRNÖK
BIZTONSÁGTECHNIKA

16. évfolyam (2021) 4. szám 5–12.
DOI: 10.32567/hm.2021.4.1

Katalin Kondás[1]

The Development of Personal Identification in Prisons

I build my publication upon 12 years of experience that I have spent in the IT field at the prison service since 2007. During this period, I continuously analysed the possibility of identifying prisoners by their biometric characteristics and I am currently conducting research on the same subject. Summary documentation on prisoner identification is currently not available. My article provides a comprehensive picture of the identification systems used in Hungarian prisons and their development, and at the same time outlines the future of personal identification.

Keywords: **biometrics, prison, identification, fingerprint, QR code**

1. Introduction

Biometric identification is one of the most common and most advanced means of identification, the essence of which is to be able to establish someone's identity with great certainty, quickly and credibly. Taking advantage of the explosive and dynamic development of information technologies, biometric identification methods are also undergoing continuous and rapid development. This type of authentication is multi-faceted, depending on what the expectations are, what purpose it is used for, how much money is planned to be spent on their implementation, and how the identification system envisioned can be designed.

In Hungary, the biometric identification method has not yet become widespread in prison service.[2]

My article focuses on summarising the identification systems having been used so far in Hungarian prisons. In the prison service, personal identification has played a key role in the admission of a detainee and in his or her daily phone calls and shop purchases in recent decades.

I believe that the biometric identification system of the Hungarian Prison Service, which I envisaged a long time ago, is already close to physical implementation.

[1] Doctoral School of Security Sciences of the Óbuda University, doctoral student, e-mail: kondaskatalin@gmail.com

[2] Katalin Kondás and Endre Szűcs, 'A személyazonosításra vonatkozó speciális szabályok a büntetés-végrehajtásban', Biztonságtudományi Szemle 2, no 2 (2020), 15–21.

2. Paper-based identification

Until 2004, prisons had not had an automatic identification system for identifying detainees. The convicts had the opportunity to make phone calls with the telephones placed in the prison wards. The registration was done on paper. The detainee filed a phone call appeal, requesting, within the regulated framework, a call to be made to his or her relative. A member of the prison service staff could provide the phone call at a specified time. The phone call was made using a telephone card, with the participation of the prison service staff. The relative or lawyer was called by the prison service staff at the time corresponding to the permit, and after making sure that it was the authorised person that actually picked up the device, the prison service staff member handed over the phone to the detainee, who could thus begin the conversation. If, according to the judicial ruling, the detainee's telephone calls could only be made with the prison service staff monitoring, then the personnel were present throughout the telephone call. At that time, the calls were only administered on paper, as were the purchases made at the institute's shop.

3. Automatic identification system

In 2004, the Hungarian prison system underwent significant development. The installation of an IT system began, with which all telephone conversations of convicts could be monitored and interrupted when prohibited information was communicated. The process of automation started. Establishing the system came at a huge cost, but the development, which was in the amount of two hundred and fifty-one million forints, delivered the expected results, and the work of the prison personnel was made easier a great deal.

They introduced the Contel telephone system, which was developed for prison service institutes to monitor the telephone conversations of convicts. The convicts were given a piece of paper with a barcode, which was made durable by laminating. This card was the barcode identification card. The barcode was the unique identifier that identified the cardholder, so it did not contain any monetary information or pre-paid minutes. A camera was installed next to the telephone. The function of the camera was that the camera feed was monitored by an operator and it could be established from the data stored in the system whether it was indeed the card owner who was making the call. The system already knew which telephone numbers belonging to the person, previously provided by him or her and verified by the authorities, could be called. In compliance with the framework of legal provisions, the operator was able to listen in on all calls, so the telephone calls no longer required a personal presence on the part of the prison service staff.

At that time, the construction of telecommunication and IT systems using databases had already begun. Each convict received a barcode identification card, identified him/herself with a card reader before the phone conversation, and thus the device allowed the detainee to call the phone numbers he or she was allowed to. Convicts could make purchases the same way. In the past, it had been much more

complicated to check phone calls, as a guard had to be placed next to each convict.[3] The new system received positive reviews and has been developed and used in all institutes over the years.

The system operated adapting to legal changes, e.g. it stored and monitored call options. A further advancement in the system was storing the facial images of inmates and the use of these images for identification. By the year 2006, a camera installed in the telephone was able to perform an automatic check using the IT system. The facial identification was rudimentary at the time.[4]

3.1. Barcode-based telephone system

The basis of the system is that each prisoner has a unique barcode identification card, and the given card also has a photo of the prisoner assigned to it, stored in the IT register. If the prisoner wants to make a phone call, for identification he or she will need the identification card, the barcode of which having been scanned, the camera built into the telephone will take a photo of the detainee and compare it to the photo in the database. Identification is based on this.

The conversations can be fully monitored, and telephone charges are settled automatically based on data from the financial system. It is important to note that the barcode card can be used for phone calls as well as for purchases at the institute store if the prisoner has financial coverage.

The first and most important activity in the system relating to the phone conversations is the safe and fast identification of the detainee. At the beginning of the call, when the detainee picks up the receiver, he or she is given a verbal instruction through the device to show the barcode on his barcode card to the flashing light of the code reader and face the camera. After the card is presented, if the light goes out, the identification has been done automatically.

The biometric identification of the detainee is carried out by comparing the image extracted from the detainees' database as put on the screen and the image from the webcam attached to the telephone.

3.2. Barcode based shopping in the store

The financial system for inmate phone calls and in-store shopping is the same. The costs of purchases and phone calls are immediately reflected in the convict's financial flows.

At a store purchase, the inmate hands over his or her barcode ID card to the seller, who reads it with the barcode reader. The photo stored and belonging to the scanned card is displayed on the monitor on the counter. In addition, the screen shows the amount of money that can be used in the store. The monitor is positioned in such

[3] Hajnalka Fülöp, 'Elektronikus pénztárca a börtönben', NOL, 10 February 2006.
[4] Gergely Gárdonyi, 'Az állóképes arcképazonosítás Magyarországon', Belügyi Szemle 69, no 7 (2021), 1133–1148.

a way that both the seller and the buyer can see it well, so the inmate can easily decide how much money to spend in the store and how much to leave to make phone calls.[5]

The Electronic Public Administration Operational Program was a significant development that allowed the introduction of new identifications.[6]

4. System-wide development

For the Hungarian prison system, the largest system-wide reform started already back in 2010. Between 1 January 2013 and 30 June 2014, within the framework of the Electronic Public Administration Operational Program, the Ministry of the Interior implemented their priority project "Responsibility and Preparedness in Penitentiary Enforcement Phase 2", in co-operation with the National Command for Penitentiary Enforcement, with a budget of HUF 500 million. Within the framework of the project, the development of the classified data management system was implemented, 7 audited security areas were established, an encrypted data connection ensuring the electronic transmission of classified data was also established between the security areas, and the system for handling non-classified data was expanded as well. 1,200 workstations were replaced with thin clients, with expanding server capacity where necessary. The reform affected the modernisation of local networks, the increase in the number of endpoints, the entirety of computer equipment (servers, workstations) and the replacement of records based on outdated software technology, as well.[7]

The aim of the reform was to create a homogeneous, standard, uniformly solid, nationwide, closed IT system.[8] At all of its locations, the system provides an identical infrastructural background for the operation of the newly developed records by creating a homogeneous office environment. At the same time, the existing IT systems were replaced by newer ones.[9]

The network bandwidth has increased, local data storage has been replaced by central data storage, remote access.[10]

Thanks to the project, with the expansion of the prison system, the ability to exchange data is improved and the administration is sped up. Thanks to the modernisation, the nominal electricity consumption of the penitentiary organisation will be reduced by HUF 30 million annually.

In 2013, the operation of the Hungarian penitentiary system received a new legal basis as the new Penitentiary Act was enacted. The greatest system-wide IT development in the life of Hungarian prisons was also made during this period. Law CCXL

5 Katalin Kondás, Fogvatartotti azonosítás a büntetés-végrehajtásban. MA thesis, 2013, 13–40.
6 Attila Sebestyén, 'Büntetés-végrehajtás informatikai fejlesztési projekt', in Kommunikáció 2009, ed. by Károly Fekete (Budapest: Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó, 2009).
7 Government Decree 1236/2012 (VII.12.).
8 Tibor Farkas, 'Védelmi infokommunikációs hálózatok és rendszerek – szakmai felkészítés', Hadtudományi Szemle 13, no 1 (2020), 37–48.
9 Katalin Kondás and Endre Szűcs, 'Informatikai korszakváltás egy büntetés-végrehajtási intézetben', Hadmérnök 12, no 2 (2017), 272–279.
10 Tibor Farkas and Szabolcs Prisznyák, 'Kormányzati célú infokommunikációs hálózatok. A rendészeti szervek infokommunikációs rendszere', Hadtudományi Szemle 10, no 4 (2017), 583–596.

of 2013 on the implementation of penalties, measures, certain coercive measures and the imprisonment for committing misdemeanour contains the determination of the convicted person's identity. The Penitentiary Institute of the Prison Service Organization is obliged to verify the identity of the convicted person, during which, based on the data recorded in the documents that form the grounds for admission, they take over the data of the convict that are handled in the personal identification and photo registries of the criminal records system and verify the data in the records.[11]

In order to identify the convict, the institute now also records the convict's fingerprints and initiates the comparison at the expert registration body pursuant to Section 82 (5) (b) of Act XLVII of 2009 on the criminal record system, the registration of convictions of Hungarian citizens by the courts of the Member States of the European Union and the registration of criminal and law enforcement biometric data. The comparison is made electronically by scanning with the electronic equipment designed for this purpose.[12]

With the change in the law, detainees were given the opportunity to keep in touch with their family members with a mobile phone provided by the organisation, which is a stripped-down device and its use does not require identification. Wall-mounted telephones have largely been phased out, with only two institutes still having this system these days. For in-store purchases, object-based identification has been retained, coupled with a more modern IT system and using a QR code.

In 2015, the replacement of QR code identification with palm vein biometric identification was discussed. The solution was not implemented due to high costs. I examined the practical application of palm vein identification in Turkish health insurance.[13]

5. Introduction of the NFC technology

The system called Service Application to Facilitate Detention (hereinafter: SAFE) enables fast, electronic retrieval of information and data on detainees and is also suitable for recording the implementation of standard protocols. Only applications required to perform service duties may be installed and run on SAFE mobile devices.

Each cell of the institute has an NFC tag that displays all the relevant information about the cell on the SAFE device, e.g. who is the detainee, what degree of security he or she has, whether the cell is a smoking cell. The inmate also has an NFC tag, which provides quick information, using the SAFE device about the inmate.

In 2019, the NFC (Near Field Communication) technology was introduced in the institutes, which allows file exchange between devices, data transfer or reading of various information from NFC tags. The two main benefits of the technology are

[11] Act CCXL of 2013.

[12] Act XLVII of 2009, para 82, point 5.

[13] Tibor Kovács, István Milák and Csaba Otti, 'A biztonságtudomány biometriai aspektusai', in A biztonság rendészettudományi dimenziói: Változások és hatások, ed. by Zoltán Hautzinger (Budapest: Magyar Rendészettudományi Társaság, 2012); Szabolcs Prisznyák, 'A tenyérvéna alapú azonosítás egyes alkalmazási lehetőségei', Pécsi Határőr Tudományos Közlemények 15 (2014), 225–234.

that it is secure and that it can be used in many ways in combination with NFC tags. This technology is able to connect devices in seconds, but only when they are a short distance apart and only when the smartphone screen is not locked. As a result, no one can connect to our device without our consent. NFC tags are tiny chips that are most commonly available in the form of stickers. The tag is freely programmable and can be affixed to the desired location.

In 2019, a pilot project was set up at the organisation to provide inmates with NFC bracelets, to ensure the rapid flow of information, and to lighten the daily workload of the staff. However, the use of the bracelet did not prove to be adequate. It was concluded from the use of the bracelet that a more robust solution was needed in the penitentiary institutes to maintain NFC technology. The introduced NFC bracelet was more prone to wear and tear due to the environmental effects, so a supplementary solution became necessary. Thus, in addition to the NFC bracelet, an NFC prisoner card was also introduced. The card is no longer paper-based but made of plastic and is more durable. The new card has a cover with the image of the owner, as well as an NFC tag and a QR code containing the detainee's personal identification.[14]

6. The future

It is one of my goals to set up a prisoner identification system using biometric features in Hungarian penitentiary institutions, for which the IT system is already available. One of the main advantages of biometric identification in prisons is that the detainees do not have to carry any identifier items on them. Thus, they cannot lose them and they cannot be stolen by others.

Considering the fact that fingerprints are taken at the admission of detainees in order to identify the person, my research does not cover which biometric feature would be appropriate for identification. The prison service has fingerprint readers, they are used to identify the persons admitted, so the fingerprints are practically available. However, the law does not currently permit fingerprints to be stored or used for other purposes by the penitentiary.

The first step is for detainees to be able to make purchases in the shops of the institutes using the newly introduced biometric identification. Telephony is not subject to changes, given that inmates have their own cell phones. The two institutes where the wall-mounted devices are still in use may be an exception to this.

Taking into account the requirements of the prison service, I would like to introduce an identification system equipped with a fingerprint scanner. With the fingerprints available, they could be used for other purposes as well, thus speeding up and lightening the daily workload.

For the time being, the introduction of biometric identification would take place on a strictly voluntary basis, in parallel with the current card identification. Upon its introduction, the detainee, by signing a statement, gives his consent to participate in

[14] Zsolt Kocsis, Büntetés-végrehajtási biztonsági ismeretek közép- és felsőfokú szaktanfolyami képzés. Jegyzet (Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, 2021).

the testing of the new system. Naturally, those who do not do so will not have any disadvantages, they keep on using the system the same way as before.

If the use of a fingerprint reader achieves the desired level of safe operation at the test institutes, its introduction could be extended to the entire country in the years ahead. However, its mandatory use requires changes in the law. The introduction of the newly envisioned systems must take place according to a specified schedule. The primary goal for me is to explore the most optimal option for prison service and to put together a concrete plan as result of a series of long analyses.

7. Summary and research results

In the course of my work, I have dealt with the identification of prisoners. The topicality of my choice of theme is justified by the dynamic development of information technologies and the possibility of using biometric identification methods.

In the course of my research, I have summarised the identification methods used throughout the organisation and their practical application. I have described the structure of the currently installed system. I have found that the IT system set up by the organisation has brought the possibility of introducing biometric identification closer. I suggest that the replacement of object-based identification be realised with fingerprints, given that the fingerprints are available during institutional admissions. However, when deploying the new identification system, it is important to emphasise that the legal background of the organisation needs to be changed before the introduction of biometric identification.

Biometric identification is constantly evolving. It can also be used in prisons. Fingerprint scanners are a cheap solution. However, because of the Covid-19 epidemic, palm vein identification and facial identification are preferable because they do not require physical contact.

References

Farkas, Tibor, 'Védelmi infokommunikációs hálózatok és rendszerek – szakmai felkészítés'. Hadtudományi Szemle 13, no 1 (2020), 37–48. Online: https://doi.org/10.32563/hsz.2020.1.3 ; DOI: https://doi.org/10.32563/hsz.2020.1.3

Farkas, Tibor and Szabolcs Prisznyák, 'Kormányzati célú infokommunikációs hálózatok. A rendészeti szervek infokommunikációs rendszere'. Hadtudományi Szemle 10, no 4 (2017), 583–596. Online: http://epa.oszk.hu/02400/02463/00037/pdf/EPA02463_hadtudomanyi_szemle_2017_04_583-596.pdf

Fülöp, Hajnalka, 'Elektronikus pénztárca a börtönben', 10 February 2006. Online: http://nol.hu/archivum/archiv-393758-205932 ; DOI: https://doi.org/10.38146/BSZ.2021.7.3

Gárdonyi, Gergely, 'Az állóképes arcképazonosítás Magyarországon'. Belügyi Szemle 69, no 7 (2021), 1133–1148. Online: https://doi.org/10.38146/BSZ.2021.7.3

Kocsis, Zsolt, Büntetés-végrehajtási biztonsági ismeretek. Közép- és felsőfokú szaktanfolyami képzés. Jegyzet. Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, 2021, 193–194. Online: https://bv.gov.hu/sites/default/files/Biztons%C3%A1gi%20jegyzet-k%C3%B6z%C3%A9p%20%C3%A9s%20fels%C5%91fok-2021.03.01..pdf

Kondás, Katalin, Fogvatartotti azonosítás a büntetés-végrehajtásban. MA thesis, 2013.

Kondás, Katalin – Endre Szűcs, 'A személyazonosításra vonatkozó speciális szabályok a büntetés-végrehajtásban'. Biztonságtudományi Szemle 2, no 2 (2020), 15–21. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/64/59

Kondás, Katalin and Endre Szűcs, 'Informatikai korszakváltás egy büntetés-végrehajtási intézetben'. Hadmérnök 12, no 2 (2017), 272–279. Online: https://doi.org/10.32567/hm.2017.2.22

Kovács, Tibor, Csaba Otti and István Milák, 'A biztonságtudomány biometriai aspektusai', in A biztonság rendészettudományi dimenziói: Változások és hatások, ed. by Zoltán Hautzinger. Budapest: Magyar Rendészettudományi Társaság, 2012, 485–496. Online: www.pecshor.hu/periodika/XIII/kovacsti.pdf

Prisznyák, Szabolcs, 'A tenyérvéna alapú azonosítás egyes alkalmazási lehetőségei'. Pécsi Határőr Tudományos Közlemények 15 (2014), 225–234. Online: www.pecshor.hu/periodika/XV/prisznyak.pdf

Sebestyén, Attila, 'Büntetés-végrehajtás informatikai fejlesztési projekt', in Kommunikáció 2009, ed. by Károly Fekete. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó, 2009, 241–260. Online: www.puskashirbaje.hu/index_html_files/Kommunikacio_2009-NSZTK.pdf

HADMÉRNÖK
BIZTONSÁGTECHNIKA

16. évfolyam (2021) 4. szám 13–24.
DOI: 10.32567/hm.2021.4.2

Veresné Rauscher Judit,[1] Berek Lajos[2]

Kórházak biztonsága és védelme I.

Kockázati tényezők és lehetséges következmények

Hospital Safety and Security 1.

Risk Factors and Potential Consequences

Az egészségügyi létesítmények, azon belül is a kórházak a kritikus infrastruktúra részét képezik mind műszaki, mind társadalmi szempontból. Legfontosabb feladatuk a gyógyítás, amelyet különböző vészhelyzetekben is folytonosan biztosítani szükséges. Emiatt fontos kérdés, hogy a kórházakban milyen külső és belső veszélyforrások merülnek fel kockázatként, és azok milyen védelmi megoldásokkal csökkenthetők.

A két részből álló cikksorozat 1. részében a kockázati tényezőket mértük fel, azok lehetséges okainak feltárása mellett, nemzetközi biztonsági ajánlások, saját tapasztalatok és megtörtént esetek gyűjtése alapján. A kockázatok és veszélyek csoportosítása a megelőzésben és kockázatcsökkentésben részt vevők és feladatok meghatározása miatt fontos. Kutatómunkánk alapján kijelenthető, hogy a kórházak esetében fontos kockázatot jelenthetnek külső és belső veszélyforrások, szándékos károkozás és véletlen meghibásodások is.

A cikksorozatban feltártuk a kórházakat érintő speciális kockázati tényezőket, és javaslatot adtunk azok lehetséges csökkentésére vagy elkerülésére. Fontos tényező azonban, hogy minden egyes intézmény egyedi funkcióval és kialakítással rendelkezik, így az általános útmutatás mellett mindig szükséges az egyedi elemzések elkészítése és a megelőző tevékenységek meghatározása. Ezekkel jelentősen növelhető az egészségügyi intézmények, különösen a kórházak működési biztonsága, ami egyben kihatással van azok gazdasági és társadalmi megítélésére is.

Kulcsszavak: **egészségügy, kórház, biztonság, kockázat, kritikus infrastruktúra, gyógyítás, üzembiztonság**

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, doktori hallgató, e-mail: judit@flamella.hu
[2] Óbudai Egyetem, Nemzeti Közszolgálati Egyetem, egyetemi tanár, e-mail: berek.lajos@bgk.uni-obuda.hu

Healthcare facilities, including hospitals, are part of critical infrastructure, both from a technical and a social point of view. Their most important task is to provide medical care, which must be provided at all times, even in emergency situations. For this reason, the question of what external and internal hazards pose a risk in hospitals and what protection solutions can be put in place to reduce them is an important issue.

In Part 1 of this two-part series of articles, we have assessed the risk factors, exploring their possible causes, based on international safety recommendations, our own experience and a collection of real cases. The grouping of risks and hazards is important to identify the actors and roles involved in prevention and risk reduction. Based on our research work, it can be stated that external and internal hazards, intentional damage and accidental failures can be important risks for hospitals.

In Part 2 of this article series, we will use the types and characteristics of the risk factors identified earlier, based on international safety recommendations and our own experience we determine whether they are avoidable and, if so, what preventive safety design or activity can be used to reduce their risks and impact. Based on our research, it can be stated that hazards to hospitals cannot be completely avoided, but that risks can be reduced by safety measures.

In this series of articles, we have identified specific risk factors that affect hospitals and suggested possible ways to reduce or avoid them. An important factor, however, is that each institution has a unique function and design, so in addition to general guidance, it is always necessary to carry out specific analyses and identify the necessary preventive actions. These can significantly improve the operational safety of healthcare institutions, particularly hospitals, and also have an impact on their economic and social image.

Keywords: **healthcare, hospital, security, risk factors, critical infrastructure, medical care, operational safety**

1. Bevezetés

2001. szeptember 11-e óta egyértelműen kijelenthető, hogy terrorista cselekmény még a legjobban védett országokban is megtörténik, megtörténhet. A cselekmények legtöbbször lokálisak, de mindenképpen nagyobb befogadóképességű épületben vagy szabadtéri rendezvény területére koncentrálódnak. Fontos a cselekmény pszichológiájában az állampolgárok minél szélesebb köréhez eljuttatni, hogy nincsenek az állam által nyújtott biztonságban, ez velük is bármikor és bárhol megtörténhet. Egyik ilyen célpont lehet az egészségügyi intézmények elleni támadás, azon belül is a kórházak, ahol nagy számban magatehetetlen (fekvőbetegek, újszülöttek) és/vagy mozgásukban korlátozott személyek tartózkodnak, emellett a társadalom szemében biztonságot és segítséget nyújtó szerepük is megkérdőjelezhetetlen.

Magyarországon még ilyen eset nem történt, de az alábbi külföldi példák azt mutatják, hogy a terrorizmus ebben a körben nem tartja be az úgynevezett „íratlan szabályokat".

- A WHO jelentése alapján 2016 novemberében öt kórházat ért terrorista-támadás Szíriában.[3]
- Az Izraelben alapított Nemzetközi Terrorelhárítási Intézet által 2013-ban publikált tanulmány szerint 1981 és 2013 között nagyjából 100 terrorista-támadás célja volt kórház vagy egészségügyi létesítmény.[4] Ezek közül a sérültek és halottak száma alapján kiemelkedően súlyos esetek is voltak. Például:
  - Oroszország, Mozdok, katonai kórház (2003) – öngyilkos merénylő rohant egy négyemeletes épületbe, teherautóra rakott robbanóanyaggal, több mint 50 fő hunyt el.
  - Ruanda, Kigali, központi kórház (1994) – a polgárháborúban az egyik fél katonái a másik fél sebesültjeit kivégezték a kórházi kezelésük helyett/közben, több mint 100 beteg halt meg.
- Az intézet egy másik, 2020-ban publikált tanulmánya szerint[5] a koronavírus-járvány miatt megerősödhet, megerősödhetett a kórházi célpontok keresése. Ennek oka, hogy egyéb tömegeket vonzó területek a korlátozások miatt elnéptelenedtek, míg a kórházakban jelentős betegszám alakult ki sok helyen. Például 2020. április 1-jén egy mozdonyvezető megpróbált vonattal belerohanni a kikötőben álló, átalakított kórházhajóba, sikertelenül.

Fontos megjegyezni, hogy az egészségügyi intézményeket nem kizárólag terrorista-fenyegetések érhetik, hiszen akár csalódott korábbi betegek, hozzátartozók, munkavállalók is jelenthetnek veszélyt. Erre is adódtak példák nemzetközi szinten:[6]

- 2018-ban a Mercy Hospitalban történt lövöldözésben 4 ember halt meg, amikor az egyik áldozat korábbi ismerőse kezdett támadásba.
- 2017-ben a cincinatti kórházban lövöldözött egy magányos elkövető, egy dolgozót és önmagát ölte meg.
- 2017-ben a New York-i Bronx-Lebanon kórházban egy 45 éves ott dolgozó orvos lövöldözött, 1 fő meghalt és 6 fő megsérült.
- 2012-ben az augustai kórházban egyik rokona lőtte le látogatás közben a beteget.

A támadások egy része nem fizikailag történik meg, hanem egyre többször a digitális térben. Erre a közelmúltból is van pár példa, ami mutatja, hogy még egy világjárvány miatt leterhelt rendszert sem kímélnek meg ettől:

- 2020 szeptemberében az USA-ban 400 kórház számítógépes rendszerét támadták meg zsarolóvírussal, ami miatt hosszabb ideig nem voltak működőképesek

[3] World Health Organization: WHO condemns massive attacks on five hospitals in Syria (2016. november 16.).
[4] Boaz Ganor – Miri Halperin Wernli: Terrorist Attacks against Hospitals Case Studies. ICT Working Paper 25. International Institute for Counter-Terrorism, 2013.
[5] Samantha Stern – Jacob Ware – Nicholas Harrington: Terrorist Targeting in the Age of Coronavirus. *International Counter-Terrorism Review,* 1. (2020), 3. 1–21.
[6] Alyssa Rege: 17 fatal hospital shootings since 2002. *Becker's Hospital Review,* 2018. november 21.

a rendszereik. A Universal Health Service jelentése szerint több mint 67 millió dollár kárt okozott a leállás.[7]

- Az Amerikai Kórházszövetség 2020 májusában figyelmeztetést adott ki az FBI jelentésére alapozva, miszerint külföldi ügynökök covidhoz kapcsolódó egészségügyi adatok, kutatások, kezelési információk megszerzésére tettek kísérletet.[8]

Emellett szintén fontos tényező, hogy az egészségügyi intézményekben, a funkcióból és a műszaki megoldásokból adódóan is előfordulnak balesetek, vészhelyzetek, meghibásodások, amelyek szintén veszélyeztetik az ellátás folytonosságát, és gazdasági, társadalmi hatásai is lehetnek.

2. Kórházak Magyarországon

A kórházat fekvőbeteg-szakellátást nyújtó egészségügyi szolgáltatónak definiáljuk, amelyből Magyarországon jelenleg 164 intézmény szerződött a Nemzeti Egészségbiztosítási Alapkezelővel.[9] Az 1997. évi CLIV. törvény 3. § *e)* pontja alapján:

„[E]gészségügyi szolgáltatás az egészségügyi államigazgatási szerv által kiadott működési engedély alapján végezhető egészségügyi tevékenységek összessége, amely az egyén egészségének megőrzése, továbbá a megbetegedések megelőzése, korai felismerése, megállapítása, gyógykezelése, életveszély elhárítása, a megbetegedés következtében kialakult állapot javítása vagy a további állapotromlás megelőzése céljából a beteg vizsgálatára és kezelésére, gondozására, ápolására, egészségügyi rehabilitációjára, a fájdalom és a szenvedés csökkentésére, továbbá a fentiek érdekében a beteg vizsgálati anyagainak feldolgozására irányul."

A kórházi alapellátáson kívül, az azt biztosító feladatok érdekében is, kiszolgáló egységeket is találunk a kórházi épületekben: raktárak, orvosi gázok tárolása, konyhaüzem, mosoda, tornaterem, uszoda, személyzeti területek és ingatlanfenntartáshoz szükséges területek. Az egészségügyi szolgáltatáson kívül egyéb gazdálkodó szervezet által működtetett szolgáltatások is megjelennek a kórházi épületekben: kereskedelmi üzlet (például optikai, gyógyszertár, orvosi segédeszközök boltja stb.), vendéglátóüzlet (például büfé), kiegészítő egészségügyi szolgáltatás (például független diagnosztikai szolgáltatás).

A kórházakban az egyik legfontosabb biztonsági feladat, hogy az ellátás folytonosságát biztosítani kell. Ennek biztosítására minden intézménynek egészségügyi válsághelyzeti tervet kell létrehoznia, amelynek tartalmi követelményét a 43/2014. (VIII. 19.) EMMI rendelet rögzíti. A terv főbb elemei rögzítik a riasztás és berendelés menetét, az intézmény részleges vagy teljes kiürítésének megoldásait, a szükségkórházi megoldásokat és a folyamatos üzemhez szükséges szállítás, élelmezés, kommunikáció megoldásait. A rendelet alapján a cselekvési tervek kidolgozása a feladat, azonban biztonságtechnikai szempontból ezt meg kell előznie egy részletes kockázati elemzésnek.

[7] UHS: Universal Health Service Inc. Reports Information Technology Security Incident. (2020. szeptember 29.).
[8] American Hospital Association: FBI, CISA warn of serious nation state cyber threats, other top vulnerabilities. (2020. május 13.).
[9] Nemzeti Egészségbiztosítási Alapkezelő, Fekvőbeteg-ellátást nyújtó intézmények, kórházak: www.neak.gov.hu/felso_menu/lakossagnak/szerzodott_szolgaltatok/fekvobeteg_ellatast_nyujto_intezmenyek_korhaz.html

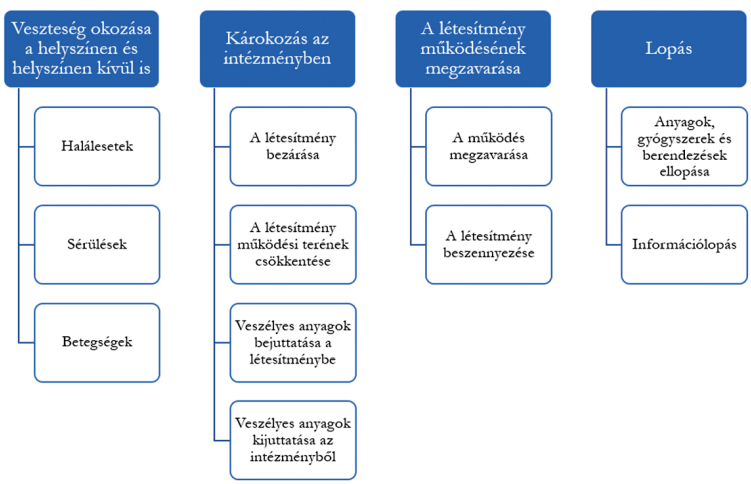
3. Potenciális fenyegetések

Tekintettel arra, hogy a kórházi intézményekben széles körű szolgáltatás jelenik meg, és a bent tartózkodó személyek – egészségügyi állapotuk függvényében – kiszolgáltatottak, igen jó alapot teremt egy esetleges támadásnak. A lehetséges fenyegetések skáláját mindig az adott intézményre, helyszínre, épületre vonatkozóan kell meghatározni az előzetes kockázatelemzés során. Az Amerikai Egyesült Államokban a Nemzetbiztonsági Szolgálat adott ki 2007-ben egy kifejezetten kórházakra vonatkozó ajánlást, amely részletesen foglalkozik a veszélyek jellegével és megoldási javaslatokat is ad az elhárítás módjára.[10]

A fenyegetéseket mindig olyan személy vagy csoport teremti meg, amely rendelkezik képességgel és szándékkal is, hogy kárt okozzon. A fenyegetések forrásai lehetnek: belföldi és nemzetközi terroristák, elégedetlen alkalmazottak, vélt vagy valós sérelmet elszenvedett személyek vagy csoportok. Fontos, hogy a fenyegetők ismerhetik a létesítmények rendszereit és a használt berendezéseket, amihez a szükséges információk származhatnak nyílt forrásokból (például online felületek) vagy akár alkalmazottaktól (jelenlegi vagy korábbi).

Adott intézmények esetében a fenyegetések felmérése érdekében javasolt feltérképezni a lehetséges támadási célokat és az azokhoz szükséges taktikát és tudást. Ezeknek a tényezőknek a világos megértése és a rendszerek értékelése adhat támpontot az esetlegesen szükséges biztonságtechnikai fejlesztések meghatározásához.

Az egészségügyi intézményhez kapcsolható lehetséges támadási célokat az 1. ábrán foglaltuk össze. Az egyes lehetséges támadási célok azonosítása az első lépés azok elkerüléséhez, vagy legalább a kockázat minimálisra csökkentéséhez.



1. ábra

A támadók lehetséges céljai

Forrás: a szerzők szerkesztése U.S. Department of Homeland Security (2007): i. m. alapján

[10] U.S. Department of Homeland Security: Hospitals, Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures (2007. október 5.).

4. A legfontosabb biztonsági rések

Az amerikai ajánlás és a hazai viszonyok ismeretében vannak speciálisan kórházakra jellemző sebezhető pontok, amelyek mellett természetesen itt is érvényesek lehetnek más területeken létező általános biztonsági rések. A kórházra jellemző biztonsági rések két nagy csoportba sorolhatók. Az első csoport abból adódik, hogy a kórházak a funkciójukból adódóan jól és könnyen hozzáférhetők, a társadalom figyelmének előterében vannak, és széles a használók köre. A második csoportot pedig az adja, hogy – szintén a funkcióból adódóan – jelentős mennyiségben és változatosságban lehetnek jelen veszélyes, mérgező és robbanásveszélyes anyagok az intézményekben.

4.1. A kórházak nyilvános létesítmények, jellemzően több bejárattal kialakítva

A legtöbb esetben a kórház főbejáratánál információs pult(ok) található, és az anyagi körülményektől függően lehet, hogy nincs is biztonsági személyzet jelen. A főbejárattól távolabbi oldalsó bejáratok azonban lehetővé teszik a bejutást, anélkül, hogy a kórházi személyzet vagy a biztonsági személyzet figyelmét felkeltenék. Jellemző, hogy a bejáratoknál szigorúbb biztonsági intézkedések, például fémdetektorok vagy egyedi beléptetőrendszer ritkán találhatók (csak speciális intézetekben). A nagy kórházak akár 20–50 nem biztonságos bejárattal is rendelkezhetnek, ami Magyarországon különösen igaz a régebbi építésű, több épületes elrendezésű intézmények esetében. Így a legtöbb kórházi terület, épület könnyen elérhető olyan egyének számára is, akik rosszindulatú cselekményt tervezhetnek.

4.2. A kórházak könnyen elérhetők motoros járművekkel

A kórházi épületeknek könnyen megközelíthetőknek kell lenniük a mentőautók és más üzemelési technológiához szükséges, nem ambuláns járművek számára (például szemétszállítás, élelmiszer-beszállítás, tűzoltógépjárművek stb.), így a fő teherkapu-bejáraton kívül általában több teherkapu-bejárattal is rendelkezik egy kórházterület. A létesítményen belül az épületek megközelítése érdekében szintén a fent említett járművek, valamint személygépjárművek rendszeres és nem rendszeres közlekedésére belső, megfelelő teherbírású útvonalak létesülnek. Emellett a betegek és a látogatók kényelmének érdekében sokszor az épületekhez közel, vagy épületek alatt parkolók létesülnek (ez Magyarországon inkább teljesen új létesítmények esetében fordul csak elő, kivéve a kötelezően létesítendő mozgássérült-parkolóhelyeket). Egy mélygarázsban történő robbantás az épület tartószerkezetét nagyobb mértékben károsíthatja, de az épület homlokzata előtt történő robbantás is jelentős károkat okozna, így az általános működési igények egyben kockázatot is jelentenek.

4.3. Tömeges áldozatok lehetősége

Egy napközbeni kórházi forgalom alatti támadás magában hordozza a nagyszámú áldozatokkal (betegek, látogatók, kórházi dolgozók) járó lehetőséget, ami például egy terroristacélokkal rendelkező támadónak kifejezett előnyt jelent. Különösen, hogy a kórházban tartózkodók kiszolgáltatott helyzete miatt, sérülések esetén nagy társadalmi visszhangot is kapna.

4.4. Nagy kockázatot jelenthet a gyakran változó személyzet és a háttérellenőrzés esetleges hiánya

A kórházak nagy létszámú és változatos személyzeti részvételt igényelnek: nemcsak egészségügyi dolgozókra van szükség, hanem nagyon sokféle kiszolgáló személyzetre is. Az esetleges belső ellenőrzések jellemzően nem minden munkavállalóra vonatkoznak egységesen, különösen igaz ez a takarítás, az élelmiszer-szolgáltatás vagy a létesítmény karbantartói esetében. Számos kórház lehetőséget kínál a tanításra, kutatásra külsős szakemberek számára, akiket szintén nem ellenőriznek biztonsági szempontok alapján. Magyarországon szükség esetén a kórházak térítés fejében külföldi személyeket is ellátnak, ami ugyancsak kockázatot jelenthet mind esetleges célpont, mind pedig esetleges támadó esetén.

4.5. A fertőzések könnyen terjeszthetők a szellőzőrendszerek segítségével

A nagyobb, újabb építésű épületek esetében általános biztonsági rés a központi szellőzőrendszer kialakítása és elérhetősége, mivel veszélyes vegyi anyagok, mikrobák vagy radioaktív nuklidok terjedésének lehetőségét legjobban a szellőzőrendszer teszi lehetővé. Ezek a rendszerek azonban a hatékony, biztonságos és minőségi működéshez elengedhetetlenek bizonyos területeken az egészségügyi létesítményekben.

4.6. Orvosi gázok és éghető, robbanásveszélyes anyagok jelenléte

Az orvosi gázok és éghető, robbanásveszélyes anyagok rutinszerűen jelen vannak a kórházakban, a mindennapi működéshez szükségesek, de okozhatnak robbanást vagy a tüzet táplálhatják. Ezt az utóbbi időszakban megnövekedett kórháztüzek is igazolják, ahol a Covid-19-megbetegedés miatt szükséges oxigénterápiák száma és koncentrációja megnőtt.[11]

Az egészségügyi gázokat számos kórházi osztályon használják (például aneszteziológia, sebészet, sürgősségi és intenzív terápiás ellátás, kardiológia, neonatológia

[11] A híradások alapján a Covid-19-megbetegedés miatti világjárvány időszakában több jelentős, halálos áldozatokkal járó kórháztűz is keletkezett, amelyet okozott vagy súlyosbított az oxigénterápia jelenléte. Ilyen volt például 2020 novemberében a romániai Piatra Neamt-i kórház intenzív osztályának tüze, vagy a 2021 februárjában az ukrajnai zaporizzsjai kórház tüze.

[újszülöttgyógyászat], tüdőgyógyászat, reumatológia, sportgyógyászat, toxikológia), és jellemzően központi raktározással és elosztó rendszerrel kiépítettek az épületek. Emellett speciális terápia esetén külön palackok is megjelenhetnek a betegek közvetlen környezetében.

Jellemzően a 2. ábrán összeszedett orvosi gázokat találjuk meg a létesítmények területén, a könnyebb azonosíthatóság érdekében a típusok színjelölését is feltüntettük az ábrán.

SZÍN

Gáz	USA	nemzetközi test / nyak
Oxigén	zöld	fekete / fehér
Szén-dioxid	szürke	szürke / szürke
Nitrogén-oxid	kék	kék / kék
Hélium	barna	barna
Nitrogén	fekete	fekete
Levegő	sárga	szürke / fehér és fekete

2. ábra

Jellemző orvosi gázok és azok színkódolása

Forrás: a szerzők szerkesztése

4.7. A kórházakban több a vonzó célpont lopáshoz

A kórházakban a kiszolgáltatott betegek személyes tárgyai mellett a kórházi technológiából adódóan is több „vonzó" célpont lehet támadások során. Személyes beszélgetés során hallottam olyat is, ahol a mosdókagylót lopták el a látogatói WC-helyiségből.

A magyarországi kórházak jellemző gyakorlata a betegekkel nyilatkozat aláíratása, hogy semmilyen felelősséget nem vállalnak a személyes tárgyak védelmére. Ez a betegekben sokszor rossz érzetet kelt, és egy megvalósult lopás esetében tényleges kellemetlenséget, kárt is okoz.

A nukleáris medicina elemei és a gyógyszerek vonzó célpontot jelentenek a lopásokhoz, mivel több formában hasznosíthatók: akár helyben is komoly károkat okozhatnak a szellőzőrendszerben elhelyezve, kiürítést és költséges fertőtlenítési eljárásokat vonva maguk után, vagy a megszerzett anyagok értékesíthetők illegális keretek között.

Több példát találtunk elektronikai berendezések, mobil gyógyászati eszközök, mobil diagnosztikai eszközök eltulajdonítására is, amelyek a jelentős anyagi kár mellett a betegellátást is veszélyeztethetik.

Ahogy láthatjuk, a betegektől való lopás „csak" kellemetlen és rontja a kórház megítélését, azonban a technológiai lopások komolyabb biztonsági kockázatokat is rejthetnek.

4.8. Védetlen, könnyen hozzáférhető kiszolgáló elemek is lehetnek

Az épület infrastruktúráját biztosító gázellátó- vagy hőközpont és vezetékei, az elektromos főkapcsoló helyisége, az elektromosszakasz-kapcsolókat tartalmazó szekrények, az energiaellátást biztosító transzformátorok, generátorok, vízlágyító berendezések és vízvezetékeik jellemzően védetlen kialakításúak és sokszor könnyen hozzáférhetők. Ezek szabotálása jelentős működési problémát jelenthet az intézmények szempontjából.

5. Potenciális veszélyforrások

A kórházi intézményekben a szándékos támadás mellett a környezetből és a funkcióból adódóan további potenciális veszélyforrások is megtalálhatók, amelyeket szintén javasolt kockázatelemzés során felmérni és részben műszaki, részben biztonságtechnikai megoldásokkal kezelni.

Ezek első csoportja a természeti hatásokat jelenti, amelyek közül Magyarországon az alábbiak szoktak jellemzően előfordulni: szélvihar, jégeső, jelentős hóesés, földrengés, extrém hőmérsékleti viszonyok, bizonyos területeken sárlavina, erdőtűz. Szintén idesorolható a pandémiahelyzet, amely különös megterhelést jelent a kórházi rendszerekre.

A második csoportba jellemzően a technológiai veszélyek tartoznak: valamelyik közműszolgáltatás kiesése meghibásodás miatt (elektromos áram, fűtés, víz, gázellátás, internet), belső ellátások kiesése meghibásodás miatt (elektromos áram, fűtés, víz, csatorna, gázellátás, orvosigáz-ellátás, vákuumellátás), gőzkitörés, csőtörés miatti ázás, MR-berendezés vészleállítása [hélium-lefújatás], tűzeset vagy füstképződés, internet és belső kommunikáció meghibásodása stb.

A harmadik csoportba a személyek okozta kockázatok tartoznak, amelyeket azonban jellemzően szándékos cselekedetek okoznak, és ezért már korábban részleteztük a típusaikat. A szándékos fenyegetésen vagy károkozáson túl azonban további biztonsági kockázatot jelenthet, amennyiben VIP (védett) személyeket kell ellátni az intézményben, és ez befolyásolja a többi beteg ellátásának módját.

A negyedik csoportba pedig a veszélyes anyagok jelenléte miatti, véletlen károk tartoznak: például a nem kontrollálható kémiai reakció (labor, fertőtlenítő anyagok), veszélyes anyag szivárgása, biológiai hatóanyagok (mikroorganizmusok, vírusok, szennyezett vér), vegyi anyagok (érzéstelenítő gázok, antibiotikumok, citosztatikumok, rákkeltő anyagok), radiológiai baleset (béta- és gammasugárzás), veszélyes anyaggal történt baleset miatti (tömeges) betegellátás stb.[12]

[12] Tiszolczi Balázs Gergely: Magyarországi kórházak biztonsági kérdései a célrendszer és a működési sajátosságok tükrében. Doktori (PhD-) értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2017. 27.

E veszélyforrások kockázatának csökkentése lehetséges fokozott műszaki biztonságú rendszerek kialakításával, hatékony karbantartási protokollok és folyamatos jelenlét kialakításával, rendszeres felülvizsgálatokkal és élőerős védelemmel.

6. Egy biztonsági esemény következményei

A kórházak elleni sikeres támadás vagy véletlen baleset, káreset következményei széles körűek lehetnek: közegészségügyi, biztonsági, gazdasági és társadalmi következmények is várhatók. A károk lehetnek helyiek, egyéniek, tulajdonosokat érintők, társadalmiak és akár – például európai létfontosságú elemnek minősített ellátási részleg esetében – nemzetköziek is.[13] A veszteségek jelentkezhetnek azonnal, napokkal később, illetve hetekkel vagy hónapokkal később. Az alábbiakban néhány példát sorolunk fel, amelyek mindegyike előfordulhat akár Magyarországon is.

- Egy kórházi terrortámadás nagyszámú halálesetet és sérülést eredményezhet. A bombatámadás következtében a veszteségek száma nagymértékben növekszik, ha a robbanás elég erős ahhoz, hogy az épület összeomlását is okozza. Szerencsére Magyarországon nem jellemzők a bombatámadások, de például magyar katonákat érhet ilyen külhoni szolgálatteljesítés közben.
- Fegyveres támadó is érkezhet a kórházi környezetbe, erre külföldön rendszeresen van példa. Itthon inkább olyan fordul elő, amikor tettlegességig fajul egy-egy vita. A rendőrségi közlemények (police.hu) alapján az alábbi példákat találtuk:
  - 2021 márciusában egy budapesti kórházban sebészeti ollóval életveszélyesen megsebesítette betegtársát egy férfi;
  - 2017 áprilisában a hatvani kórházban a sürgősségi osztály egy orvosát verte meg egy család három tagja.

Az ilyen incidensek csökkentik a betegek és az ott dolgozók biztonságérzetét, ami kihathat a munkavégzésre és a gyógyulásra is.

- Ha egy biológiai-kémiai szer szétterjed a kórházban, az áldozatokra ez fokozatosan lesz hatással, és a kórházon kívül is lehetnek áldozatok. A hatások enyhíthetők, ha az ágens felismerhető és elérhető az ellenszer. Hasonló a helyzet a kórházi fertőzésekkel, amelyek kockázatot jelentenek a folyamatos betegellátás biztosítására.
- Egy kórházra irányuló támadás, áttételesen hatással van a helyi közegészségügyi szolgáltatásra. Például egy 1. szintű traumaközpont kiesése az ellátási rendszerből különösen negatív hatással lehet a regionális traumaegészségügyi szolgáltatásra.
- Gazdasági következmények lehetnek, hogy egy támadásban vagy balesetben az épületkárosodás felújítási költségei nagyon magasak. Emellett további költséget jelent a betegek átszállítása a részükre ideiglenes elhelyezést biztosító intézményekbe, és adott esetben a védelem hiánya miatti elvesztett kártérítési perekből adódó költségek.

[13] Nagy Rudolf: A klímaváltozás hatása a kritikus infrastruktúra védelmére. *Nemzet és Biztonság,* 3. (2010), 2. 35–44.

- Társadalmi és intézményi következmények közé tartozik, hogy egy sikeres kórház megtámadása a használattól való félelemhez vezethet a lakosság körében. Széles körben elterjedhet az általános szorongás, az az érzés, hogy egy intézmény, amelyet általában menedékhelynek és biztonságosnak tekintettek, adott ideig nem volt biztonságban, illetve biztonságos.

7. Összefoglalás

Összességében kijelenthető, hogy egy kórházi létesítmény a működési jellemzőiből adódóan több biztonsági kockázatot is magában hordoz. Ezek felmérése és lehetőség szerinti csökkentése mindenképpen szükséges a rövid és hosszú távú biztonság növelése és az esetleges káros hatások csökkentése érdekében.

A kockázatok között meg lehet és kell különböztetni a külső és a belső veszélyforrásokat, valamint a szándékos vagy véletlen eseményeket. Ezek kombinációja alapján többféle esemény lehetséges általánosan és kórházakban a funkció miatt speciálisan. A külső és nem szándékos eseményekre példák a természeti jelenségek és hatások. A külső és szándékos eseményeket példázzák a különböző erőszakos támadások, a működéshez szükséges szállítást akadályozó tüntetések, az infrastruktúra szándékos rongálása. A belső és nem szándékos események a meghibásodásból fakadó vészhelyzetek, véletlen tűzesetek. A belső és szándékos veszélyforrásra példák a szándékos gyújtogatás, a szándékos rongálás, a tudatos támadások.

A kockázatok felmérése minden intézményben arra szabottan, egyedileg szükséges, mivel minden intézmény saját funkcióval és műszaki jellemzőkkel rendelkezik. Ezt követően lehet és szükséges meghatározni a kockázatok csökkentése érdekében elvégzendő feladatokat, az adott intézmény ellátórendszerben lévő pozíciójának ismeretében.

Felhasznált irodalom

American Hospital Association: FBI, CISA warn of serious nation state cyber threats, other top vulnerabilities (2020. május 13.). Online: www.aha.org/news/headline/2020-05-13-fbi-cisa-warn-serious-nation-state-cyber-threats-other-top-vulnerabilities

Ganor, Boaz – Miri Halperin Wernli: Terrorist Attacks against Hospitals Case Studies. ICT Working Paper 25, International Institute for Counter-Terrorism, 2013. Online: www.ict.org.il/UserFiles/ICTWPS%20-%20Ganor%20&%20Halperin%20Wernli%20-%2025.pdf

Nagy Rudolf: A klímaváltozás hatása a kritikus infrastruktúra védelmére. *Nemzet és Biztonság,* 3. (2010), 2. 35–44. Online: www.nemzetesbiztonsag.hu/cikkek/nagy_rudolf-a_klimavaltozas_hatasa_a_kritikus_infrastrukturak_vedelmere.pdf

Rege, Alyssa: 17 fatal hospital shootings since 2002. *Becker's Hospital Review,* 2018. november 21. Online: www.beckershospitalreview.com/population-health/17-fatal-hospital-shootings-since-2002.html

Stern, Samantha – Jacob Ware – Nicholas Harrington: Terrorist Targeting in the Age of Coronavirus. *International Counter-terrorism Review,* 1. (2020), 3. 1–21. Online: www.ict.org.il/images/Terrorist%20Targeting%20in%20the%20Age%20of%20Coronavirus.pdf

Tiszolczi Balázs Gergely: Magyarországi kórházak biztonsági kérdései a célrendszer és a működési sajátosságok tükrében. Doktori (PhD-) értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2017. Online: https://doi.org/10.17625/NKE2017.15

UHS: Universal Health Service Inc. Reports Information Technology Security Incident (2020. szeptember 29.). Online: https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-information-technology

U.S. Department of Homeland Security: Hospitals, Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures (2007. október 5.) Online: www.calhospitalprepare.org/sites/main/files/file-attachments/cvpipm_report_hospitals_2.pdf

World Health Organization: WHO condemns massive attacks on five hospitals in Syria (2016. november 16.). Online: www.who.int/news/item/16-11-2016-who-condemns-massive-attacks-on-five-hospitals-in-syria

Jogi források

1997. évi CLIV. törvény az egészségügyről

43/2014. (VIII. 19.) EMMI rendelet az egészségügyi intézmények egészségügyi válsághelyzeti terveinek tartalmi követelményeiről, valamint az egyes egészségügyi tárgyú miniszteri rendeletek módosításáról

HADMÉRNÖK
HADITECHNIKA
16. évfolyam (2021) 4. szám 25–40.
DOI: 10.32567/hm.2021.4.3

János Gyula Kocsi,[1] Gergely László Kiss[2]

Challenges of the Application of Lynx KF-41 Infantry Fighting Vehicle in the Hungarian Defence Forces

Continuous changes in the world and Europe have posed new challenges to NATO. The Russian–Ukrainian conflict that began in 2014 has shown that, in addition to the fight against terrorism and peace operations, the possibility of procedures and confrontations in the traditional sense must not be forgotten either. In the 21st century, the battlefield conflicts are already taking place in a complex and rapidly changing environment that requires forces to keep pace with change because that is the only way they can perform their duties successfully.

In response to the challenges listed, the Hungarian Government launched the Zrínyi 2026 Defence and Armed Forces Development Program, a full-spectrum force development program aimed at making the Hungarian Armed Forces a dominant force in the region. Among the developments affecting the shooting range of the program, the regularisation of the Lynx KF-41 infantry fighting vehicle should be highlighted. Due to its capabilities, the new Western instrument is sufficiently feasible for the battlefields of the future, but the procedures that we used before IFOR, i.e. the Eastern military equipment can no longer be applied.

In our study, we present the features, modern challenges that a modern battlefield poses for a combat vehicle. We analyse the unique features of the Lynx Kf-41 and the challenges that will require vehicle application and team training in the future.

Keywords: **Lynx Kf-41 infantry fighting vehicle, features of the modern battlefield, deployment of the Lynx Kf-41 infantry combat vehicle, Zrínyi 2026 Defence and Force Development Program, new infantry combat vehicle**

[1] University of Public Service, Lieutenant, Assistant Professor, e-mail: kocsi.janos.gyula@uni-nke.hu
[2] University of Public Service, infantry cadet, e-mail: yeti.kiss@gmail.com

1. Introduction

On 20 December 2016, then Minister of Defence István Simicskó announced the Zrínyi 2026 military development program, a 10-year, comprehensive and complex military investment for the Hungarian Defence Forces. The program aims to renew and modernise the Army's outdated, post-Soviet military technology park and the equipment of Hungarian soldiers in accordance with the requirements and challenges of modern warfare, as well as not only force development but also the complete transformation of the Army. As part of this development program, it was announced on 9 September 2020 that the Hungarian Armed Forces would also develop its infantry fighting vehicles, namely the Lynx KF-41, presented in 2015, thus regaining an ability that the Hungarian Defence Forces lost with the withdrawal of the BMP-1 infantry fighting vehicles in 2007.

The Armed Forces can achieve this at the expected level if it can respond to the challenges of the age in accordance with the age. Thus, the continuity of modernisation and the maintenance of up-to-date status are practically essential requirements in the light of the success of the task.

Furthermore, looking at the section on international treaties, the amount required by NATO to spend 2% of GDP on defence must also be realised. At the start of Zrínyi 2026, this was approximately 0.7% of GDP. With the continuous increase of defence expenditures, the modernisation of the Armed Forces became possible, which was, and still is, an urgent need in terms of the armaments of the surrounding countries and the global security policy situation.[3]

2. New demands are followed by new needs

At present, the mechanised infantry units of the Hungarian Defence Forces use obsolete and improperly used BTR-80 and BTR-80/A armoured personnel carriers.

It is essential to clarify the significant differences between infantry fighting vehicles and armoured personnel carrier vehicles.

The purpose of IFVs is to fight together with infantry in armoured or combined combat. To do this, they have adequate armour protection, transport capacity, manoeuvrability and armaments.

The purpose of the APCs, on the other hand, is to transport the subunits to the battlefield so that their safety is guaranteed until the troops reach the battlefield. To do this, they have a specific, but not enough to fight armour protection, transport capacity and armament. Currently, this device is more capable of performing only 'support by fire' tasks because of the 30mm machinegun.

The BTR-80 and BTR-80/A combat vehicles do not meet the requirements of infantry fighting vehicles, as their armour protection, off-road capability and armament are much weaker than it is provided.

[3] Tibor Farkas, 'A védelmi tevékenységeket támogató MH Kormányzati Célú Elkülönült Hírközlő Hálózat fejlesztési lehetőségeinek vizsgálata a honvédelmi és haderőfejlesztési program (Zrínyi 2026) tükrében. Hazai/nemzetközi szakirodalmi összefoglaló', Hadtudományi Szemle 12, no 4 (2019), 5–16.

Until 2007, this capability was provided by the BMP-1 infantry combat vehicle. However, in 2007, at the discretion of the then regulating Government and relevant decision-makers, this by then obsolete but easily modernisable combat vehicle was withdrawn from the system. A significant portion of these vehicles was donated by the country to other countries (e.g. Iraq) and destroyed or sold. Thus, these combat vehicles cannot be recovered.

So to restore this ability, a new tool needs to be systematised. There is still an embargo on Russian techniques, and they are not compatible with NATO STANAG ammunition, NATO STANAG requirements and equipment. As well as other devices systematised within the framework of Zrínyi 2026, the decision-makers chose to systematise German and Swedish techniques.

Regarding testing the German line, either Rheinmetall AG or Krauss-Maffei-Wegmann military companies carry out research, development and production in line with and beyond world standards. A perfect example of this is the Leopard 2 A7 +, PzH2000 or Lynx KF-41. All three tools have been developed to meet the challenges of the age, with forward-looking development opportunities.

Lynx KF-41, as a new technology, also argues that if a country develops a force, it does not plan for five years but for the next 20–30 years. So systematising a technique that is already obsolete would not have been expedient in the long run. However, the potential of a new instrument with future development potential to meet the challenges of the future already has even more significant potential.

Furthermore, the transfer of other assets from the German line and the integration of Lynx will create a comprehensive, complex system, as NATO views warfare systematically, so as a NATO member, the country's forces must develop a system compatible with NATO systems, where soldiers and assets form a joint system.

Examining the meaning of the decision, it is essential to see what challenges the modern area of operations poses to the soldiers.

While in the period before the regime change, as a member of the Warsaw Pact, the Hungarian People's Army was organised as a mass army, trained on the Soviet model, and was ready only to purely conventional warfare. In 21st century, the Hungarian Defence Forces have to face much different challanges during combat operations. Perfect examples of this are the conflicts in the Middle East, the military operations in eastern Ukraine, the Armenian–Azerbaijani (Nagorno–Karabakh) conflict.

Soldiers of the modern age and their equipment must face drones, intelligent ammunition, IEDs, asymmetric warfare, precision combat equipment and a rapidly changing environment. Where targeting is done in a fraction of a second, cover-hide is no longer just about installing a camouflage net and ordering radio silence. Where serious electronic warfare devices are in place to disrupt military equipment, render it incapacitated and destroy the enemy. Based on the measurement of soldiers' cell phones, a precision fire is directed at them by an enemy force. The first shot is a real hit, and after our first shot, the enemy knows where our forces are. Moreover, there is still a need for infantry and infantry fighting vehicles in this environment, perhaps more than ever before, since IFV is also intended to protect forces. We must continue to have the force that physically appears in enemy territory and, using a combination of weapon systems, fights the fight, defeats the enemy and sets the flag.

In response to all these challenges and factors, a change of strategy and attitude took place in the Hungarian Armed Forces. An integral part of this is the revival of the IFV ability embodied by the Lynx KF-41.

3. What induced the change of assets?

The purchase of a new combat vehicle, combat equipment, weapon system or any equipment does not just mean that that equipment is now included in the equipment of the subunit. This will have a wide-ranging impact on training methods, the military organisation and combat procedures under the specifications and dimensions of the given device. The following figure well illustrates this:

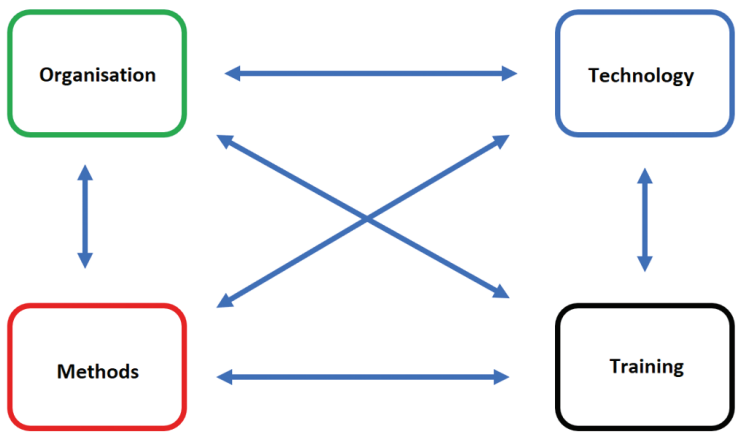


Figure 1
Effects on the assets
Source: Compiled by the author.

So, based on this, in connection with the systematisation of the Lynx KF-41, reform is also needed in the structure of the training, the combat procedure and the organisation using the combat vehicle.

The questions are:

- How do we train soldiers for the new device?
- How to make the most of the opportunities provided by the combat vehicle from the training ground, through peacekeeping missions, in the full spectrum of conventional attacks that may hit the country?
- How to adapt the organisational structure to the specifications of the new technology?

The answer is to be found in the combat vehicle and the services provided by the manufacturer.

4. Training

The training of soldiers no longer depends only on the number of hours spent in the training ground and the shooting range but also on the number of hours spent in the simulation room. Although the sums invested in simulation devices may seem like a lot at first glance, vehicles are protected from possible depreciation, less ammunition must be used, which is more than any shot with such precision weapons, and combat vehicles do not have to consume fuel. Thus, in the long run, the amount invested in the simulation tools pays off and makes the training more economical.[4]

In addition, the training must be transformed so that the soldiers also become precise human resources, handle the military equipment with precise movements, know what they are doing before they touch it and what effect it will have on the tactical situation.

The training methodology of Lynx KF-41 is based on the idea of 'train as you fight', so Rheinmetall has developed its training system based on this. Using tactical situations that a soldier can encounter while operating a combat vehicle by accustoming soldiers to successful and quick decision-making and maximising their professional training.

5. Training system

The Lynx training system consists of 4 main training components:

5.1. Training course system

Rheinmetall provides the training base for the forces that systematise the Lynx KF-41. So T3, i.e. Train the Trainer – the training of the trainer. It also equips course participants with primary operator and maintenance skills in the Introduction Into Service system.

5.2. Training simulators and real training

The training also includes real-world techniques and simulator programs but targets cost-effectiveness, a high level of training and safe training methods. This includes practice ammunition and subtask training.

[4] Tibor Horváth (ed.), A honvéd és a harcászati szintű kis alegységek (raj és szakasz szintű kötelékek) általános harcászati gyakorlati felkészítése. Oktatási segédlet (Budapest: Nemzeti Közszolgálati Egyetem, 2014), 25.

5.3. Technologically accepted learning and training aids

In addition to the training that requires continuous drilling, there is a strong emphasis on real-world teaching, as the application of techniques also requires significant theoretical material.

5.4. SME support

Rheinmetall also provides training instructors for its customers. They monitor the adequacy of training and help improve training systems.

5.5. Xerena – portable information tablet with video conferencing capability

The training support tool, the Xerena, was designed to continuously support the work of the operator and maintenance personnel on the combat vehicle. Important information becomes directly available to the user on a tablet at the location where the work or repair is to be performed, ensuring immediate availability. If this would not be enough to do the job, an expert with specific knowledge of the subject can provide additional instructions through the tool within the framework of video conferencing.

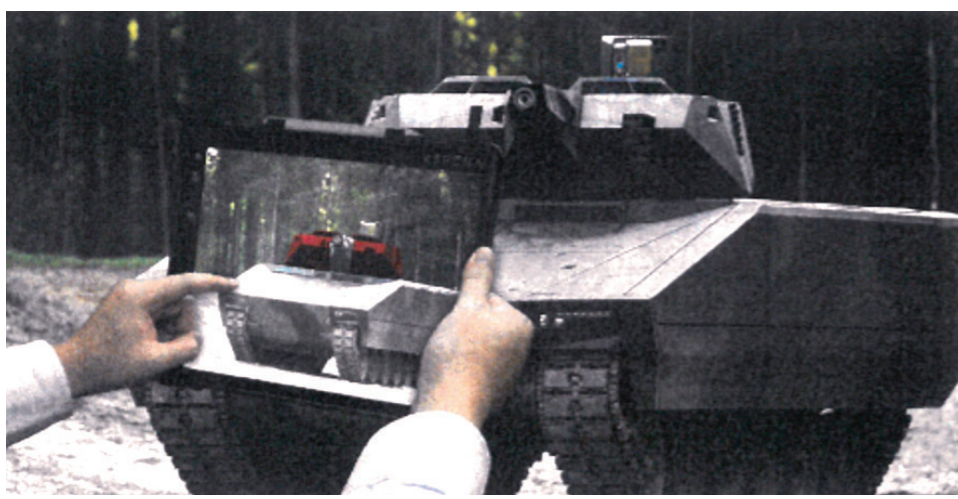


Figure 2
The Xerena System
Source: 'The Lynx Family', 80.

The user can see the information about the system through an "Augmented Reality" system in an interactive 3D model with attached documentation or training modules.

The information is updated based on a server system. The tool can be supplemented with additional components to work more efficiently.[5]

5.6. Virtual reality and augmented reality

The VR system provides additional opportunities in training. Through advanced VR goggles, the trainee finds himself in a complex virtual reality to gain profound user experience for even more effective training. No vehicle will be seized as a result and will not be damaged, for example, during maintenance training. In addition, each installation phase can be performed repeatedly on the vehicle, thus, if not new knowledge, but experience can be gained in performing that particular maintenance phase. The trainer can track the work done in the virtual space and intervene if he/she thinks he/she finds an error in the work. With the help of augmented reality, the trainer can pass on additional information during the training.

5.7. Simulation and training for Lynx KF-41 operators

Simulation training was given an essential role in familiarising prospective Lynx operating personnel with the combat vehicle. In addition to 24/7 availability, it is also a cost-effective solution and protects military technology and the environment.

The simulation can apply multiple levels of readiness, depending on where the training takes place, to fully prepare the operating personnel to perform real-life shootings. Furthermore, trainees may find themselves in situations that would be dangerous beyond a training practice, but in reality, they can quickly happen.

In addition to individual training, stage and higher unit-level training will also be possible.

6. Driver training simulator

6.1. Training stand

DTS Lynx creates a complete simulated environment from inside a combat vehicle. Allowing driving with a closed and open hatch, on the road and in the field, in different environmental conditions, such as day–night, rain, snow, etc. The cabin has been given an entire Lynx interior, with propulsion engines, sound system and visibility to make it entirely realistic. The training simulator includes:

- vehicle-specific steering, gear shifting, pedals and parking brake
- complete instrument panel
- simulated vehicle failures

[5] 'The Lynx Family', Defence Technology Review Wehrtechnischer Report 2 (2020), 81.

6.2. Desk tactical trainer

DTT is a computer system developed for classroom education by Rheinmetall. This also facilitates imitation learning with a less realistic control panel. However, it allows procedures and fighting within the framework of collective training. Doing so will help the soldiers to gain experience at the platoon or company level.

6.3. Mounted trainer

This training phase is implemented using VR technology, closing the gap between virtual and accurate training. With the help of this control of the landed infantry, its tactical procedures can be mastered without fighting vehicles on the training field. In addition, the descent trainer can work with DTT and ITT elements to train all personnel together.[6]

6.4. Cooperation

The Lynx KF-41 is a modular, task-oriented modifiable combat vehicle that enables it to operate comprehensively across the full spectrum of modern warfare. However, it will be a challenge for the soldiers to cooperate with the combat vehicle, as even more attention must be paid to combat procedures, recording and maintaining safety distances and space and distances when recording combat formations. Thus, although the Lynx KF-41 represents a significant force in any combat mission, for maximum utilisation, combat procedures must be modified in a manner that does not impede either the protection of forces or the effective destruction of the enemy. Thus, the rules of engagement should be modified according to the capabilities of the combat vehicle.

One such factor is the active self-defence system, which, considering the capabilities of the soldiers, cannot remain near the combat vehicle after a landing. Since enemy fire comes to the soldiers from the front, regardless of the inversion, it will not be advisable to place the main firepower and defence device behind the soldiers' line.

Lynx is currently the most balanced IFV, which is also the result of its sleek shape. As a result, Lynx has the necessary armour protection, the tactical capabilities of a 30mm machine gun, a shallow specific gravity, and the best weight-to-horsepower ratio, which gives it mobility and manoeuvrability. Furthermore, Lynx KF-41 has a more significant indoor space than most manually operated turret combat vehicles. Essentially nine fully equipped soldiers can sit in the personnel compartment, in addition to 3 operating personnel. The driver as well as the hatch are located on the left, which makes it easier to get in and out and allows the driver to drive with the hatch open for a better view. The driver was also given a seat with mine protection to reduce the possibility of injury in the event of a mine hit. The rear part is the

[6] 'The Lynx Family', 81.

personnel carrier compartment, which can comfortably accommodate eight soldiers if they have all their equipment.

In addition, the seats of all soldiers, placed in the personnel carrier compartment, were provided with mine protection and multi-point seat belts to protect them from possible mine hits or injuries caused by accident. At the very end of the landing space is a hydraulic ramp that ensures fast and safe embarkation and disembarkation. Every departing person leaves the vehicle here.

6.5. Adaptability

The modular Lynx KF-41 chassis can be developed into a single-vehicle family with various superstructures, providing unified logistics service and simplified design and application, which results from the vehicle's characteristics.

The Lynx KF-41 is a complete family of vehicles that supports a unified driver module, making it easier to train drivers and provide a flexible, task-oriented assembly for vehicles. Reassembly between individual superstructures can be done in a minimal infrastructure environment, if necessary, within a few hours. Different armour sets are available for peacekeeping operations, counter-insurgency operations, urban environments, and conventional open-air warfare. There is virtually no other fighting vehicle capable of such modularity as Lynx.

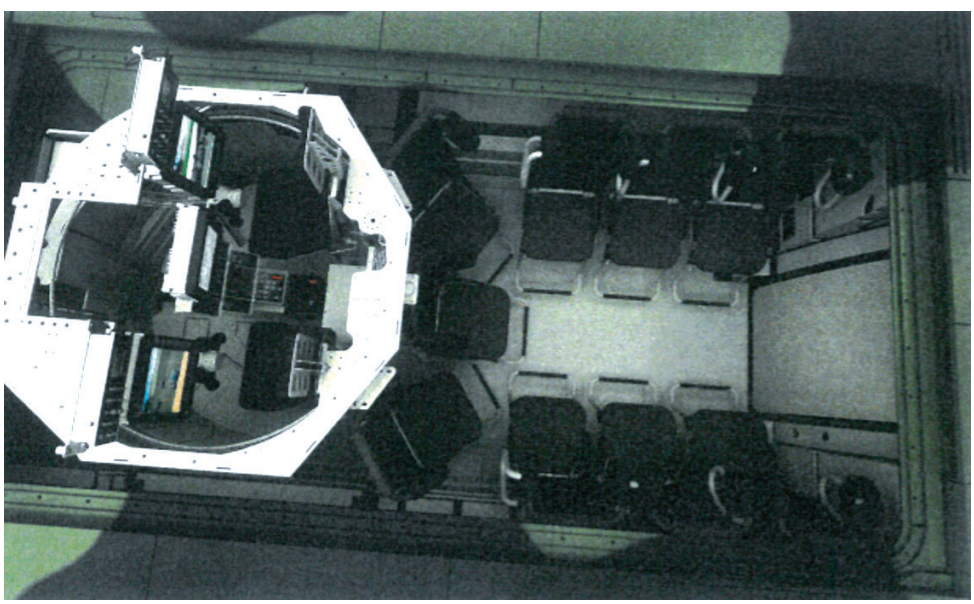


Figure 3
The interior of the Lynx KF-41 IFV
Source: 'The Lynx Family', 64.

6.6. Challenges and requirements of the self-defence system

With the advent of active defence systems, a particular challenge has emerged that needs to be addressed through combat procedures. In practice, this means that the incoming enemy projectile is destroyed by the combat vehicle's active defence system with an anti-grenade. At the same time, this results in the infantry personnel around the combat vehicle being endangered, even by their fighting vehicle, as the destruction of the projectile involves a rupture, shock wave and explosion. Thus, the safety distances, space and distances from the combat vehicle should be increased for the soldiers. So it becomes even more important how we place the combat elements on the battlefield. The position of the combat vehicle becomes even more important compared to its infantry so that the active defence system of its combat vehicle does not pose a threat to them. Furthermore, the ability of the combat vehicle to be able to distinguish the grenades of a hand-held armour-piercing device from armour-piercing enemy grenades is also important.

6.7. Self-defence

The essential equipment of the combat vehicle is the peacekeeping armoured personnel carrier. In this form, it weighs 34 tons. This can be extended up to 50 tons, with armour packs and defence packs. If even the deadliest projectiles have to withstand the Lynx in an urban environment, it weighs 48 tons, leaving 2 tons for possible future developments. Thus, the Lynx must withstand tank mines, side-armour-breaking armour, IEDs, in-vehicle IEDs and explosive devices attacking from above. It can also be equipped with passive protection against rocket-propelled grenades such as against RPG, with a mobile camouflage system and active defence.

Figure 4
The Lynx KF-41 IFV
Source: 'The Lynx Family', 64.

In essence, this makes Lynx suitable for operations of different intensities in different environments, such as:

- training tasks
- peacekeeping operations
- mechanised infantry operations
- peace support operations

For self-protection, Lynx also includes Rheinmetall's 40mm fog generation system. The design of the vehicle also allows the combat vehicle to have very low visibility, heat and sound emissions, thereby increasing battlefield survival. In order to reduce the thermal signals of the combat vehicle, the exhaust was routed to the end of the combat vehicle and is connected to the cooling system to reduce the heat of the exhaust gases.

A complete new heat shield has been developed around the barrel to reduce the heat emitted by the barrel to the lowest level available.

6.8. Destructive ability

Lynx KF-41 received the latest version of the Lance 2.0, 2-man gun turret. The turret is fully connected to the chassis, from where it receives its protection, propulsion, automatic movement and ammunition. This weapon turret is, of course, designed to be upgraded or modularly reassembled. Furthermore, its ammunition stock was housed separately from the soldiers stationed in the combat and dessants for their protection.

Figure 5
The turret of the Lynx KF-41
Source: 'The Lynx Family', 21.

6.9. Firepower

If the Lynx is equipped as an IFV, the Lance 2.0 weapon turret will be placed symmetrically in the centre of the combat vehicle. The Lance 2.0 is a two-person gun turret equipped with an automatic machine gun as the primary weapon to ensure the decisive mortality of the fighting vehicle. It uses two different versions of SEOSS-2. A unit projecting a panoramic image is available to the commander for complex observation of the battlefield. Moreover, for the aimer, a firing-sector image shows its aiming tool. Both targeting devices were equipped with monitoring instruments suitable for day, night and adverse weather conditions.

Both have a built-in laser rangefinder to aid in target marking, connected to the off-platform Battlefield Management System (BMS). This will equip the dessants with professional fire control. In addition, the tower has a task-oriented modifier module on the right side of the tower where other accessories needed for the machine gun can be applied depending on the combat mission. Examples of such accessories are:

- ATGM module
- Mortar module
- UAVs
- Electronic warfare equipment

Lance has a 30mm x 173mm MK 30-2/ABM machine gun and a 7.62mm NATO ammunition-fired parallel machine gun. The MK 30-2/ABM can be moved vertically at a maximum of +45° and –10°.

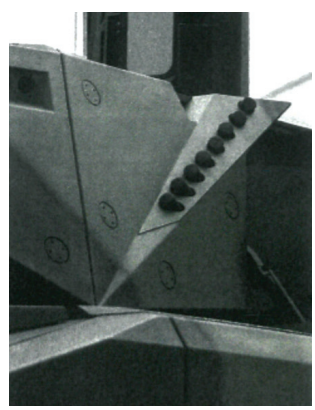


Figure 6
ROSY – Rapid Obscuration System
Source: 'The Lynx Family', 42.

In addition, the tower can be equipped with a 40mm automatic grenade launcher to destroy secondary targets that the commander can handle. This device, called MSSA (Main Sensor Slaved Armament), can also be equipped with non-lethal ammunition, promoting mass dispersal and peacekeeping.

Furthermore, the Lance 2.0 tower can trigger fire extremely quickly for moving and stationary purposes, regardless of whether the combat vehicle is moving or stationary, regardless of the weather conditions, both day and night.[7]

The aiming and commanding position were equipped with general human-controlled devices such as a turret controller and a central, multifunctional display. The commander and the aimer have a standard main operation panel and a 'general battlefield monitoring system' display. The technical variability of Lance 2.0 is limitless.

The protection of Lance 2.0 and the defence part of the turret crew and the base system are also modular. Even NATO level 6 protection can be provided to the weapon turret.

6.10. Optional accessories

In order to maximise task orientation, the turret includes an armoured, multi-purpose weapon console on the right. The container can accommodate an ATGM (Anti-Tank Guided Missile), a short-range ground-to-air missile, or a guided missile device. However, even electronic warfare devices can be placed here.[8]

6.11. High manoeuvrability

The combat vehicle has the latest generation powertrain. This is ensured by an 850 kW (1140 hp) engine and an already well-proven Renk transmission. Despite its weight differences, the new device also got a flexible undercarriage to move the modular armour properly, developed by an Australian company called Supashock specifically for Lynx. Its total combat weight, including the gun turret and the most substantial armour pack, is 45 tons. With this, it is a leader in its class when looking at the power-weight ratio, which means 26 horsepower/1000 kg. In the meantime, it will be able to carry an additional 6 tonnes of payload should it be needed in future developments.

7. Possible combat procedures with the Lynx KF-41

Observing the basic matches, Lynx is similar to the BMP-1 in its construction as an infantry fighting vehicle, only surpassing its self-defence, agility and firepower. However, the mechanised infantry soldiers will have to use the landing ramp at the rear of the fighting vehicle in the same way as in the BMP-1 after uttering command words: 'From fighting vehicle to fighting, forward!' Therefore, in examining possible combat procedures, we can rely on combat procedures with BMP-1. The main difference between combat operations is the active self-defence system of the Lynx KF-41. This

[7] 'The Lynx Family', 24.
[8] 'The Lynx Family', 22.

is because the equipment can pose a danger to its own forces during operation if they are close to the fighting vehicle. Thus, the safety distance from the vehicle must be examined in the given combat order, combat formation when placing soldiers.

In addition to the fact that the fighting vehicle is currently classified as one of the most modern shooting armour, or that has surpassed most of it, has tactical abilities and tactical factors. In light of this, the infantry combat vehicle can be placed in front of the line of soldiers since the main firepower and defence of a given subunit is the combat vehicle itself.

It is essential to look at the seizure possibilities, as this is no longer the weak armoured BTR-80 and 80/A. Thanks to this, the combat vehicle can bring the infantry as close as possible to the enemy positions so that the soldiers have to spend as little time in the open field as possible, and they have to run as little distance as possible in an attack, which can significantly extend the time of capture.

A further issue is the separation of combat vehicle operating and landing personnel. Soldiers must remain in contact with the combat vehicle even after landing. However, it is questionable whether squad commanders will leave the combat vehicle during the landing or should the combat vehicle and the carried personnel have separate commanders? Do we entrust the handling of the complete weapon system to the turret if the squad leader leaves the combat vehicle with the soldiers?

An effective solution from a tactical and managerial perspective is for four combat vehicles to form a mechanised infantry squad. All in a way, that the platoon leader is responsible for the four combat vehicles and each subordinate soldier of the section. However, the combat vehicles have a separate commander who remains in the combat vehicle turret even in combat contact. The soldier holding this position is solely responsible for the combat vehicle and its operating personnel, with the rank of non-commissioned officer.

In this case, the service foreman of the combat vehicle commanders would be the platoon leader, the platoon sergeant and the squad commander.

This would also be necessary because, in the Lance 2.0 weapon turret, the gunner has only the image of a sector. With only one person, it cannot make the most of the capabilities and abilities of the combat vehicle. So the tactically maximised use of the weapon turret's firepower and landing support capabilities can be accomplished by the work of two major teams. In this case, the organisational structure can also be maintained. The three squads have a separately organised combat vehicle, plus the platoon commander's combat vehicle for the platoon leader and other soldiers of his section (for example, platoon sergeant and radio soldier).

In this case, the number of people in the platoon would be a minimum of 40 instead of the current 29. However, filling all the seats, this is already 44 people, or if the version equipped with a 9-person landing space is regularised, in that case, it is 48 people. In addition, a new category of staff, the post of 'combat vehicle commander', should be introduced. However, in this form, a large but more manageable mechanised infantry platoon is created with high firepower. Namely, the commanding members of the section also carry out landings while retaining full use of the combat vehicle's abilities. In addition, it provides a more accurate and transparent solution

for the section commander, and the coordination of the driving of combat vehicles with the driving of the dessants is much faster, simpler, more expedient and safer.

8. The comprehensive nature of the reform

Zrínyi 2026 as a military reform, a comprehensive, system-based military development program is covering almost all areas of the Armed Forces. So in terms of this, the improvements of the infantry branch do not only lie in the systematisation of a new infantry fighting vehicle but the totality of the units unified, tactical equipment and military equipment, as well as training modernisation. In light of this, in parallel with the acquisition of the Lynx KF-41, the equipment of the soldiers will also be comprehensively developed, both in terms of personal firearms, clothing and tactical equipment, and training.

The result of this comprehensive reform is the acquisition of infantry assault rifles, CZ Bren 2, CZ P09 pistols, the standardisation of the 2015M uniform, the equipment included in the "digital soldier" tactical equipment, new protective vests and new helmets.[9]

So the acquisition of the Lynx KF-41 is only a part of the comprehensive reform. However, this is much needed, as modern battlefields require military organisations to think systematically when procuring, training and performing tasks. The Lynx KF-41 infantry fighting vehicle has also been developed to be one of the main pillars of a complex, all-encompassing system. Without the unified system, the use of military technology and tactical capabilities will certainly not be maximised, nor will the military development program significantly advance the task execution of the soldiers, if the reform does not take place at the system level.

9. Conclusion

The Lynx KF-41 brought a complex systematisation process for the Hungarian Defence Forces, which effectively affects all areas of the above-mentioned four units. So, in connection with the regularisation process, the responsible persons of the Defence Forces will have to adapt the training, organisational structure and combat procedures to the military equipment. This will be a rather complicated and lengthy process, but as a result, Hungary's armed forces will have a percussive mechanised infantry capability that has never been seen before in the country's history. With this investment, the infantry branch will leap forward roughly 50 years in time and will be up to its task perfectly in international and domestic settings.

Thus, for NATO, a modern and task-oriented ground force equipped with one of the most modern combat vehicles of today will be represented by the units of the

[9] Krisztina Budavári, 'Zrínyi 2026 program. Korlátozott lehetőségek a magyar védelmi ipar fejlesztésére', Hadtudományi Szemle 29, no 3 (2019), 143.

Hungarian Armed Forces equipped with Lynx KF-41 infantry fighting vehicles. Provided that the combat service support units are also adequately modernised, the Lynx KF-41 will provide long-lasting, effective service to protect the country and NATO.

References

'The Lynx Family'. Defence Technology Review Wehrtechnischer Report 2 (2020).

A BMP-1 harcjármű műszaki leírása és igénybevételi szakutasítása I. és II. kötet, PC/27. A Honvédelmi Minisztérium kiadása, 1980.

A Magyar Honvédség szárazföldi haderőnemének harcszabályzata III. rész – Szakasz, raj, kezelőszemélyzet, honvéd. A Honvédelmi Minisztérium kiadása, 1993.

Horváth, Tibor (ed.), A honvéd és a harcászati szintű kis alegységek (raj és szakasz szintű kötelékek) általános harcászati gyakorlati felkészítése. Oktatási segédlet. Budapest: Nemzeti Közszolgálati Egyetem, 2014.

A BTR-80 páncélozott szállító harcjármű műszaki leírása és igénybevételi szakutasítása, Gjmű/166-2, I. és II. kötet. A Magyar Honvédség kiadványa, 1994.

A BTR-80/A páncélozott szállító harcjármű típussajátosságai, 583/439. A MH páncélos- és gépjárműtechnikai szolgálatfőnökség kiadványa, 2000.

Budavári, Krisztina, 'Zrínyi 2026 program. Korlátozott lehetőségek a magyar védelmi ipar fejlesztésére'. Hadtudományi Szemle 29, no 3 (2019), 142–159. Online: https://doi.org/10.17047/HADTUD.2019.29.3.142

Farkas, Tibor, 'A védelmi tevékenységeket támogató MH Kormányzati Célú Elkülönült Hírközlő Hálózat fejlesztési lehetőségeinek vizsgálata a honvédelmi és haderőfejlesztési program (Zrínyi 2026) tükrében. Hazai/nemzetközi szakirodalmi összefoglaló'. Hadtudományi Szemle 12, no 4 (2019), 5–16. Online: https://doi.org/10.32563/hsz.2019.4.1

HADMÉRNÖK
HADITECHNIKA
16. évfolyam (2021) 4. szám 41–53.
DOI: 10.32567/hm.2021.4.4

Attila Zsitnyányi[1]

Development of Hungarian Light Armoured Vehicles for Disaster Management and Military Applications

When launching the Zrínyi 2026 program, the Hungarian Government set the goal of taking into consideration the opportunities for the development of the Hungarian defence industry with regards to procurements, and in connection with this, the Irinyi plan defined the defence industry as one of the national strategic industries. This, of course, requires domestic products, such as the Komondor[2] light armoured vehicle family developed in Hungary. The study depicts the main vehicle and model variants through the development process.

Keywords: **Hungarian defence industry, armoured vehicle R&D, RDO, Komondor, disaster management**

1. Introduction

International practice shows as an example to follow that in the performance of national defence tasks, within the framework of allied obligations, countries try to rely primarily on their own industries. But in Hungary after the change of regime, the loss of external and internal markets caused a functional and structural crisis in the military industry. The research and development background related to the sector in a narrower and broader sense has also suffered a serious decline.

The Zrínyi 2026 program can present new opportunities. An important factor in the developments is the government's consideration of the widest possible, well-thought-out revival of the domestic defence industry.

All countries with a vehicle industry have developed their light armoured vehicles adapted to modern forms of warfare, thus developing, further developing and

[1] University of Public Service Doctoral School of Military Engineering, PhD student, e-mail: zsitnyanyi@gamma-tech.hu

[2] Komondor is a Hungarian breed of livestock guardian dog; it is a large, white-coloured breed with a long, corded coat.

maintaining their own national industries. Accordingly, the design and production of the Komondor combat vehicle family will have an impact on other companies, also operating in the defence industry, and other related industries.

This study presents the historical stages of the development. It summarises the main features and capabilities of the Komondor base vehicles and model variants implemented so far.

2. Historical antecedents of the development process

2.1. Antecedents of military vehicle production in Hungary after World War II

At the beginning of the sixties, the improvement of the armour protection of the infantry units was planned in the Hungarian People's Army. The decision on the development of the Hungarian reconnaissance amphibious vehicle was made in 1960, the design process started in 1961 based on the plans of the Ministry of Defence, Institute of Military Technology (HM HTI).

The goal was to create a vehicle that would enable the detection of opposing forces and radiation contamination even in enemy territory. For this purpose, an amphibious, armoured vehicle was designed on the basis of the Hungarian D-344 Csepel off-road truck. The D-442 reconnaissance amphibious vehicle was brought into the system in 1963, the production was carried out by the Hungarian Railway Carriage and Machine Works Plc in Győr (Rába) between 1963 and 1968. A total number of 2,300 vehicles (the commercial name is FUG) were produced, of which 1,574 pieces were delivered to Czechoslovakia and Poland.[3]

Based on the FUG, the D-944 armoured personnel carrier vehicle, or PSZH[4] in its Hungarian abbreviated form, was developed. Rába started the serial production of the D-944 PSZH in 1970, 2,848 pieces were produced by the termination of its manufacturing in 1980.[5]

2.2. Why was the development started, where did the idea come from?

The supply of chemical protection and nuclear measuring instruments to the Hungarian defence forces (HDF) is one of the fields of expertise that has been continuously achieved through domestic development and production, as a result of decades of cooperation between Gamma Műszaki Zrt. (hereinafter: Gamma) and the HM HTI. Gamma (founded in 1920), as a profile owner, has been a key supplier

[3] Ferenc Hajdú and Gyula Sárhidai, A Magyar Királyi Honvéd Haditechnikai Intézettől a HM Technológiai Hivatalig 1920–2005 [From the Royal Hungarian Army Institute of Military Technology to the HM Technology Office 1920–2005] (Budapest: HM Technológiai Hivatal, 2005).

[4] PSZH armoured personnel carrier, in Hungarian páncélozott szállító harcjármű.

[5] Hadtörténeti Intézet és Múzeum, Fegyverzet és hadfelszerelés [Armament and military equipment].

of HDF CBRN[6] reconnaissance vehicle developments since the 1950s. Following the change of regime, the modernisation of the VS[7] BRDM vehicles was started in 2001, for which Gamma developed an onboard CBRN reconnaissance system.

In 2007, this system was further developed on the basis of BTR-80 (as BTR-80 VSF[8]). Subsequently, there were constant requests from abroad to supply a complex CBRN reconnaissance vehicle, when they realised that in the absence of a domestically manufactured vehicle, they could not provide a competitive offer. This highlighted a very important problem of the Hungarian defence industry; namely, if there is no carrier device, then the chances of selling vehicle-mountable systems are minimal.

Figure 1
VS BRDM-2, BTR-80 VSF
Source: Gammatech, Gamma Company Profile.

2.3. Development of disaster management capabilities

In 2007, the company also began to develop in other areas related to vehicle manufacturing. As a result, the Disaster Management Mobile Laboratory (KML[9]) developed by Gamma and its reduced capability versions (KML ADR) appeared in the application of BM OKF.[10] They are capable of emergency assessment, radiation and chemical detection, decontamination, and they also function as a mobile office when performing roadside checks.

6 CBRN: Chemical, Biological, Radiological and Nuclear.
7 VS – NBC: Nuclear Biological Chemical.
8 VSF – NBC reconnaissance.
9 KML: Hungarian abbreviation of Disaster Management Mobile Laboratory.
10 BM OKF: Hungarian name of National Directorate General for Disaster Management, Ministry of the Interior.

Figure 2
KML, KML ADR vehicles
Source: Gammatech, Gamma Company Profile.

In 2010, as one of the leading companies in the Hungarian defence industry, Gamma launched Hungary's first independent light armoured vehicle development project. During the past years, the expansion of the vehicle family, the modernisation of the existing vehicles, the installation of new solutions and, of course, the design and construction of new versions to satisfy the emerging customer needs have been ongoing. In this article, in addition to describing the development process, I focus on the technical details of the implemented vehicles, and I present the additional possibilities inherent in the vehicle family.

3. Main steps in the development of light armoured vehicles

3.1. The beginnings

In 2010, Gamma started to develop the concept of a complete light armoured combat vehicle family and its possible model variants. The aim of the development was to create a base vehicle family that meets the application principles of NATO and satisfies the needs of the users and operators of the Hungarian Defence Forces, with sufficient protection, firepower, agility, survival, etc. and, as a result of its design, is suitable, or can be made suitable for any special tasks.

3.2. The RDO-3221 Komondor

The first base vehicle version of the vehicle family with type identifier RDO-3221[11] was manufactured during the implementation of the project awarded in state scheme

[11] In the numbering of vehicles, "RDO" is the name referring to the manufacturer (abbreviation for "Respirator Design Office" refers to the Respirator company, which started the development and merged into Gamma Műszaki Zrt. in 2015). The first two digits of the number combination refer to the wheelbase, followed by the number of axes, followed by the design ID. (Based on these, 3221 is interpreted as 3200 mm wheelbase, 2 axles and a closed body.)

"Encouraging Corporate Innovation (KMOP 1.1.4-09)" announced by the National Development Agency (NFÜ) in November 2010. As the traditional profile of Gamma, the main focus was on presenting the NBC reconnaissance capability that can be integrated into a vehicle. However, the basic technical solutions that characterise the whole vehicle family have also appeared, a welded self-supporting armour body that also standardises the external appearance, with a 'V' shape lower part running along the entire length of the vehicle.[12]

An Iveco Tector 279 diesel engine was installed in the body manufactured by Gamma. The undercarriages are rigid, wheel-reduced, semi-elliptical leaf-suspension, with hydraulic shock absorbers. Both axles have electronically controlled, pneumatically activated cross differential locks. Depending on the primary infantry character, the design can accommodate a staff of 2 + 7 persons.

As a result of the development, in addition to the base vehicle, the first type variant was the RDO-3221 CBRN.[13] The vehicle's equipment and on-board detection system (chemical, radiation and biological detectors, sampling and collective protection devices) are built based on the most advanced technical solutions available.

Figure 3
RDO-3221 CBRN with add-on armour
Source: RDO Komondor.

[12] Gammatech, Gamma Komondor MRAP.
[13] Miklós Kovácsházy, 'Az RDO Komondor többcélú páncélvédett járműcsalád I. rész', Haditechnika 49, no 4 (2015), 50–53.

The construction of one of the most complex type variants (CBRN) proved that practically any other capability suitable to be placed in the useful space given, may also be implemented in the base vehicle (e.g. gunnery, reconnaissance, ambulance, anti-tank missile, technical recovery, law enforcement vehicles).

3.3. The second generation vehicles

Following the successful implementation of the RDO-3221, a new chapter in the development of the vehicle family has started. The capabilities have already been designed in accordance with the specific requirements defined by potential users, some elements of the transmission system have changed. The previous rigid suspension has been changed to an independent suspension and the manual transmission has been replaced by an automatic one. Based on these new principles, the development of the RDO-3921, intended to be the successor of the RDO-3221, and also its big brother, the RDO-3932 with a 6 x 6 wheel formula, was started with the aid of a scheme announced by the New Széchenyi Plan, Research and Technological Innovation Fund in 2012.

3.4. The RDO-3921 Komondor

The second version of the vehicle family was a 4 x 4 version, permanent all-wheel drive with independent suspension system. It is powered by a Cummins ISLe diesel engine with a maximum output of 340 hp. Developed specifically for heavy trucks and military purposes, this engine drives nearly 70% of similar LAV[14] vehicles. The propulsion delivered by the vehicle's engine is transmitted to the transfer case via an Allison 3200 SP six-speed automatic transmission.

The vehicle's drive axles come from a special military ISAS 4000 series made by the U.S.-based AxleTech company's factory in France. An equipment of the Hungarian company Silex, which manufactures several modules of the vehicle's electronic system, can pre-program the air pressure values for different road conditions and load levels, even to different degrees for each wheel.

According to the relevant standard (NATO STANAG 4569[15]) classification, the composite armour solution, implemented on a prototype vehicle and tested in shot tests, provides level 2 ballistic protection as standard. During the ballistic tests, several composite solutions have been developed (ceramic, armour plate, internal cover) so that the ballistic protection of the vehicles can be increased up to level 4. Based on the performed simulations and tests, the vehicle's self-supporting body, which protects both the engine and crew compartments, the 'V' shape armour, the technical solutions and special safety elements applied in the interior, successfully protect the crew at protection level 3a/3b in case of explosion.

[14] LAV: Light Armoured Vehicle.
[15] NATO STANAG 4569: Protection Levels for Occupants of Armoured Vehicles.

Figure 4
RDO-3921
Source: RDO Komondor.

To demonstrate the variability of the RDO-3921 base vehicle, the prototype was developed in two model variants. The basic 2 + 8 person transport version can be converted into a casualty transport vehicle – suitable for 3 + 2 inpatients or 6 seated casualties – by the operating staff in a short time.

3.5. The RDO-3932 Komondor

A 6 x 6 all-wheel drive, half armoured body version of the vehicle family. Due to its design and good off-road capability, depending on the replacement superstructure used, it can be utilised for many different purposes, from ambulance, C2, technical recovery, CBRN reconnaissance, minesweeper or logistic vehicle.

Considering the family principle in the applied technical solutions, it is almost exactly identical with the RDO-3921 4 x 4 base vehicle, the only differences are in the parameters of the individual components and in the three-axle design.

Higher vehicle weights require a more powerful powertrain. Accordingly, the Cummins 6-cylinder engine, which is identical in design with the smaller version, delivers 450 hp and 1640 Nm of torque to the more robust 4000 Series Allison automatic transmission, thanks to a different charging system. In order to meet the hydraulic energy requirements of the superstructure, a stationary hydraulic pump that can be connected to the transfer case has been installed.

Figure 5
RDO-3932
Source: RDO Komondor.

The RDO-3932 prototype is suitable for transporting 2 + 3 persons in a half armoured, double cabin design; of course, this version can also be made with a fully enclosed armoured body. In this case, in addition to the current dimensions, it can be used to transport 2 + 12 persons and their equipment. In order to demonstrate the possibilities, a technical recovery superstructure was developed for the completed prototype vehicle. This assembly can be easily dismantled and replaced with other replacement superstructures, ensuring targeted multifunctional applicability.

3.6. The first sale

The first sale took place in 2015. As the winner of a public procurement procedure, Gamma entered into a contract with MVM Paksi Atomerőmű Zrt. (MVM Paks Nuclear Power Plant Ltd.) for the supply of a "radiation-shielded vehicle". The company had not yet had a vehicle that fully complied with the tender requirements, so it was a perfect opportunity to present the possibilities of the vehicle, to prove the company's capabilities as well as the viability of the domestic implementation of a vehicle of such complexity.

A vehicle suitable for satisfying the special needs specified by the Accident Prevention Department of MVM Paks Nuclear Power Plant Ltd. was developed on the basis of the RDO-3221 vehicle. The vehicle is simultaneously equipped with radiation shielding, a certain level of physical protection and off-road capability, and a radiation protection monitoring system. In order to achieve the required attenuation of gamma radiation, the body had to be thickened at several points; special glass, providing radiation protection was installed and the driver and staff compartments were separated. With the decontamination possibilities in mind, the interiors were given

a flexible polyurethane cover. In addition to the filtering (ventilation) system, which also provides the required overpressure, based on the requirements of the tender, an individually developed radiation measuring and alarm system (by Gamma) has also been integrated into the vehicle.

Figure 6
RDO-3221 RSV
Source: RDO Komondor.

3.7. The RDO-3121 Komondor

During the development and testing of the existing model variants, the need arose to create a vehicle that is smaller in size but has greater protection even without the use of composite systems. In its appearance, equipment and basic construction, the RDO-3121 follows the family principle; it is the smallest member, is nearly a meter shorter, and it is also significantly lower compared to its counterparts. Its interior provides the possibility to transport 2 + 3 persons, to create workplaces and there is enough space left for the integration of special systems, for transporting load. The 6.7-liter Cummins engine built into the vehicle, due to its lower environmental rating, is capable of 364 hp at 1,100 Nm of torque. Due to the lower torque, the vehicle has been given a different gearbox (ZF VG 750), which, however, has a three-speed, switchable longitudinal differential lock, similar to its predecessors. The armour of the RDO-3121 prototype provides a higher level of ballistic protection as standard (STANAG 4569 level 3).

Figure 7
RDO-3121
Source: RDO Komondor.

Like the other members of the vehicle family, the prototype vehicle can be manufactured in different sizes, equipment and interior layout.

4. Development of new versions for disaster management (also) purposes

4.1. Historical background

In previous developments, the company has emphasised that the prototypes are basically used to showcase the capabilities of the vehicle family, and are ready to "make" it based on any domestic or foreign needs. In 2018, the time for proof came, an international tender was launched for the supply of S3 category, double cab, multi-purpose vehicles (where the previously developed Komondor versions did not meet the technical requirements set by the tender). Gamma, as the winner of the public procurement procedure, delivered three double-cab, multi-purpose vehicles to BM OKF. The RDO-4336 vehicles, which were launched in the summer of 2020 and have special interchangeable superstructures, are based on a new version of the base vehicle with the RDO-4332 type identifier which was developed within 1 year due to the contract.

4.2. The RDO-4336 Komondor

The multi-purpose, double-cab base vehicle with interchangeable superstructure carries the characteristics of the vehicle family, but due to its intact uniqueness, it also

shows many differences in the technical solutions. The vehicle has a self-supporting armour body, which ensures its applicability even when approaching focal points where there is a risk of explosion and consequently the possibility of fragmentation. The base vehicle is capable of carrying 2 + 4 persons under difficult terrain conditions with a large amount of water and/or equipment. In order to meet the applicability requirements, the base vehicle is fitted with integrated fire extinguishing elements, a front adapter to accommodate a worktop, hydraulic power supply systems, a quick-acting extinguishing device and its accessories.

To meet the requirements, this variant is powered by the 500 hp 2300 Nm Euro5 environmental rated 12-liter Cummins engine, the first ones implemented in vehicles in Europe. AxleTech ISAS 4500 undercarriages were fitted to the vehicles, which were different from the previous ones, with a stronger load-bearing capacity, but also with an independent suspension solution.

The vehicle consists of three separate units, the base vehicle, the water transporter/forest firefighting superstructure and the technical recovery superstructure.

BM Heros Zrt. carried out the firefighting design of the vehicle and the construction of the water transporter/forest firefighting superstructure. The bodywork includes a 7,000 litre water tank and a fire extinguishing pump capable of foam mixing as well, which supplies the remote-controlled front nozzles, the emergency extinguishing and self-defence systems with low or, if necessary, high-pressure extinguishing agent. It provides an opportunity to apply water to operational areas that are difficult to access from a road supply point or are inaccessible by road vehicles. The vehicle is also suitable for carrying out professional tasks standard for conventional fire trucks.

The technical recovery superstructure provides the ability to intervene through integrated hydraulic systems (11 tm self-loading hydraulic crane, fork-lift truck) and loaded technical rescue equipment (hydraulic cutting/tensioning, support, lifting equipment, aggregator, tools, etc.) which are especially useful in the event of extensive road accidents.

Figure 8
RDO-4336, with different superstructures
Source: RDO Komondor.

The RDO-4336 Komondor vehicle-based professional capability can be expanded by additional individual superstructures if required.

5. The future

The development of the vehicle family will not stop with the fulfilment of the contract either. On the basis of the existing base vehicles, additional model variants, superstructures and accessories will be made by the 100 years old Gamma. In the framework of a new R&D project, in addition to the RDO-4332 base vehicle version, Gamma will develop a universal open and a universal closed superstructure. With minimal modifications and possible special additions, due to the basic protection of the vehicle, it can be used well by other defence or law enforcement organisations, not only for disaster management tasks.

The available R&D funds, of course, allow for larger-scale developments, but self-financed developments will not be stopped either. Based on a special customer requirement, an extended (L) version of the RDO-3121 is being designed, which will be an extended and elevated version of the base vehicle with modified interior layout and doors in accordance with individual application requirements. By retaining the original wheelbase, the vehicle's manoeuvrability is maintained, which is particularly advantageous in applications in urban environments. The increased interior provides the opportunity to create a unique workplace, to accommodate an increased number of operators and special equipment. Despite the changes indicated, it will be smaller than the next RDO-3921 in the vehicle family in size, and of course, in the event of additional user demand arising, this version will also be available in single or double cab flatbed versions.

In the context of military and disaster management applications, there is already a need to use remotely controlled or even self-controlled vehicles for certain special, particularly dangerous operations. It may be useful to control vehicles remotely to reduce the need for manpower, to protect it, or to perform simple routine tasks. In special operating environments, remotely controlled as well as self-driving vehicles may also be needed. In this case, there is no need to compromise on the usability/deployment requirements for the protection of manpower, the vehicle and superstructure can be optimised during design to perform the task.

Hungary's ambitions in the field of autonomous vehicle research provide a huge opportunity for participants in domestic and foreign testing, sensor, vehicle and application developers. Based on the experience gained during the development of the Komondor vehicle family, one of the long-term goals of Gamma is to create new, remotely controllable base vehicle family members that can be made suitable for self-driving. As a result of the ongoing development, such vehicle version will be created, which will also provide other developers and research institutes with the opportunity to test their own solutions or present their existing related products.

6. Summary

International practice shows as an example to follow that in the performance of national defence missions, within the framework of allied obligations, countries seek to rely primarily on their own industries. Most countries with an existing vehicle industry have built their light armoured vehicles adapted to modern forms of warfare, thus developing, further developing and maintaining their own national industry.

When launching the Zrínyi 2026 program, the Hungarian Government set the goal of taking into consideration the opportunities for the development of the Hungarian defence industry with regards to procurements, and in connection with this, the Irinyi plan defined the defence industry as one of the national strategic industries. This, of course, requires domestic products, such as the Komondor light armoured vehicle family, developed and manufactured by Gamma.

Through the example of the development of the Komondor vehicle family, Gamma has proved that the Hungarian military industry has the necessary capabilities to develop, manufacture and provide full-lifecycle logistic support and later modernise a vehicle family or other products of similar complexity suitable for Hungarian defence tasks. Of course, this also requires foreign partners with whom co-created products can even be sold to third countries.

References

Gammatech, Gamma Company Profile. Online: http://gammatech.hu/downloads/cat/Gamma_company_profile.pdf

Gammatech, Gamma Komondor MRAP. Online: http://gammatech.hu/downloads/cat/Gamma_komondor_MRAP.pdf

Hadtörténeti Intézet és Múzeum, Fegyverzet és hadfelszerelés [Armament and military equipment]. Online: https://m.militaria.hu/digitalis-hadtortenelem-hadtortenelmi-oktatasi-csomagok-iskolak-szamara/magyar-nephadsereg-es-varsoi-szerzodes/magyar-nephadsereg-es-varsoi-szerzodes-fegyv-hadfelsz

Hajdú, Ferenc and Gyula Sárhidai, A Magyar Királyi Honvéd Haditechnikai Intézettől a HM Technológiai Hivatalig 1920–2005 [From the Royal Hungarian Army Institute of Military Technology to the HM Technology Office 1920–2005]. Budapest: HM Technológiai Hivatal, 2005.

Kovácsházy, Miklós, 'Az RDO Komondor többcélú páncélvédett járműcsalád I. rész'. Haditechnika 49, no 4 (2015), 50–53.

NATO STANAG 4569, Protection Levels for Occupants of Armoured Vehicles.

RDO Komondor. Online: www.facebook.com/rdoKomondor

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
16. évfolyam (2021) 4. szám 55–66.
DOI: 10.32567/hm.2021.4.5

Zoltán Őze[1]

Weapons of Mass Destruction and the Secret Services

The threat posed by chemical, biological, radiological and nuclear (CBRN) weapons has been growing for years due to technological advances and the changing political environment. These weapons are attractive to states mainly because of their deterrent value, and non-state actors, especially terrorist groups, may use them causing an enormous psychological impact. The diversity of the threat is increased by the recent and highly unusual trend of attacks by state actors in Europe and Asia using CBRN weapons. How should states deal with this new threat? Does it imply a new set of tasks for CBRN protection?

Keywords: **secret services, CBRN weapons, CBRN protection**

1. Introduction

CBRN weapons caused hundreds of thousands of deaths in the wars of the previous century, decimating both soldiers on the battlefield and civilians in the cities of the hinterland. The images of the massacres are so deeply etched in the memory of societies that countries around the world have signed international treaties to ban toxic, infectious and nuclear weapons. Nevertheless, the proliferation of nuclear weapons remains a real threat and chemical weapons are still present in the war zones of the Middle East in the present times. Terrorists are also seeking to acquire weapons of mass destruction.

Even more worrying is the recent inclusion of chemical weapons in the arsenal of certain countries' secret services, but interestingly, they are not used to destroy the masses, but to eliminate target individuals. The nerve agent attacks in Europe and East Asia have led to a radical reassessment of the CBRN threat.[2]

[1] University of Public Service, Faculty of Military Science and Officer Training, Institute of Military Course Management, Senior Officer, e-mail: ozezoltan@gmail.com

[2] Simon Schofield, 'Toxic Relationships: A History of CBRN Assassinations', 25 March 2018.

2. The new threat: assassinations with weapons of mass destruction

In addition to the emergence of chemical weapons in war conflicts, an unusual phenomenon has emerged in both Europe and Asia: assassinations with CBRN agents.

On 13 February 2017, a weapon of mass destruction was used to assassinate the half-brother of North Korean dictator Kim Jong Un, Kim Jong Nam, at Kuala Lumpur International Airport in Malaysia. Kim was about to board a plane when a Malaysian and a Vietnamese woman smeared two kinds of drugs in his face. The two components mixed together to form VX neurotoxin on Kim's skin, killing him within minutes. During the operation, at least four North Korean agents were waiting nearby, ready to intervene if anything went wrong. After the assassination, the four North Korean agents left the airport in a hurry to avoid being directly accused of the assassination by North Korea. The two women who sprayed the ingredients of the two-component poison in the victim's face claimed they knew nothing about the assassination, believing they were part of a TV hoax.[3]

The Russians have gone even further – as if the diversity of chemical weapons developed so far was not enough – by using the Novichok (Figure 1), born in the Soviet-era laboratories. The poison causes muscle spasms that stop the heart, causes fluid to build up in the lungs, which can also be fatal, and can damage other organs and nerve cells. In the 1980s and 1990s, a new family of nerve toxins was developed against NATO forces and exists in powder, liquid or aerosol form. For nearly three decades, since a Soviet informant told the world of the compound's existence, Novichok has struck fear into the hearts of U.S. weapons experts. The Pentagon has even sent special units to Uzbekistan to destroy abandoned laboratories that once produced the chemical.[4] Because the development was top secret, nothing concrete is known about the properties of the substance, but experts believe the new family of nerve agents, known in Russian as 'new guy', is orders of magnitude more deadly than Sarin or VX, which are well-known in the West. Until 2018, there was no sign that it had ever been used.

On 4 March 2018, however, Sergei and Yulia Skripal were poisoned in Salisbury, U.K.[5] Analysis of samples taken at the scene revealed[6] the discovery in Salisbury of a Novichok chemical weapon that was not on the CWC's list of prohibited substances.[7] Since then, a proposal has been submitted to the organisation to add a new family of chemical weapons to the ban list. But the case did not end there: on 30 June 2018, 45-year-old Charlie Rowley and his partner, 44-year-old Dawn Sturgess, were taken ill at their Amesbury home, 13 kilometres from Salisbury. According to Rowley's account, he found a perfume in a bin, took it home, opened it together and 15 minutes after using it, they were sick. Both were transported from their home in Amesbury to Salisbury Hospital a few kilometres away. Tests proved that they had the same

[3] Oliver Holmes and Tom Phillips, 'Kim Jong-nam killed by VX nerve agent, say Malaysian police', The Guardian, 24 February 2017.
[4] Louise Hidalgo, 'World: Asia-Pacific US dismantles chemical weapons', BBC News, 09 August 1999.
[5] Ellen Barry and Ceylan Yeginsu, 'The Nerve Agent Too Deadly to Use, Until Someone Did', The New York Times, 13 March 2018.
[6] UK Delegation to the OPCW, 'Update on the Use of Nerve Agent in Salisbury, United Kingdom', 13–16 March 2018.
[7] Richard Pérez-Peña, 'What Is Novichok, the Russian Nerve Agent Tied to Navalny Poisoning?', The New York Times, 02 September 2020.

Novichok in their bodies as Scripal had had in his a few months earlier. Dawn Sturgess tragically died of poisoning. The perfume bottle is believed to have been one of the items used in the assassination attempt on Skripal.[8]

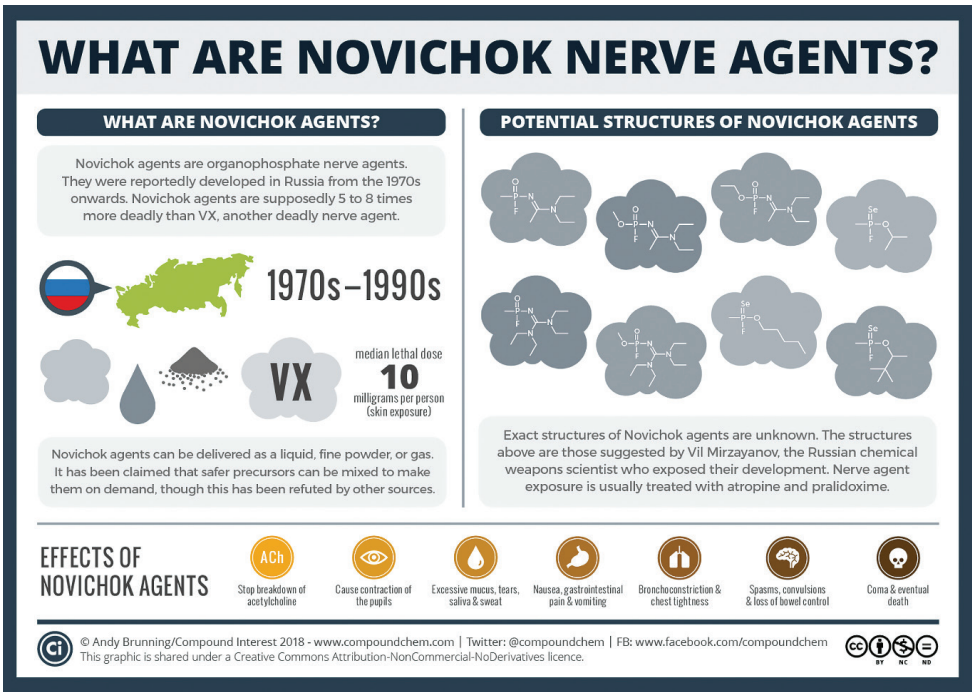


Figure 1

All you have to know about Novichok

Source: Compound Interest, 'What are Novichok agents? What we do (and don't) know about them', 12 March 2018.

That the use of poisons is a common tool in Russian politics is illustrated by the following incident: on the morning of 20 August 2020, Russian opposition politician Alexei Navalny suddenly fell ill on a flight from Tomsk to Moscow. On board of the plane, he started to feel strange and passed out. He went to the toilet to wash up, but by then he felt that he was in big trouble. When he came out of the toilet, all he could suddenly say to the flight attendant was: 'I've been poisoned. I'm dying.' Then he collapsed, and his last memory is of being asked if he had a heart disease. Alexei Navalny was then absolutely certain that he was going to die. He said the plan was that if he died on the plane and was put in a morgue, it would never be revealed that he had been poisoned. 'It was just going to be a suspicious death.' But the plane stopped in Omsk, where Navalny was rushed to hospital and put on a respirator.[9] After the politician, who was in a medically induced coma, was taken to Berlin for treatment

[8] Jordan Davis, 'Salisbury Novichok clean-up mission 'couldn't fail',' BBC News, 12 December 2019.
[9] BBC News, 'Alexei Navalny, 'Poisoned' Russian opposition leader in a coma', 20 August 2020.

on 22 August, a sample of his body taken at a special Bundeswehr laboratory clearly showed the presence of a substance belonging to the Novichok family of neurotoxins.[10] German laboratory tests showed that Navalny was poisoned with a new type of Novichok combination, not the one used against Sergei Skripal in 2018. Novichok is a special neurotoxin that can only be produced in state-controlled laboratories with the most advanced equipment. The poisoning of Navalny has led to very serious diplomatic tensions between Germany and the European Union and Russia.

On 14 December, according to the German news magazine Der Spiegel, it was reported in the world press that Alexei Navalny, the most important figure in the anti-Putin Russian political forces, had been poisoned by a special unit of the Russian National Security Service in a covert operation. This in itself is not ground-breaking news: German military scientists, two independent European laboratories and the Organisation for the Prohibition of Chemical Weapons (OPCW) have already identified[11] the compounds found in Navalny's body as nerve agents belonging to the group of Novichok, developed in the former Soviet Union. Although strictly speaking they are new and not yet on the list of banned warfare nerve agents. European countries and the U.S. Government have accused the Russian Government of the poisoning attack on this basis – Moscow has denied the allegations all along, with official communications claiming that Navalny's sickness was caused by circulatory failure and that if any poison entered his body, it was not in Russia.

The European Union (EU) was unimpressed by it. In mid-October, senior Russian state officials close to Putin – Alexander Bortnikov, Director of the Federal Security Service (FSB), Sergei Kiriyenko, Deputy Head of the Presidential Administration, Andrei Yarin, Head of the Internal Policy Department of the Presidential Administration, and Alexei Krivorushko and Pavel Popov, two Deputy Defence Ministers, and the State Research Institute of Organic Chemistry and Technology (GosNIIOKhT) have been banned from the EU. Their assets[12] have also been frozen for violating international conventions on banned neurotoxins.

The case is essentially closed, the judicial system of neither country has officially addressed the question of who, why and how Navalny was poisoned, nor the Russian authorities have launched an investigation, as their version of events is that there was no poisoning in the first place. Then a few journalists and a little-known investigative portal founded a few years ago came along and in a single article they uncovered the movements of the secret agents of the Russian secret service, the FSB, specially trained in chemical warfare, and identified the members and leaders of the unit, including those who were active near Navalny on the day of the poisoning.[13] The entire Navalny operation was reconstructed going back years and even details of the operation of Russia's secret and banned chemical weapons programme, which according to the

[10] Summary of the report on activities carried out in support of a request for technical assistance by Germany. Online: www.opcw.org/sites/default/files/documents/2020/10/s-1906-2020%28e%29.pdf

[11] Organisation for the Prohibition of Chemical Weapons, The Hague, 03 March 2021.

[12] European Council, 'Use of chemical weapons in the assassination attempt of Alexei Navalny: EU sanctions six individuals and one entity', 15 October 2020.

[13] Bellingcat, 'FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning', 14 December 2020.

official version was closed by 2010 at the latest. It is a shocking article, giving the full names, photographs, drone footage of the eight-man from the FSB unit and exact address of a secret chemical weapons laboratory operating near Moscow. Although they had no direct evidence that these eight people had carried out the poisoning, Alexei Navalny, referring to this investigation, claimed that Russian President Vladimir Putin was behind the assassination attempt. The article mentions the 'Kaliningrad fiasco', the incident in which members of the task force accidentally poisoned Navalny's wife, Yulia Navalnaia, during a romantic beach holiday of the Navalny couple.

Based on call logs and personnel connections, it is claimed that the special unit belongs to the Institute of Criminalistics within the FSB, which was created in 1977 as a high-tech investigative sub-unit of the Soviet state security service, the KGB. In the legal institute, which still provides forensic tools for investigations, the secret laboratory has apparently continued to operate and is still located in the same place, at 2 Akademika Vargi Street. The main man behind the covert chemical weapons programme at the Institute of Criminalistics is Stanislav Maksakov, who until the official closure of the chemical weapons programme worked in the closed military town of Shikhan (as of 1 January 2019, the city is no longer closed), where experts believe that Novichok-type nerve agents used to be produced, and that this laboratory may have been the source of the nerve agent used in the Skripal assassination, but that the area also contains large quantities of other chemical warfare agents.

All the signs are that the Russian chemical weapons programme, which was supposed to have been dismantled, has in fact been dispersed into a network of state or state-related institutions, with the nerve agent specialists being taken over by laboratories or institutes that have a legitimate front.

It is believed that two laboratories, the St Petersburg-based Experimental Medicine Institute (GNII VM), part of the Ministry of Defence, and SC Signal in Moscow, are active in the Novichok programme. These are officially masquerading as laboratories for military defence purposes or as protein drinks development for athletes. They came under Bellingcat's[14] radar because both labs made a lot of calls to the Russian Military Intelligence, i.e. to the GRU, with phone numbers linked to the Novichok attack on Sergei and Yulia Skripal. The laboratories are likely to continue to be supported by the military facility 33 in Shikhan, also belonging to the Ministry of Defence, the Scientific Research and Experimental Institute.[15]

However, a fourth laboratory, the Moscow-based State Scientific Research Institute of Organochemistry and Technology is on the EU's banning list – the reason given is that it is responsible for the destruction of nerve agents left over from the Soviet era. In an earlier article, Bellingcat reports that the EU has sanctioned Institute 33 and GosNIIOKHT, but that the other two laboratories, which were involved

[14] Bellingcat is an independent international collective of researchers, investigators and citizen journalists that uses open source and social media to investigate a wide range of topics – from drug lords and crimes against humanity in Mexico to tracking the use of chemical weapons and conflicts around the world. Online: www.bellingcat.com/about/

[15] Máté Pálos, 'Hogyan buktatta le pár újságíró a titkos orosz Navalnij-műveletet?', Magyar Narancs, 17 December 2020.

in the background work on the Skripal and Navalny assassinations, are apparently operating freely.

One interesting fact about the Bellingcat articles is that these texts are not summaries of Western intelligence material and intelligence reports, but the results of the journalists' own investigations. To prove this, the journalistic team[16] wrote a separate article entitled 'Hunting the Hunters: How We Identified Navalny's FSB Stalkers', which is a unique example of open source intelligence (OSINT) journalism and data use.

The journalists essentially exposed the Russian secret agents by cross-referencing the relevant databases, many of which were bought on the Russian black market. Lax Russian data protection legislation is the basis for all these (this is especially true for the civilian sector). There is a continuous leakage of data and a well-organised and active black market in leaked databases. With a few creative Google or Yandex searches and a few hundred euros of cryptocurrency in your virtual pocket, you can access mobile phone data (calls and geolocation), flight passenger lists, individuals' registered addresses or even the number plates of cars they have ever owned, through a simple automated interface. Many databases have long been circulating on torrent sites, but new data can also be ordered from various data brokers, the latter being somewhat more cumbersome.[17] The Russians have acted: in December 2020 they adopted the Law on the Privacy of Operatives' Data and their Activities, which further tightened[18] data protection for the GRU and FSB.

Bellingcat stresses that this investigation is made possible by the shortcomings of Russian data protection and data management practices and the booming data black market, which would not be accessible in other countries of the world – the specificities of the Russian system were used to expose the Russian system.

While it is highly doubtful that the phone numbers of the GRU can be obtained from open sources, as mentioned in the article, the pervasive corruption means that a lot of information can be obtained for money.[19] The Russian position, however, stresses that such results could not have been achieved by journalists without the powerful support of Western intelligence organisations. There is no investigation into the attempted assassination of Navalny, nor is Moscow investigating the matter. This may be partly because official requests for information from the Russian authorities (six official requests to German, Swedish and French authorities) have been systematically rejected. Neither the German doctors treating Navalny nor the Swedish and French laboratories carrying out the toxicology tests have been willing to cooperate. This information was intended to prove the fact of Novichok poisoning, on the basis of which the investigations could have been launched. This level of non-cooperation is truly incomprehensible. The Russians claim that no trace of poisoning was found before the transport of Navalny to Germany.[20]

[16] Aric Toler, 'Hunting the Hunters: How We Identified Navalny's FSB Stalkers', Bellingcat, 14 December 2020.
[17] Pálos, 'Hogyan buktatta'.
[18] The State Duma News, 22 December 2020.
[19] Szabad Európa, 'Célkeresztben a Navalnij-mérgezésről szivárogtató orosz biztonsági tisztek', 07 March 2021.
[20] 'Mandates of the Special Rapporteur on extrajudicial, summary or arbitrary executions; and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', 30 December 2020.

Also according to an article in Bellingcat, Bulgarian arms dealer Emilian Gebrev believes that he was poisoned by Russian intelligence services in April 2015.[21] The Bulgarian entrepreneur and arms and ammunition dealer became increasingly ill on 27 April 2015 after a business dinner in Sofia. His eyes itched and bled all the next day, but the businessman refused to miss that day's business dinner, where he met Polish and Russian businessmen. During the dinner Gebrev started hallucinating and vomiting. He was immediately taken to hospital.

Shortly afterwards, his adult son and a manager of his business also became sick and were also taken to hospital.[22] The businessman recovered and sought help from international chemical laboratories to find the substance that had poisoned him. The Verifin laboratory in Finland took on the job and detected traces of two chemicals in the man's urine. One was identified as organophosphate. The group of organophosphate-type compounds includes various pesticides and neurotoxins developed for military purposes. This is an occasion for the conspiracy theorists to get really excited about, because even with a large dose of imagination, there are only traces of a Russian thread in the case.

What these attacks have in common is that state actors are invariably behind them. Although the suspected states consistently deny in all forums that they are involved in the attacks, the circumstantial evidence does not support this.

One such piece of evidence is the extremely limited access to nerve gases. Since the production and storage of nerve gases is a very complex process, access to the stocks is not easy for unauthorised persons. Historical examples show that VX or Sarin have only been used in war conflicts or through assassinations. The only exception to this is the terrorist attack with VX in the Tokyo subway in 1995.

Another example of such restricted material is radioactive polonium (Po210). The world's annual production of polonium is estimated to be about 100 grams.[23] This alpha-emitting material has certainly played a major role in one assassination, and only probably in another.

In November 2014, Yasser Arafat, President of the Palestine Liberation Front, died in a military hospital in France, a month after a sudden illness that started with diarrhoea, vomiting and abdominal pains. After Arafat's hospitalisation, a great many medical tests were carried out to find out the cause of his illness. Urine and stool samples were also subjected to radiological tests, but as all the results were negative, no diagnosis could be made. However, after his death, the clothes he wore in the hospital showed unexplained and higher than normal levels of radioactivity of polonium 210.[24] Some sixty samples of the remains were taken and distributed among the Swiss, French and Russian experts who were asked to take them. The tests were carried out independently and separately, in strict secrecy, and the results were contradictory. Russian and French medical experts reported that Arafat's death was not caused by polonium poisoning, while experts at the Institute of Radiophysics

[21] Bellingcat, 'Third Skripal Suspect Linked to 2015 Bulgaria Poisoning', 07 February 2019.
[22] Index, 'Engem is ugyanúgy mérgeztek meg mint Szkripalt', 21 February 2019.
[23] John Emsley, 'Q&A: Polonium 210', Royal Society of Chemistry, 27 November 2006.
[24] Pascal Froidevaux et al., 'Po210 poisoning as possible cause of death: forensic investigations and toxicological analysis of the remains of Yasser Arafat', Forensic Science International 259 (2015), 1–9.

(CHUV) of the Lausanne University Hospital in Switzerland said that it could neither be confirmed nor excluded that Arafat had been poisoned by polonium.

The other such assassination took place in London in November 2006, the victim was former Soviet secret agent Alexander Litvinenko, whose tea was laced with polonium. When Litvinenko fell ill, he was immediately suspected of having been poisoned. The identification of the polonium was a coincidence, but by then it was too late and the victim's life could not be saved. Unlike in the Arafat case, the coroner's report clearly showed the presence of Po210.

There were some clinical differences between the Litvinenko and Arafat cases: unlike Litvinenko, Arafat did not show symptoms of osteoporosis and hair loss. However, these differences can be explained by the difference in age and the difference in the amount of radioactive material ingested. Small doses given regularly may produce completely different symptoms from a single high dose.[25]

Also common to the above cases are that they all occurred in public space.

3. CBRN terrorism threats

The intelligence methods mentioned above are not part of the intelligence functions of democratic states. The potential terrorist attacks[26] with this type of material, which only deepen the dimension of the threat posed by weapons of mass destruction, are even more so. Hungary's National Security Strategy formulates the fight against terrorism as follows: 'Hungary pays special attention to the fight against terrorism in all its forms: the most decisive action against this phenomenon is in our national interest. The fight against terrorism is based on both preventing terrorist acts, detecting and dismantling terrorist groups and organisations, dealing with the consequences of terrorist acts, strengthening defence capabilities and preparing for emergencies.'[27]

CBRN weapons are the deadliest weapons in existence today, taking their victims indiscriminately. In addition to physical injury, this type of weapon is capable of causing the greatest panic, and the effects of a single use can cause economic and social disruption. For this reason, it is very attractive to various terrorist organisations and they are keen to acquire it.[28] Scientific progress and market forces are driving the cost of DNA synthesis down faster than Moore's Law: more and more people in the world have access to biotechnological scientific advances that were previously only available to scientists. Depending on the type of WMD used, we can talk about nuclear, chemical and bioterrorism. Fortunately, the use of CBRN weapons by non-state actors is relatively rare, a fraction of terrorist attacks happen using CBRN weapons, according to the University of Maryland Global Terrorism Database (which contains over 190,000 cases).

[25] Fei Su and Ian Anthony (eds), Reassessing CBRN Threats in a Changing Global Environment (SIPRI, June 2019).

[26] In 2018, a coordinated operation by counter-terrorism organisations in Germany led to the arrest of a Tunisian extremist man in his apartment in Cologne who was planning to carry out a terrorist attack using ricin (Florian Flade, 'The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror', Combating Terrorism Center 11, no 7 [2018]).

[27] 'Hungary's National Security Strategy', 23 April 2020.

[28] United Nations, 'Government, 'Islamic State' Known to Have Used Gas in Syria, Organisation for Prohibition of Chemical Weapons Head Tells Security Council', 07 November 2017.

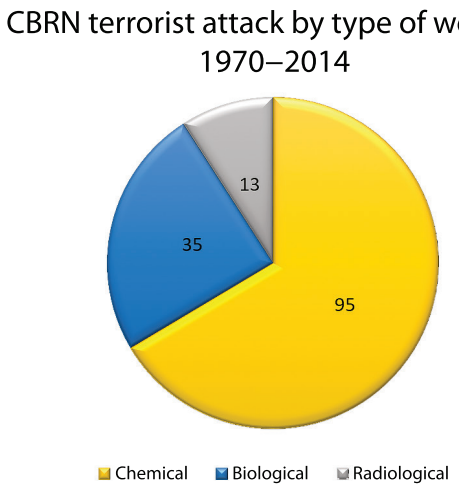


Figure 2
Volume of ABV terrorist attacks in the world, 1970–2014
Source: Lloyd's, 2016.

The likelihood of using CBRN materials is determined by the likelihood of terrorist organisations and sabotage groups being able to acquire these materials and the financial costs of acquiring and weaponising them. The CBRN threat posed by terrorist and sabotage groups is linked to a few factors: capabilities, intentions and limited access to materials.

Fortunately, our country is one of the lowest risk areas in the world in this respect.[29] Nevertheless, the risk of this hazard is not zero, and although the probability of such an extreme event occurring is extremely low, the consequences would have a huge impact on the functioning of the state.

4. Summary

Chemical weapon attacks have been a recent cause for concern in Asia and Europe. Dealing with the aftermath of these types of CBRN incidents is currently not part of states' security protocols. This type of use does not only pose a threat to direct targets: the use of toxic agents in public areas is likely to result in collateral damage, and the consequences require inter-ministerial cooperation and involve multiple disciplines.

The fact that other countries can use weapons of mass destruction in peacetime, without any precedent, to achieve their political goals is a new and frightening prospect. In this area too, the methodology of hybrid warfare seems to be emerging:

[29] Global Terrorism Database, s. a.

the boundary between a state of war and a state of peace is blurring. The CBRN protection task force must be prepared for this eventuality: during the visits of some political actors, not only the bomb-sniffing dog but also the CBRN specialist with special detection equipment may be needed.

The situation can only be addressed in a comprehensive approach. Cooperation at both regional and international level needs to be made more effective, as addressing the challenges of CBRN protection requires international cooperation, as CBRN threats do not stop at national borders.

References

Barry, Ellen and Ceylan Yeginsu, 'The Nerve Agent Too Deadly to Use, Until Someone Did'. The New York Times, 13 March 2018. Online: www.nytimes.com/2018/03/13/world/europe/uk-russia-spy-poisoning.html

BBC News, 'Alexei Navalny: 'Poisoned' Russian opposition leader in a coma', 20 August 2020. Online: www.bbc.com/news/world-europe-53844958

Bellingcat, 'Third Skripal Suspect Linked to 2015 Bulgaria Poisoning', 07 February 2019. Online: www.bellingcat.com/news/uk-and-europe/2019/02/07/third-skripal-suspect-linked-to-2015-bulgaria-poisoning/

Bellingcat, 'FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning', 14 December 2020. Online: www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/

Compound Interest, 'What are Novichok agents? What we do (and don't) know about them', 12 March 2018. Online: www.compoundchem.com/2018/03/12/novichok/

Davis, Jordan, 'Salisbury Novichok clean-up mission 'couldn't fail'.' BBC News, 12 December 2019. Online: www.bbc.com/news/uk-wales-50748163

Emsley, John, 'Q&A: Polonium 210'. Royal Society of Chemistry, 27 November 2006. Online: www.chemistryworld.com/news/qanda-polonium-210/3003354.article

European Council, 'Use of chemical weapons in the assassination attempt of Alexei Navalny: EU sanctions six individuals and one entity', 15 October 2020. Online: www.consilium.europa.eu/hu/press/press-releases/2020/10/15/use-of-chemical-weapons-in-the-assassination-attempt-on-alexei-navalny-eu-sanctions-six-individuals-and-one-entity/

Flade, Florian, 'The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror'. Combating Terrorism Center 11, no 7 (2018). Online: https://ctc.usma.edu/june-2018-cologne-ricin-plot-new-threshold-jihadi-bio-terror/

Froidevaux, Pascal et al., 'Po210 poisoning as possible cause of death: forensic investigations and toxicological analysis of the remains of Yasser Arafat'. Forensic Science International 259 (2015), 1–9. Online: https://doi.org/10.1016/j.forsciint.2015.09.019

Global Terrorism Database, s. a. Online: www.start.umd.edu/gtd/search/Results.aspx?search=&sa.x=54&sa.y=3

Hidalgo, Louise, 'World: Asia-Pacific US dismantles chemical weapons'. BBC News, 09 August 1999. Online: http://news.bbc.co.uk/2/hi/asia-pacific/415742.stm

Holmes, Oliver and Tom Phillips, 'Kim Jong-nam killed by VX nerve agent, say Malaysian police'. The Guardian, 24 February 2017. Online: www.theguardian.com/world/2017/feb/24/kim-jong-nam-north-korea-killed-chemical-weapon-nerve-agent-mass-destruction-malaysian-police

'Hungary's National Security Strategy', 23 April 2020. Online: http://njt.hu/cgi_bin/njt_doc.cgi?docid=219153.382110

Index, 'Engem is ugyanúgy mérgeztek meg, mint Szkripalt', 21 February 2019. Online: https://index.hu/kulfold/2019/02/21/emilian_gebrev_bolgar_fegyver_szkripal_mergezes_gru_orosz/

Lloyd's, 'Use of Chemical, Biological, Radiological and Nuclear Weapons by Non-State Actors', 01 February 2016. Online: www.insurancehound.co.uk/lloyds-london-market/new-market-entry-advice/use-chemical-biological-radiological-and-nuclear-weapons-non-state-actors-emerging-trends-and-risk-factors-27002

'Mandates of the Special Rapporteur on extrajudicial, summary or arbitrary executions; and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', 30 December 2020. Online: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25830

Organisation for the Prohibition of Chemical Weapons, The Hague, 03 March 2021. Online: www.opcw.org/sites/default/files/documents/2021/03/Letter%20PR%20Russia%203-3-2021.pdf

Pálos, Máté, 'Hogyan buktatta le pár újságíró a titkos orosz Navalnij-műveletet?' Magyar Narancs, 17 December 2020. Online: https://magyarnarancs.hu/kulpol/hogyan-buktatta-le-par-ujsagiro-a-titkos-orosz-navalnij-muveletet-234444

Pérez-Peña, Richard, 'What Is Novichok, the Russian Nerve Agent Tied to Navalny Poisoning?' The New York Times, 02 September 2020. Online: www.nytimes.com/2020/09/02/world/europe/novichok-skripal.html

Schofield, Simon, 'Toxic Relationships: A History of CBRN Assassinations', 25 March 2018. Online: https://encyclopediageopolitica.com/2018/03/25/toxic-relationships-a-history-of-cbrn-assassinations/

Stansall, Ben, 'Salisbury Russian agent linked to novichok attack in Bulgaria'. The Times, 08 February 2019. Online: www.thetimes.co.uk/article/salisbury-russian-agent-linked-to-novichok-attack-in-bulgaria-006wpp22x

Su, Fei and Ian Anthony (eds), Reassessing CBRN Threats in a Changing Global Environment. SIPRI, June 2019. Online: www.sipri.org/publications/2019/other-publications/reassessing-cbrn-threats-changing-global-environment

Szabad Európa, 'Célkeresztben a Navalnij-mérgezésről szivárogtató orosz biztonsági tisztek', 07 March 2021. Online: www.szabadeuropa.hu/a/oroszorszag-celkeresztben-a-navalnij-mergezesrol-szivarogtato-biztonsagi-tisztek/31134991.html

The Global Risks Report 2019. 14th Edition. Online: www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf 46-49

The State Duma News, 22 December 2020. Online: http://duma.gov.ru/news/50380/

Timeline of Syrian Chemical Weapons Activity, 2012–2019. Online: www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity

Toler, Aric, 'Hunting the Hunters: How We Identified Navalny's FSB Stalkers'. Bellingcat, 14 December 2020. Online: www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology/

UK Delegation to the OPCW, 'Update on the Use of Nerve Agent in Salisbury, United Kingdom', 13–16 March 2018. Online: www.opcw.org/sites/default/files/documents/EC/87/en/UK_Statement_EC-87.pdf

United Nations, 'Government, 'Islamic State' Known to Have Used Gas in Syria, Organisation for Prohibition of Chemical Weapons Head Tells Security Council', 07 November 2017. Online: www.un.org/press/en/2017/sc13060.doc.htm

HADMÉRNÖK
VÉDELEMINFORMATIKA
16. évfolyam (2021) 4. szám 67–83.
DOI: 10.32567/hm.2021.4.6

Baglyos Sándor[1]

A toborzás egy innovatív formája

An Innovative Way to Recruit

A digitalizációnak köszönhetően átalakult a hadviselés, aminek következtében olyan katonák sokaságára van szükség, akik megfelelő ismeretekkel rendelkeznek a digitális eszközök használatát, valamint a kiberhigiéniai képességeket illetően. A kibertérben lezajló paradigmaváltások miatt a fiatalok figyelmét is egyre nehezebb a régi, elavult katonai toborzóeszközökkel megragadni, így a siker érdekében új típusú megközelítésre van szükség.

A cikk betekintést nyújt az idegen haderőkbe és azok toborzási szokásaiba, abba, hogyan alakult ki dollármilliárdokat érő kapcsolat a katonaság és a film-, később videójátékipar között, továbbá felhívja a figyelmet a videójátékokban rejlő hatalmas potenciálra.

Kulcsszavak: **digitalizáció, haderő, videójátékok, toborzás**

Digitalisation has transformed warfare, requiring a large number of soldiers with the right skills in the use of digital tools and cyber-humanitarian capabilities. Paradigm shifts in cyberspace are also making it increasingly difficult to capture the attention of young people with old, outdated military recruitment tools, so a new type of approach is needed to succeed.

The article gives an insight into the foreign military and their recruitment habits, how billions of dollars' worth of links between the military and the film and later video game industries were forged, and the huge potential of video games.

Keywords: **digitalisation, armed forces, video games, recruitment**

[1] Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Közigazgatás-szervező alapképzési szak, hallgató, e-mail: sandor19990213@gmail.com

1. Bevezetés

A videójátékokról hallva sok embernek értelmetlen időtöltés juthat eszébe, és hogy ezek többsége tizenévesek vagy gyermekek szórakoztatására készült. Tanulmányomban megpróbálom ezt cáfolni, és feltárni az egyre növekvő politikai, kulturális és katonai vonatkozásokat a videójátékokkal kapcsolatban.

Kutatásom feltárja, hogyan is jutottunk el a katonaság egyik legjobban bevált toborzói módszerétől, a háborús filmektől a videójátékokig, úgy, hogy közben a Pentagon és Hollywood közötti szoros történelmi kapcsolatokat is megvizsgáljuk. Ma ez az együttműködés, amelyet Phil Strub, a Pentagont és Hollywoodot összekötő iroda vezetője „kölcsönös kizsákmányolás kapcsolatának"[2] nevez, egyre inkább magában foglalja a háborús filmek és az FPS[3]-játékok viszonyát Amerikával.

A cikkben megvizsgálom azokat a történelmi eseményeket, amelyek szerepet játszottak a fent említett „szövetségben". Miként is lett a katonai ipari komplexumból a szakértők szerinti *the military-industrial-media entertainment network* (MIME-Net), vagyis a katonai-ipari-média szórakoztató hálózat. Továbbá az informatikai fejlődésnek köszönhetően milyen új platformok jöttek létre, amelyek segítettek a katonaságnak különböző céljaik kivitelezésében. A katonai toborzás nemcsak a toborzási misszió nagysága miatt, hanem a toborzás jelenlegi környezete miatt is kihívást jelent a toborzótiszteknek, hiszen nehéz egy új generációt, a korábban használt néhol talán már elavult eszközökkel megfogni/„katonáskodásra" ösztönözni. Mindazonáltal a katonai szolgálat sok fiatal számára vonzóbbá vált az évek során, hiszen a világ hadseregei célzottan, a háborús filmek mellett, már a videójátékokkal is próbálják megszólítani ezt a célcsoportot.[4] Az emberek nagy részét már gyermekkora óta érdekli a hadászat világa, és a számítógépes játékok segítségével hamar elsajátítják azokat a taktikai készségeket, amelyek hatalmas előnyben részesítik majd őket leendő katonai karrierjükben.[5]

1.1. Tudományos probléma

A digitalizációnak köszönhetően átalakul a hadviselés. Olyan katonák sokaságára van szükség, akik tudják tartani a lépést a technikai fejlődéssel és kiberbiztonsági szempontból is meg tudják védeni a hazájukat. A fiatalokat is egyre nehezebb lesz a régi, elavult módszerekkel megszólítani. Meg kell találni azokat a csatornákat a filmek és videójátékok mellett, amelyek hatással lehetnek rájuk.

[2] Sebastian Kaempf: 'A Relationship of Mutual Exploitation': The Evolving Ties between the Pentagon, Hollywood, and the Commercial Gaming Sector. *Social Identities,* 25. (2019), 4. 542–558.

[3] FPS – *first person shooter.*

[4] Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata,* 13. (2016), 1. 61–81.

[5] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36.

1.2. Kutatási célkitűzések

Cikkemben többek között a Pentagon és Hollywood közötti szoros történelmi kapcsolatokat vizsgálom az 1920-as évektől napjainkig, feltárva, hogyan jutottunk el a filmektől a valóságshow-kon keresztül a számítógépes szimulációk és videójátékok világáig. Az amerikai hadseregre mint mélyreható esettanulmányra támaszkodva megtudhatjuk, hogy a háborúk körzete jóval túlmutat a tényleges harctereken. Kutatásom célja a videójátékokban rejlő potenciál ismertetése, amelyet a Magyar Honvédség toborzási missziója és a kiképzései során alkalmazni tudna.

1.3. Hipotézisek

Kutatásom során az alábbi hipotéziseket fogalmaztam meg:

H1. Akik videójátékokat játszanak, nagyobb eséllyel döntenek úgy, hogy katonának állnak.

H2. A katonaságra vonatkozó percepcióra pozitív hatást gyakorolnak a filmek és sorozatok.

H3. Akik videójátékokat játszanak, szívesebben állnának be a seregbe, ha az ottani feladatuk az lenne, hogy e-sportolóként tevékenykednek.

H4. Az e-sport kifejezés említésének az interneten többségében pozitív jelentéstartalma van.

2. Kutatási módszertan

Kutatásomban empirikus vizsgálattal elemeztem a videójátékok hatását a katonai toborzásra, és megismertem a játékprogramokban rejlő hatalmas potenciált a katonai szakma népszerűsítésére. Kutatásom első fázisában kérdőíves felmérést végeztem a videójátékok, e-sport, illetve filmművészet témakörében. A kérdőívek kiértékelését kereszttábla-elemzéssel végeztem el. Cikkemben ezen kívül szentimentanalízis segítségével vizsgáltam az e-sportokkal kapcsolatos internetes attitűdöt. Kutatásom alapját nagyrészt a külföldi cikkek, tanulmányok és azok általam készült fordításai képezik, valamint néhány magyar forrás is.

3. A haderők kapcsolata a filmiparral

Kiindulópontunk Hollywood, valamint annak a filmipar és a katonaság közötti szimbiotikus kapcsolata. A Pentagon hamar felismerte a celluloid történetmesélés erejét, és arra ösztönözte Hollywoodot, hogy hősi portrékat teremtsen az eddigi amerikai háborúkról.[6]

[6] Georg Löfflmann: Hollywood, the Pentagon, and the cinematic production of national security. *Critical Studies on Security,* 1. (2013), 3. 280–294.

3.1. A filmipari együttműködés története

A Pentagon és Hollywood közötti történelmi együttműködés a 20. század elején kezdődött. 1942-ben a Pentagon megnyitotta első saját irodáját Los Angeles szívében, a „Motion Picture Liason Office"-t. Az Egyesült Államok II. világháborúba való belépésével a kezdeti cél az volt, hogy propagandafilmeket[7] állítsanak elő. Olyan neves színészek és filmrendezők, mint James Stewart, Clark Gable, Henry Fonda és John Ford a katonaság szolgálatába állították tehetségüket. A legerősebb láncszem pedig Frank Capra rendező volt, aki hét propagandafilm-sorozatot készített *Why We Fight* címmel.

Annak ellenére, hogy sok idő telt el azóta, a Pentagon és Hollywood között az együttműködés folytatódott, igaz a propagandának sokkal finomabb formájában. Az elmúlt évtizedekben a legtöbb amerikai háborús film a showbiznisz és a hadsereg szoros együttműködésében készült. A hosszú listán olyan híres filmek szerepelnek, mint a *Top Gun,* a *Pearl Harbor,* a *Black Hawk Down,* a *Wind Talker,* a *We were Soldiers,* a *Transformers* és az *Iron Man.* Ebből a szimbiotikus kapcsolatból mindkét fél profitál. A Pentagon számára a filmek hatékony eszközök voltak a hősi mítoszok létrehozására és a történelmi események átírására, kiszínezésére. Toborzási eszközként is szolgáltak, hiszen folyamatos áramlást eredményeztek a lelkes fiatalok köréből.[8]

Az első mérföldkő a *Wings* gyártása volt az 1920-as években. A *Wings* egy 1927-es némafilm volt, amely az akciódús háborús filmek klasszikusa. A film az I. világháború idején játszódott, és tele volt amerikai katonák nagyszabású csatáival a német erők ellen. A film sikere a Pentagonnak a későbbi együttműködését eredményezte Hollywooddal.[9]

Másik kulcsfontosságú mérföldkő az 1986-os *Top Gun* volt. A *Top Gun* sikere után a katonaságnál jelentősen megnövekedtek a toborzási számok, ami nagyban segítette a vietnámi háború okozta trauma leküzdését.[10] A forgatott filmtől függően a Pentagon harckocsikat, teherautókat, repülőgép-hordozókat, vadászgépeket vagy akár tényleges amerikai katonákat is kölcsönbe adott. Nehéz mérni, hogy a filmgyártók mennyit spóroltak. A filmtől és a helyszíntől függően ez a katonai hozzájárulás többségében ingyenes volt, bár amikor a gyártóknak fizetniük kellett, például egy repülőgépes kaszkadőrért, ez körülbelül 16 000 dollárba kerülhetett óránként. Ezt természetesen szigorú szerződés kapcsolta össze, amelyet „Production Assistance Agreement"-nek hívtak.[11]

Egy dolog számít: a katonaság imázsát nem szabad rontani. Más szóval, nem feltétlenül szükséges a 100%-os egyetértés, némi engedékenység az egész cselekményben értékesebbnek tekinthető, mint a produkció együttes befolyásolásának elvesztése.

---

[7] Eszméknek, nézeteknek, politikai elméleteknek szóban vagy írásban (vagy egyéb módon) való tervszerű hirdetése, terjesztése, népszerűsítése.

[8] Bányász Péter: A közösségi média szerepe a katasztrófaelhárításban a Sandy-hurrikán példáján keresztül. In Horváth Attila (szerk.): *Fejezetek a kritikus infrastruktúra védelemből: kiemelten a közlekedési alrendszer.* Budapest, Magyar Hadtudományi Társaság, 2013. 281–292.

[9] Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77.

[10] Tibor Farkas – András Tóth: Electronic warfare in full spectrum operation. In Proceedings of the International Scientific Conference: New Trends in Signal Processing, 2012. 181–188.

[11] Tamás Szádeczky: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *Academic and Applied Research in Public Management Science,* 19. (2020), 1. 83–93.

A Pentagon részvételének megőrzése azt eredményezi, hogy az továbbra is befolyást tud gyakorolni, potenciálisan javítva a toborzási számokon. A filmesek számára pedig az, hogy a katonaság gyakran fedélzeten van, hozzájárul ahhoz az izgalomhoz és realizmushoz, amelynek megtalálása egyébként nehézkes lenne.

3.2. A katonai életről szóló valóságshow-k/sorozatok

Ez a fajta együttműködés később a filmkészítésen is túlszárnyalt. Most már a valóságshow-k is a repertoárba tartoznak. Jerry Bruckheimer és Bertram van Munster ötlete az volt, hogy indítsanak egy valóságshow-t, amelyben amerikai katonákat mutatnak be Afganisztánban járőrözve.[12] Az ötlet a szeptember 11-ei események után valósult meg, amikor éppen az al-Káida elleni műveletek zajlottak. Alapvetően követték az afganisztáni háború eseményeit. A valóságshow neve a *Profiles from the Frontline* volt. A háború steril változatát mutatta be, senki nem halt meg egyik oldalon sem a felvételeken, mert amint a harc közeledett az operatőrök felé, a kamerákat kikapcsolták. Inkább reklámfilmnek tűnik, mintsem dokumentumfilmnek. Ez volt a Pentagon első együttműködése a valóságshow-k gyártásában.[13] Azóta ez a televíziós műfaj exponenciális növekedési ütemet mutat az amerikai médiapiacon. Míg a 2000-es évek elején csak maréknyi ilyen műsor volt, 2015-re ezeknek a műsoroknak a száma meghaladta a 300 amerikai tévéműsort. Legkiemelkedőbbek az *NCIS, NCIS Los Angeles* és *Hawaii Five-0*. Az akkori legnagyobb együttműködés azonban az *Inside Combat Rescue* (magyar cím: *Bevetések hősei*) volt, amelyet a *National Geographic* együttműködésével készítettek. A *National Geographic* kameracsapatai közvetlenül beépültek az Egyesült Államok mentőegységeibe. Minden egyes forgatási nap végén valaki átnézte az összes felvételt, és a nem tetsző részeket meg kellett semmisíteni. Csak azokat a felvételeket használhatták fel később, amelyeket engedélyeztek. Ez végül sikeres módszerré fejlődött ki mind a filmesek, mind a DOD[14] számára. A műsor egy afganisztáni bevetést mutat be, a „Pararescuemen" elit légierő harci mentőegységének feladatait, amely az amerikai erők és a szövetségesek kimenekítését végzi. A *National Geographic* rengeteg pozitív visszajelzést kapott az *Inside Combat Rescue*-nak köszönhetően, ami rengeteg új együttműködési kérelmet eredményezett.[15]

4. A haderők kapcsolata a játékiparral

A történelem során a játékokat egész életen át tartó alapvető és normális tevékenységnek tekintették. A játékok révén a gyerekek megtanulják felfedezni, elsajátítani a különböző kognitív képességeket, és kötődést alakítanak ki rajtuk keresztül

[12] Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Csengeri János – Krajnc Zoltán (szerk.): *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése.* Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673.
[13] Kelefa Sanneh: The Reality Principle. The Rise and Rise of Reality Genre. *The New Yorker,* 2011. május 9.
[14] DOD – *Department of Defense,* Amerikai Védelmi Minisztérium.
[15] Go 'Inside Combat Rescue'. *Military.com,* 2013. február 15.

a szülőkkel és társaikkal egyaránt. A játékok olyan feltételeket teremthetnek meg, amelyek lehetővé teszik az emberek számára, hogy fejlesszék a különböző készségeiket, vagy akár olyan szerepet ölthetnek magukra, amelyet a való életben is el szeretnének érni. Sőt, az a fajta játék, amelyet az emberek választanak, befolyásolhatja a személyiségük fejlődését is.[16] A memóriajátékok fejleszthetik a kognitív képességeket, a társasjátékok pedig az együttműködési és kommunikációs készségekre vannak pozitív hatással. Az emberek azt játsszák, amit szeretnek, és idővel egyre jobbá válnak abban, ami tetszik nekik.

4.1. A videójátékok evolúciója

Mik is a videójátékok? Sok millió ember játszik rendszeresen videójátékokkal. A videójáték kifejezés nagyjából a digitális szórakozás interaktív formájára utal. A tipikus irányításért felelős eszközök a billentyűzet és a kontroller. Ezekkel lehet manipulálni az eseményeket egy kijelzőn, amely lehet monitor, tévé vagy akár okostelefon. (Viszont ezeket lehet extrémebb szintre is emelni, például 2020 szeptemberében egy klasszikus játékot, a *Doom*ot sikerült egy digitális terhességi teszt kijelzőjére varázsolni.) Általánosságban elmondható, hogy a játékos nyerhet, továbbjuthat vagy veszíthet.[17] Ez a technikai meghatározás azonban nem ragadja meg a játék pszichológiai tapasztalatait, különösen a modern játékok esetében. Számos modern játék korlátlan élményt nyújt (főleg a multiplayer játékok, amelyeknek fő mozgatórugója nem egy történet elmesélése, hanem a más játékosok elleni végtelen versengés), emellett komplex narratívákat, karaktereket, nagy nyitott világokat tár a szemünk elé, lehetőségeket adva arra, hogy megismerkedjünk új emberekkel (Coop, vagy multiplayer játékmódoknál). A játékok lehetővé teszik a játékosok számára, hogy megtapasztaljanak különböző lelkiállapotokat, különböző érzelmeket éljenek át, vagy csak szimplán eltöltsék az időt és „elmeneküljenek" kicsit a valóságból. A játékok alternatív helyet kínálhatnak a társasági élethez a hétköznapi élet mellett. A játékok és a játékélmények nagyon változatosak.[18] Meg lehet őket különböztetni műfajuk szerint (lövöldözős, szerepjáték, stratégiai játék), platform szerint (számítógépek, konzolok, okostelefonok), módok szerint (egy játékos, több játékos), online kapcsolattartás szerint (online vagy offline) és a játék célkitűzése alapján is (ellenfél legyőzése az erőszak, a meggyőzés, a lopakodás taktikájával vagy teljesen más stratégiával).

[16] Tóth András: A NATO kommunikációs rendszerének elméleti és gyakorlati vizsgálata. In Fekete Károly (szerk.): *Kommunikáció* 2014. Budapest, Nemzeti Közszolgálati Egyetem, 2014. 65–76.

[17] Zsolt Bederna – Tamás Szádeczky: Cyber espionage through botnets. *Security Journal.* 33. (2020), 43–62.

[18] Tóth András: Internet of Things Traps in National and International Cyber-Security Solutions. In Peter Spilý (szerk.): *Zborník príspevkov z medzinárodnej vedeckej konferencie: Národná a medzinárodná bezpečnosť 2020.* Liptovsky Mikulas, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2020. 468–475.

4.2. A katonaság új stratégiája

Az elmúlt években a Pentagon érdekeltsége túlnyúlt a filmek, a sorozatok és a valóságshow-k műfaján.[19] Tekintettel a játékkonzolok, az FPS-játékok és sportszimulátorok kereskedelmi sikerére, a hadsereg úgy gondolta, hogy hiba lenne nem kihasználni a médiaszektor adta lehetőségeket.[20] Ezért 1999-ben megalapították a Los Angeles-i „Institute for Creative Technologies" (ICT) nevű intézményt, vagyis a Kreatív Technológiai Intézetet. A fő cél az volt, hogy a Pentagon finanszírozásából összefogják azokat a hollywoodi tehetségeket, neves játékkészítőket és magát a játékipart, hogy a katonaság segítségére legyenek.[21] A cél az, hogy minél valósághűbb (immerzív) élményt tudjanak kreálni az amerikai hadseregnek, hogy a katonák kiképzésén, a taktikai döntéshozatalán, a kulturális tudatosságán áttörő fejlődést érjenek el, továbbá, hogy a PTSD-ben (poszttraumás stressz) szenvedő betegeket a legmodernebb technológiával tudják meggyógyítani.

5. A videójátékok térhódítása

A videójátékok piaca már több mint egy évtizede felülmúlja a mozis sikereket. Jó példa erre az egyik leghíresebb FPS-játék, a *Call of Duty: Modern Warfare 2*. A játék 2009-es kiadásának eladási adatai meghaladták ugyanezen év két legmagasabb kasszasikeres filmjeinek, a *Harry Potter és a Félvér Herceg,* továbbá a *Sötét Lovag* bevételeit. 2011-ben a *Call of Duty: Modern Warfare III* ötnapos világszintű eladási rekordot állított fel (775 millió dollár); összehasonlítva az év legkelendőbb filmjével, a *Harry Potter és a Halál Ereklyéi*vel (202 millió dollár).[22] Ez a virágzó piac segít megmagyarázni, hogy az összes nagy szórakoztató óriás, mint a Sony, a SEGA, az EA és a „Ubisoft" miért része az ICT-nek.[23]

5.1. Toborzás a videójátékokban

A szimulációkat és az FPS-játékokat nemcsak katonai kiképzésre vagy magánszemélyek számára tervezték, hanem egyre inkább toborzási célokra is. 2002-ben például a Pentagon kiadta az *America's Army*[24] játékát, egy ingyenes, korszerű

[19] Tóth András: International information security in hungary. In Ivan Majchút et al. (szerk.): *National and International Security 2017*. Liptovsky Mikulas, Szlovákia, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. 548–557.

[20] Pierre Corbeil: Payne, M.T.: Playing War: Military Video Games after 9/11. *The Computer Games Journal,* 8. (2019), 2. 63–64.

[21] Szádeczky Tamás: E-kormányzati szolgáltatások kommunikációbiztonsága. *Hadmérnök,* 12. (2017), 2. 280–289.

[22] Farkas, Tibor – Hronyecz, Erika: The Infocommunication System Requirements and Analysis of the Communication of the Deployable Rapid Diagnostic Laboratory Support „Sampling Group" II. *Academic and Applied Research in Public Management Science,* 14. (2015), 1. 53–61.

[23] Matt Liebl: Lifetime Call of Duty Sales Exceed Earnings for Harry Potter and Star Wars Film Franchises. *GameZone,* 2012. november 16.

[24] America's Army: www.americasarmy.com/

videojátékot, amelyet kizárólag a fiatal férfiak és nők katonai szolgálatra vonzása céljából fejlesztettek ki. A 2005-ben felvett hallgatók mintegy 40%-a korábban játszott a játékkal, és a 16 és 24 év közötti amerikaiak 30%-a azt mondta, hogy a tudásuk egy része a hadseregről a játékból származik.[25] Eredeti verziójában a játék két részből állt, az egyik a „Soldier" nevű Boot Camp edzésszimulációból, és egy másik, hagyományosabb „Operations" nevű FPS-játékból, amelyben a játékosok online csapatokba szerveződve küzdenek meg egymással, és oldanak meg különböző feladatokat. Az *America's Army* a 21. századi katonai fogyasztói kultúra monumentális lépését jelentette. Óriási siker volt mind a játékosok, mind a toborzás szempontjából. A játék a legmagasabb interaktív és dizájnminősítést kapta (többek között a *PC Games Magazine*-tól „Triple A Quality" minősítést kapott). 7,5 millió dollárba került a programot létrehozni, és a hadsereg reklámarzenáljának állandó eszköze lett. PC-n a www.americasarmy.com weboldalon keresztül érhető el, de később kiadták Xbox és Playstation konzolokra is. 2005-re több mint 6 millió regisztrált felhasználóval rendelkezett, és maga a hadsereg toborzási aránya is az egekbe szökött.

Az amerikai hadsereg sikerei után 2008-ban úgy döntött, hogy a nagyvárosok bevásárlóközpontjaiba játékgépeket telepít. Erre az egyik legnevesebb példa a Philadelphiában létrehozott Army Experience Center (AEC). Komplett központ volt tele különleges játékgépekkel, amelyeken ki lehetett próbálni harci helikoptereket, harckocsikat, különböző fegyvereket – természetesen a virtuális valóságban. Ezeket a játékgépeket toborzótisztek felügyelték, és bárkinek bármi kérdése volt a katonasággal kapcsolatban, egyből választ kaphatott rá ezektől a tisztektől.[26]

A videójáték és a médiaalapú toborzás azonban nem csak az állami hadseregekre szűkült le. Sajnos erőszakos nem állami szereplők, terroristák is előszeretettel alkalmazzák ezeket az eszközöket embereik oktatására/toborzására. Ilyen szoftver volt például a „Blackwater" (azóta Academi-re lett keresztelve).[27] A híres GTA V-ben is különböző „modokkal" próbáltak katonákat toborozni a terroristák.[28] Az al-Káida és a Daesh bár nem fejleszt videójátékokat, ezekkel kapcsolatos videókat, mémeket használnak fel felkeléseik, toborzásaik során.

5.2. E-sport

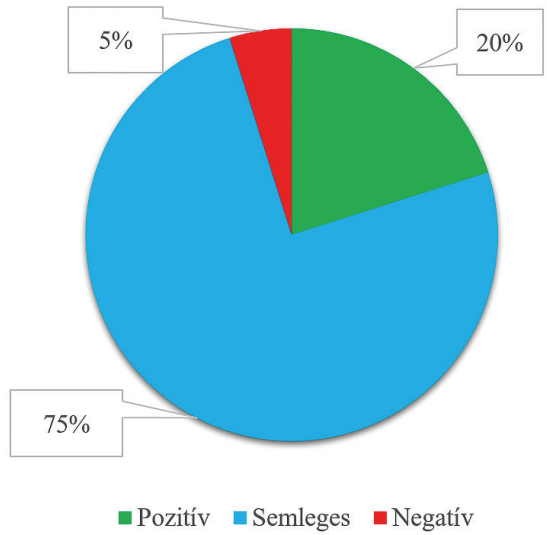
A videójátékok sok országban jelentős kulturális jelenséggé váltak.[29] Ezt megerősíti az e-sport, vagy a profi bajnokságok és versenyek térnyerése, ahol a játékosok

[25] Nick Robinson: Military Videogames. *The RUSI Journal,* 164. (2019), 4. 10–21.
[26] Tamás Szádeczky: Enhanced Functionality Brings New Privacy and Security Issues – An Analysis of eID. *Masaryk University Journal of Law and Technology,* 12. (2018), 1. 3–28.
[27] Farkas Tibor – Sándor Miklós: A honvédség állandó hírhálózatának fejlesztési kérdései. *Kard és Toll,* 1. (2006), 2. 158–164.
[28] Miron Lakomy: Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment. *Studies in Conflict & Terrorism,* 42. (2019), 4. 383–406.
[29] Tóth András: Information-Sharing Challenges and Issues in Multinational Operations, Part 2. *Land Forces Academy Review,* 26. (2021), 1. 22–30.

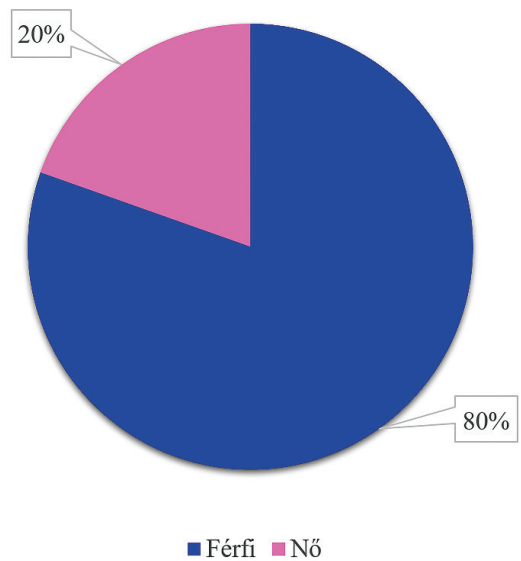
külön-külön vagy csapatokban is versenyezhetnek egymással. Ezek az események különösen népszerűek Dél-Koreában és Kínában. 2017-ben az e-sportok 756 millió dolláros bevételt termeltek a két országnak.[30] A népszerű játékok között a legkiemelkedőbb a *League of Legends* és az *Overwatch* volt, nézőközönségük megtöltött egy egész stadiont, és az online nézők száma meghaladta a 250 millió főt 2017-ben. Az e-sportban hatalmas pénznyeremények vannak a nagy nézőbázisnak köszönhetően. A legnagyobb nyereményalap a „The International 2017" volt a *Dota 2* játéknál, amely 24 millió dollár összdíjazású alap volt a csapatok számára. A győztes csapatok kovácsolt fizikai trófeákat is kaptak, amelyeket a Wētā Workshop (*A Gyűrűk Ura*-filmek mögött álló speciális effektekkel foglalkozó cég) készített bronzból és ezüstből. A *Dota 2* adta eddig a legnagyobb díjazásokat, összesen 133 millió dollárt osztott szét 880 verseny között, azon belül 2335 játékosnak.[31] Bár ezek a bevételek magasnak tűnnek, meg kell jegyezni, hogy a legtöbb játékos átlagfizetése viszonylag alacsony a többi sportághoz képest. Ehhez kapcsolódó fejlemény a játéktevékenységek online közvetítésének növekedése, televíziós műsorszolgáltatáshoz hasonló szórakoztatási formában. Sok millió ember nézi, ahogy mások online platformokon játszanak, mint például a Twitch és a YouTube Gaming. Ezeknek a műsoroknak két fajtája van: az egyik, amikor online történnek az események, és a „streamer" kapcsolatot tud létesíteni a nézőközönséggel, a másik pedig, amikor előre fel van véve az anyag, és az, mint egy tévéműsor, meg van vágva. Az egyik leghíresebb streamer, Felix Kjellberg (nicknevén PewDiePie), teljes karriert épített a videózásra. Óriási fogyasztói igény lett, különösen a fiatalabb közönség körében az ilyen tartalmakra. Karrierje során Felix tartalma főleg a „Let's Play" videókból tevődött ki. A horrorjátékokkal kapcsolatos reakciói alkották meg sikerének kezdeti alapjait, és az, hogy más videósokkal ellentétben először a nézőközönségével próbált meg nagyon szoros kapcsolatot kialakítani.[32]

Negyedik hipotézisem, hogy az e-sport említése globálisan az interneten pozitív jelentéstartalommal történik. Ezt a SentiOne adatelemző szoftver segítségével végeztem el. Az adatok a 2018. január 1-je és 2020. október 21-e közötti időszakot reprezentálják. Ez idő alatt 150 589 alkalommal volt pozitív, míg 36 478 alkalommal negatív jelentéstartalommal említve az e-sport, ami arra enged következtetni, hogy az emberek az e-sportot pozitív dolognak tekintik. Bár döntő többségében, vagyis az összes említés 75%-ában semleges volt az e-sport kifejezésre kapott találatok attitűdje, ennek egyik oka az lehet, hogy kontextus nélkül osztották meg az ezzel kapcsolatos tartalmakat, és ezáltal nem lehetett vizsgálni a kapcsolódó érzelmet.

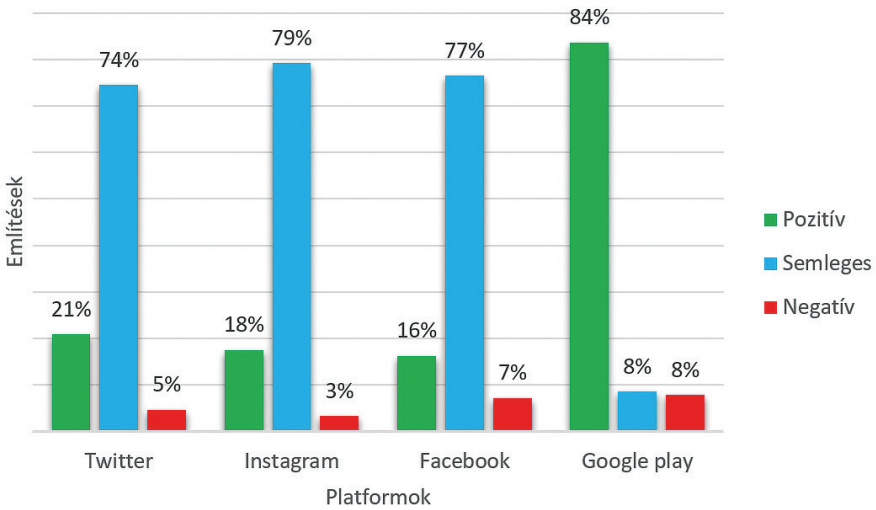
[30] SuperData: 2018 Year in Review (2019. január).
[31] Statistics. Esports Earnings: www.esportsearnings.com
[32] Tóth András: Information-Sharing Challenges and Issues in Multinational Operations, Part 1. *Land Forces Academy Review,* 25. (2020), 4. 307–316.



1. ábra
Az e-sportról alkotott vélemények az interneten
Forrás: a szerző szerkesztése a SentiOne adatai alapján



2. ábra
Az e-sport említése az interneten, nemek közti megoszlásban
Forrás: a szerző szerkesztése a SentiOne adatai alapján



3. ábra

Az e-sport megítélése a különböző internetes platformokon

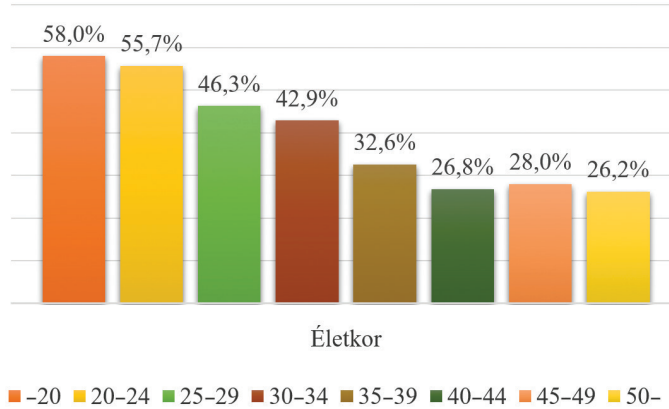
Forrás: a szerző szerkesztése a SentiOne adatai alapján

5.3. Kérdőíves felmérés eredményei

Ebben az alfejezetben két kérdőív elemzésével foglalkozom. Az egyiket én készítettem, amelyet a Facebook-ismerőseim és több videójátékos Facebook-csoport között osztottam meg (az ottani adminok engedélyével). A másik pedig a Karin A. Orvis által készített *Are Soldiers Gamers?* című kutatás.[33]

Azért tartom fontosnak a fent említett, nem általam készített kérdőívet, mert több mint 10 000 amerikai katona töltötte ki. A katonák 43%-a állította azt, hogy legalább hetente játszik valamilyen típusú videójátékkal. Rendfokozat alapján is vizsgálták a válaszokat, amelyben az az eredmény jött ki, hogy a frissen besorozott katonák játszanak a legtöbbet, 51–59% között. Az életkor szerint végzett adatelemzések alapján kiderült, hogy szignifikáns negatív korreláció volt az életkor és a videójátékok használata között ($r = -.23$, $p < .001$). Ez hatalmas előnyt jelent a friss katonáknak, hiszen a kutatás alapján kiderült, hogy akik rendszeresen játszanak videójátékokkal (főleg FPS), azok magasabb eredményeket érnek el az FPP (first person perspective) (virtuális katona szemszögén keresztül látott események) típusú videójáték alapú kiképző szoftvereken ($r = .33$, $p < .01$).

[33] Karin A. Orvis: Are Soldiers Gamers? Videogame Usage among Soldiers and Implications for the Effective Use of Serious Videogames for Military Training. *Military Psychology,* 22. (2010), 2. 143–157.



4. ábra

Videójátékok használata életkor szerinti megoszlásban az amerikai hadseregben vizsgált katonák között

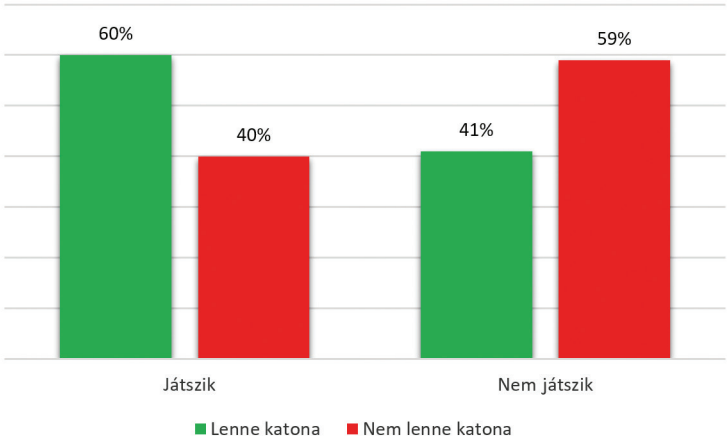
Forrás: a szerző szerkesztése, Karin A. Orvis kérdőívének eredményei alapján

Az általam végzett felmérés adatait az IBM SPSS Statistics Data Editor segítségével elemeztem kereszttábla elemzéssel, amely során a Pearson-féle khi-négyzet értékét vettem figyelembe.

Kérdőívem kitöltői 61,4%-a volt nő, míg 38,6%-a férfi. Életkori különbségeket vizsgálva a kitöltők 55%-a volt 18 és 25 év közötti fiatal, és a kitöltők 48%-a játszik valamilyen videójátékkal.

Első vizsgálatom arra vonatkozott, van-e összefüggés a videójátékok használata és a katonai életpálya választása között (n = 140). A vizsgálat khi-négyzetének megfigyelt értéke 4,837, amelynek kétoldali szignifikanciaszintjének értéke 0,028, tehát megállapíthatjuk, hogy a két változó között az összefüggés szignifikáns, vagyis az, hogy valaki rendszeresen játszik videójátékokon, befolyásolja azt, hogy lenne-e katona vagy sem. Vizsgálatomban a Cramer's V mutató megfigyelt értéke 0,186, kétoldali szignifikanciaszintjének értéke szintén 0,028. A 0,186-os érték viszont alacsony korrelációra utal a két változó esetében. Ez azt magyarázhatja, hogy Magyarországon a katonai toborzást a videójátékok csak minimálisan befolyásolják. Viszont a 18 és 25 év közötti kitöltők 52%-a játszik rendszeresen valamilyen videójátékkal, ezért a megfelelő eszközökkel talán van rá mód, hogy ezen számok növekedjenek.

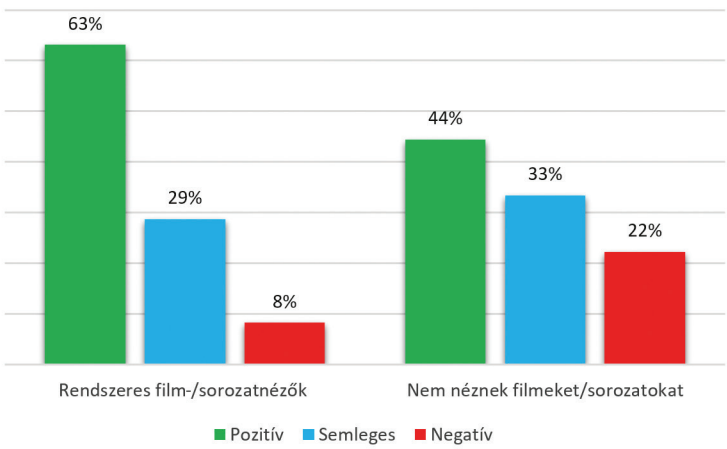
Második vizsgálatom arra vonatkozott, van-e összefüggés a filmek és sorozatok gyakori használata és a katonaság megítélése között (n = 140). A vizsgálat khi-négyzetének megfigyelt értéke 4,102, amelynek kétoldali szignifikanciaszintjének értéke 0,129, tehát megállapíthatjuk, hogy a két változó között az összefüggés nem szignifikáns. Vizsgálatomban a Cramer's V mutató megfigyelt értéke 0,171, kétoldali szignifikanciaszintjének értéke szintén 0,129. A 0,171-es érték alacsony korrelációra utal a két változó esetében.



5. ábra

A videójátékok hatása a toborzásra

Forrás: a szerző szerkesztése



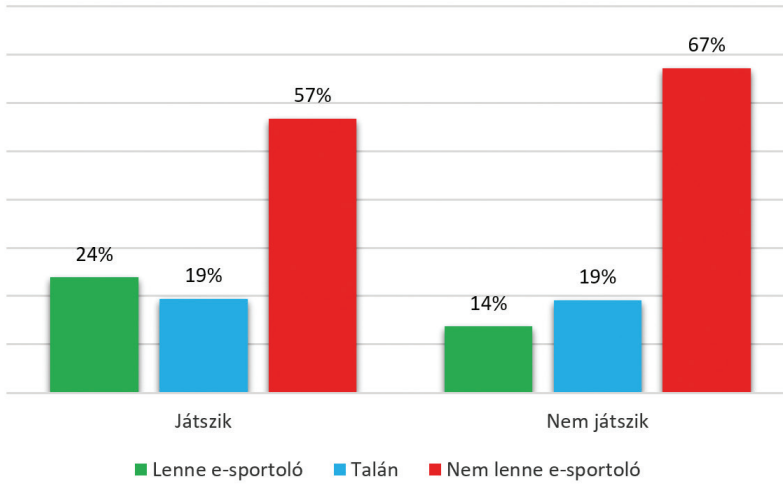
6. ábra

A rendszeres film- és sorozatfogyasztás hatása a katonaságról alkotott véleményre

Forrás: a szerző szerkesztése

Kérdőívemben felvázoltam, hogy az Amerikai Egyesült Államok hadserege úgy próbálja felkelteni a fiatalok érdeklődését a katonáskodásra, hogy saját e-sport-programokat szervez, ahol saját katonáik mint e-sportolók versenyezhetnek civilek ellen. Az „e-sportoló katonák" ugyanazt a fizetést és juttatásokat kapják, mint bárki más a hadseregben. Emellett fizetik az e-sportolók minden engedélyét, a nevezési díjakat és utazásokat, és a teljes gamerfelszerelést egyaránt. Olyan katonákat várnak, akik szolgálatukat e-sportolással töltenék. Illetve olyan civileket, akik emiatt a lehetőség

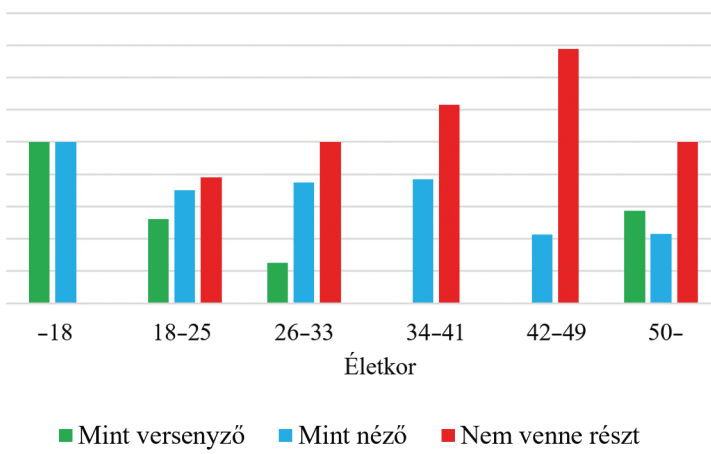
miatt belépnének a hadseregbe. Harmadik vizsgálatom arra vonatkozott, van-e összefüggés a videójátékok használata és a hasonló szakma iránti érdeklődés között (n = 140). A vizsgálat khi-négyzetének megfigyelt értéke 2,560, amelynek kétoldali szignifikanciaszintjének értéke 0,278, tehát megállapíthatjuk, hogy a két változó között az összefüggés nem szignifikáns.



7. ábra

A Magyar Honvédség által finanszírozott csapatban való részvétel kapcsolata a videójátékok használatával

Forrás: a szerző szerkesztése



8. ábra

Bármilyen e-sport-rendezvényen való részvétel és az életkor közötti kapcsolat vizsgálata

Forrás: a szerző szerkesztése

6. Összefoglalás

A katonaságra hatalmas szükség van Magyarországon, hiszen az utóbbi időben olyan új biztonsági fenyegetések jelentek meg a digitalizáció hatására (például a hibrid hadviselés),[34] amelyek modern, kiváló felkészültségű katonákból álló haderőt követelnek meg az országoktól. Benkő Tibor (honvédelmi miniszter) szavaival élve: „Olyan új biztonsági fenyegetések jelentek meg, amelyek befolyásolhatják és meghatározhatják a jövőben a Magyar Honvédség helyét és feladatát."; „A katonai fenyegetettségek – például a hibrid hadviselés – színtere, formája, tartalma és módszere jelentős változáson megy keresztül", s „amely befolyásolhatja, meghatározhatja a jövőben a Magyar Honvédség helyét és feladatát,"; „figyelembe véve a biztonsági környezet változásait, a kormány úgy döntött, hogy egy modern, ütőképes, hazája iránt lojális, kiváló felkészültségű katonákból álló Magyar Honvédségre van szükség, mely biztosítani tudja Magyarország és a magyar állampolgárok biztonságát".[35]

7. Tudományos eredmények

T1. Igazoltam, hogy a videójátékok hatással vannak a katonai toborzásra, igaz magyar viszonylatban még gyenge korrelációt figyelhettünk meg.

T2. Igazoltam, hogy nem mutatható ki összefüggés a film- és sorozatfogyasztók katonaságról alkotott véleménye között.

T3. Nincs összefüggés a Magyar Honvédség által finanszírozott e-sport-csapatba való bekerülési hajlandóság és a videójátékok használata között, amire talán az adhat választ, hogy az e-sport még a mai napig küzd azzal, hogy elfogadtassa magát a magyar sportvilág szemében.

T4. Igazoltam, hogy az e-sport kifejezés internetes említése döntően semleges kontextusban történik.

Felhasznált irodalom

Bányász Péter: A közösségi média szerepe a katasztrófaelhárításban a Sandy-hurrikán példáján keresztül. In Horváth Attila (szerk.): *Fejezetek a kritikus infrastruktúra védelemből: kiemelten a közlekedési alrendszer.* Budapest, Magyar Hadtudományi Társaság, 2013. 281–292. Online: http://real.mtak.hu/94342/

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36. Online: https://doi.org/10.32561/nsz.2015.2.2

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Csengeri János – Krajnc

[34] Tibor Farkas: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289; Tibor Farkas: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15.

[35] Révész Béla: Magyarország biztonsági környezete szabja meg a feladatokat. *Honvedelem.hu,* 2020. február 4.

Zoltán (szerk.): *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése.* Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673. Online: http://real.mtak.hu/94339/

Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata,* 13. (2016), 1. 61–81.

Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77. Online: https://doi.org/10.32561/nsz.2018.1.4

Bederna, Zsolt – Tamás Szádeczky: Cyber Espionage through Botnets. *Security Journal,* 33. (2020), 1. 43–62. Online: https://doi.org/10.1057/s41284-019-00194-6

Corbeil, Pierre: Payne, M.T.: Playing War: Military Video Games after 9/11. The *Computer Games Journal,* 8. (2019), 2. 63–34. Online: https://doi.org/10.1007/s40869-018-0064-9

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289. Online: https://doi.org/10.2478/raft-2020-0034

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15. Online: https://doi.org/10.2478/raft-2021-0002

Farkas, Tibor – András Tóth: Electronic warfare in full spectrum operation. In Proceedings of the International Scientific Conference: *New Trends in Signal Processing.* 2012. 181–188.

Farkas, Tibor – Hronyecz, Erika: The Infocommunication System Requirements and Analysis of the Communication of the Deployable Rapid Diagnostic Laboratory Support „Sampling Group" *II. Academic and Applied Research in Public Management Science,* 14. (2015), 1. 53–61. Online: https://doi.org/10.32565/aarms.2015.1.5

Farkas Tibor – Sándor Miklós: A honvédség állandó hírhálózatának fejlesztési kérdései. *Kard és Toll,* 1. (2006), 2. 158–164. Online: https://m2.mtmt.hu/api/publication/1809565

Go 'Inside Combat Rescue'. *Military.com,* 2013. február 15. Online: www.military.com/undertheradar/2013/02/go-inside-combat-rescue

Kaempf, Sebastian: 'A Relationship of Mutual Exploitation': The Evolving Ties between the Pentagon, Hollywood, and the Commercial Gaming Sector. *Social Identities,* 25. (2019), 4. 542–558. Online: https://doi.org/10.1080/13504630.2018.1514151

Lakomy, Miron: Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment. *Studies in Conflict & Terrorism,* 42. (2019), 4. 383–406. Online: https://doi.org/10.1080/1057610X.2017.1385903

Liebl, Matt: Lifetime Call of Duty Sales Exceed Earnings for Harry Potter and Star Wars Film Franchises. *GameZone,* 2012. november 16. Online: www.gamezone.com/news/lifetime-call-of-duty-sales-exceed-earnings-for-harry-potter-and-star-wars-film-franchises/

Löfflmann, Georg: Hollywood, the Pentagon, and the cinematic production of national security. *Critical Studies on Security,* 1. (2013), 3. 280–294. Online: https://doi.org/10.1080/21624887.2013.820015

Orvis, Karin A.: Are Soldiers Gamers? Videogame Usage among Soldiers and Implications for the Effective Use of Serious Videogames for Military Training. *Military Psychology,* 22. (2010), 2. 143–157. Online: https://doi.org/10.1080/08995600903417225
Révész Béla: Magyarország biztonsági környezete szabja meg a feladatokat. *Honvedelem.hu,* 2020. február 4. Online: https://honvedelem.hu/hirek/hazai-hirek/magyarorszag-biztonsagi-kornyezete-szabja-meg-a-feladatokat.html
Robinson, Nick: Military Videogames. *The RUSI Journal,* 164. (2019), 4. 10–21. Online: https://doi.org/10.1080/03071847.2019.1659607
Sanneh, Kelefa: The Rise and Rise of Reality Television. *The New Yorker,* 2011. május 9. Online: www.newyorker.com/magazine/2011/05/09/the-reality-principle
SuperData: 2018 Year in Review (2019. január). Online: https://adindex.ru/files2/access/2019_01/230617_SuperData%202018%20Year%20in%20Review.pdf
Szádeczky Tamás: E-kormányzati szolgáltatások kommunikációbiztonsága. *Hadmérnök,* 12. (2017),2. 280–289. Online: https://doi.org/10.32567/hm.2017.2.23
Szádeczky Tamás: Enhanced Functionality Brings New Privacy and Security Issues – An Analysis of eID. *Masaryk University Journal of Law and Technology,* 12. (2018), 1. 3–28. Online: https://doi.org/10.5817/MUJLT2018-1-1
Szádeczky, Tamás: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *Academic and Applied Research in Public Management Science,* 19. (2020), 1. 83–93. Online: https://doi.org/10.32565/aarms.2020.1.7
Tóth András: A NATO kommunikációs rendszerének elméleti és gyakorlati vizsgálata. In Fekete Károly (szerk.): *Kommunikáció 2014.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 65–76.
Tóth András: International Information Security in Hungary. In Ivan Majchút – Vladimír Andrassy – Štefan Ganoczy – Michal Hrnčiar – Ondrej Kredatus – Gabriela Kredatusová – Jakub Sasarák – Juraj Šimko – Jaroslav Varecha – Lubomír Belan – Stanislav Morong (szerk.): *National and International Security 2017.* Liptovsky Mikulas, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. 548–557."
Tóth, András: Information-Sharing Challenges and Issues in Multinational Operations, Part 1. *Land Forces Academy Review,* 25. (2020), 4. 307–316. Online: https://doi.org/10.2478/raft-2020-0037
Tóth András: Internet of Things Traps in National and International Cyber-Security Solutions. In Peter Spilý (szerk.): *Zborník príspevkov z medzinárodnej vedeckej konferencie: Národná a medzinárodná bezpečnosť 2020.* Liptovsky Mikulas, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2020. 468–475.
Tóth, András: Information-Sharing Challenges and Issues in Multinational Operations, Part 2. *Land Forces Academy Review,* 26. (2021), 1. 22–30. Online: https://doi.org/10.2478/raft-2021-0004

HADMÉRNÖK
VÉDELEMINFORMATIKA
16. évfolyam (2021) 4. szám 85–99.
DOI: 10.32567/hm.2021.4.7

Bak Gerda,[1] Kiss Sándor[2]

A biztonságtudatosság szisztematikus szakirodalmi áttekintése

Systematic Literature Review of Safety Awareness

Napjainkra a digitális eszközök a mindennapok elengedhetetlen részévé váltak, legyen szó munkáról vagy kikapcsolódásról, az élet minden területén jelen vannak, azonban számos veszélyt is magukban hordoznak. A technológia fejlődésével rengeteg információ cserél gazdát online, kerül fel a felhőbe, tároljuk a digitális eszközökön, amelyek feltételezhetően lehetőséget nyújtanak a magánszféra és az érzékeny adatok illetéktelenek általi megszerzésére, kiszivárogtatására. A potenciális veszélyek kivédésére megoldás lehet a digitális eszközöket használók tudatosítása. A kutatás célja áttekintést adni azokról a tényezőkről, amelyek az egyének biztonságtudatosságát befolyásolják. Ezeknek a tényezőknek a feltárására és összegyűjtésére szisztematikus irodalomelemzést alkalmaztunk a ScienceDirect, a Google Scholar és a Web of Science adatbázisokban 2012. január és 2020. december közötti időszakot vizsgálva. Az elemzés során kizárólag angol nyelvű és teljes terjedelmükben elérhető cikkek keresése történt, amihez megfelelő kulcsszavakat választottunk ki és alkalmaztunk. A keresés lefolytatása után potenciálisan 419 közlemény képezte a részletesebb elemzés tárgyát, amelyekből végül 92 felelt meg az előzetesen megfogalmazott kritériumoknak. Ezek alapján a biztonságtudatossági szintre hatással van többek között az egyén neme, kora, tanulmányai, gondolkodásmódja, továbbá a tapasztalatai és a személyisége is, valamint a vállalati kultúra.

Kulcsszavak: biztonságtudatosság, szisztematikus szakirodalmi áttekintés, 2012–2020

Today, digital devices have become an indispensable part of everyday life, whether for work or leisure; they are present in every aspect of life, but they also carry several dangers. As technology advances, a lot of information is exchanged online, uploaded to the cloud, stored on digital devices, potentially allowing privacy and sensitive data to be obtained or leaked by unauthorised parties. A solution to potential threats can be to raise awareness of the people using digital devices. This research aims

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, doktori hallgató, e-mail: bak.gerda@uni-obuda.hu
[2] Nemzeti Közszolgálati Egyetem, egyetemi docens, e-mail: kiss.sandor@uni-nke.hu

to provide an overview of the factors that influence individuals' security awareness. To this end, a systematic literature review was conducted in ScienceDirect, Google Scholar and Web of Science databases between January 2012 and December 2020. The analysis was performed by searching only for articles in English and available in full text, for which appropriate keywords were selected and applied. After conducting the search, a potential 419 publications were analysed in more detail, of which 92 finally met the pre-defined criteria. They found that the level of safety awareness is influenced by, among other things, the individual's gender, age, education, mindset, experience and personality, as well as corporate culture.

Keywords: **security awareness, systematic literature review 2012–2020**

1. Bevezetés

A biztonságtudatosság minden biztonsági infrastruktúra fontos eleme, főként, mert gyakran az emberi tényező bizonyul a leggyengébb láncszemnek. Az utóbbi években a vállalatok és a különböző szervezetek is felismerték a biztonságtudatosság jelentőségét, aminek következtében olyan programokat dolgoztak ki, amelyek a biztonság népszerűsítését és fontosságának tudatosítását tűzték ki célul. Ez azonban nem egyszerű, hiszen a tudatosság növelése folyamatosságot igényel, különösen, hogy a technológia rohamos ütemben fejlődik, továbbá számos kampány nem hozza el a kívánt eredményt, mert az emberek viselkedésének megváltoztatásához a tudatosság és a tudás növelése önmagában nem elegendő.[3] Jelen tanulmány ezért a biztonságtudatosság humán aspektusával foglalkozó tanulmányokat gyűjti egybe és elemzi.

A tanulmány a következő részekből tevődik össze: elsőként bemutatjuk a szakirodalmi áttekintés módszerét, valamint az összegyűjtött tanulmányok fő jellemzőit. A következő részben összefoglaljuk a biztonságtudatosságot befolyásoló tényezőket, amelyeket az elemzett publikációk azonosítottak. A tanulmány végén pedig áttekintjük a tanulmányban bemutatott eredményeket és a jelentőségüket.

A tanulmány két kérdésre keresi a választ. Először is, hogy milyen tendencia figyelhető meg a biztonságtudatossági kutatásokban, illetve hogy melyek a biztonságtudatosság-kutatások főbb eredményei az emberi tényező kapcsán.

2. Biztonságtudatosság

Az információbiztonsági fenyegetések és incidensek komoly veszélyt jelentenek a digitalizált gazdaságok túlélésére. Az ilyen incidensek jelentős pénzügyi veszteségeket, csökkent tőzsdei értékelést, csorbult hírnevet és jogi szankciókat eredményeznek.[4] A bizalmas

[3] Maria Bada – Angela Sasse – Jason R. C. Nurse: *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* In International Conference on Cyber Security for Sustainable Society. United Kingdom, Coventry University, 2015. 118–131.

[4] Daniele Bianchi – Onur Kemal Tosun: Cyber Attacks and Stock Market Activity. *International Review of Financial Analysis,* 76. (2019), 101795.

és érzékeny információk elvesztése vagy ellopása adatonként 150 dollár, évente pedig átlagosan 8,9 millió dolláros veszteséget eredményez az Amerikai Egyesült Államokban.[5]

A szervezetek az informatikai költségvetés mintegy 36%-át fordítják a Security Incident Managementre, amely érték várhatóan az elkövetkező években növekedni fog.[6] A Security Incident Management alatt a biztonsági fenyegetések vagy incidensek valós idejű azonosításának, kezelésének, rögzítésének és elemzésének folyamatát értjük. Célja, hogy megbízható és átfogó képet adjon az informatikai infrastruktúrán belüli biztonsági problémákról. A biztonsági incidens lehet bármi, az aktív fenyegetéstől kezdve a behatolási kísérleten át, a sikeres adatszerzésig. A biztonsági incidensekre példaként említhető a szabályzatok megsértése és az olyan adatokhoz való jogosulatlan hozzáférés, mint az egészségügyi, pénzügyi, társadalombiztosítási számok és személyazonosításra alkalmas adatok.

A szervezeti erőfeszítések és befektetések ellenére az adatvédelmi incidensek sokszorosára nőttek, különösen az ázsiai és a csendes-óceáni térségben.[7] Az egyik nemzetközi kutatás[8] arra a következtetésre jutott, hogy a biztonsági szakemberek nem képesek időben azonosítani a biztonsági incidenseket és azok hatókörét, aminek következtében negatív hatást gyakorolnak a szervezetre. Ezeknek a mulasztásoknak a kezelése létfontosságú a szervezeti üzletmenet folytonossága és túlélése szempontjából.

A digitális eszközök használatával összefüggő bűncselekményekkel növekvő számuk miatt feltétlenül foglalkozni kell. A felhasználók tudatosságának tanulmányozása elengedhetetlen ahhoz, hogy kellően védekezni tudjanak a támadások ellen, illetve tudatosabban létezhessenek a digitális világban.

3. A szisztematikus irodalmi áttekintés módszertana

A vizsgált kutatási területen a releváns publikációk kiválasztásához beválasztási és kizárási kritériumokat határoztunk meg. Úgy döntöttünk, hogy nemcsak az ajánlott[9] magas színvonalú szakirodalomra összpontosítunk, hanem olyan folyóiratokat is bevonunk, amelyek nem szerepelnek magasan a nemzetközi folyóiratrangsorokban. Erre azért volt szükség, mert e folyóiratok némelyike az információbiztonság területére specializálódott (például *Computers & Security* és *Information Management & Computer Security*), és számos olyan témával foglalkozó publikációt tartalmaz, amelyek relevánsak a jelen irodalmi áttekintés szempontjából.

A biztonságtudatosság és az emberi tényező kapcsolatának átfogó áttekintése céljából internetes szakirodalom-keresést folytattunk le a PRISMA protokoll módszertana alapján a Google Scholar, a Scopus-adatbázis és a Web of Science (WoS)

[5] IBM: *Cost of a Data Breach Report* (2019).
[6] Capgemini Consulting: *Information Security Benchmarking 2017*. Report. (2017).
[7] Frost & Sullivan: *Cybersecurity Threats to Cost Organizations in Asia Pacific US$1.75 Trillion in Economic Losses* (2018. május 18.)
[8] PwC: *Information Security Breaches Survey* (2015).
[9] Jane Webster – Watson T. Richard: Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly,* 26. (2002), 2. 13–23; Jan vom Brocke – Christian Buddendick: Security Awareness Management – Konzeption, Methoden und Anwendung. In Otto K. Ferstl et al. (szerk.): *Wirtschaftsinformatik 2005.* Heidelberg, Physica, 2005. 1227–1246.

elektronikus tudományos adatbázis-keresők felhasználásával. Az említett adatbázisok kiválasztását és használatát a következő tényezők indokolták:

A Google Scholars hatalmas adatbázissal rendelkezik, mivel nyilvános, és rengeteg, nem csak indexált folyóiratból származó tanulmányt tartalmaz(hat).

A Web of Science (WoS) esetében éppen fordítva van, mivel magas színvonalú, de nagyon korlátozott számú publikációval rendelkezik.[10]

A Scopus minőségi folyóiratokat tartalmaz, amelyek kiterjedt publikációs készletet fednek le.

Több tanulmány[11] is bizonyítja, hogy a Google Scholar számos témakörben lényegesen több hivatkozást és publikációt eredményez, mint a WoS és a Scopus, illetve mind a WoS-, mind a Scopus-adatbázisokban fellelhető publikációkat is tartalmazza. Ez azt jelenti, hogy az említett két adatbázis eredményeinek nagy arányát a Google Scholar is megtalálja, listázza.

Az internetes keresés a „security awareness" kifejezés segítségével történt, amelynek a keresett irodalom címében, absztraktjában vagy kulcsszavaiban kellett megjelennie.

Az egyszerűsítés kedvéért csak angol nyelven írt anyagok képezték a keresés fókuszpontját, illetve kizárólag a tudományos folyóiratcikkek (a könyvfejezetek vagy a teljes könyvek és a konferenciaanyagok nem képezték az elemzendő adatbázis részét). A releváns cikkek kiválasztásában a Covidence online szoftver nyújtott segítséget. Azokat a publikációkat kiszűrtük, amelyek elsősorban nem az emberi tényező és a biztonságtudatosság témakörével foglalkoznak.

A szisztematikus szakirodalmi áttekintés főbb kutatási kérdései a következők:

1. Milyen tendencia figyelhető meg a biztonságtudatossági kutatásokban?
2. Melyek a biztonságtudatosság-kutatások főbb eredményei az emberi tényező kapcsán?

3.1. Keresési és kiválasztási stratégia

A szakirodalom gyűjtése 2021 májusában zajlott. A szisztematikus irodalmi áttekintések a szakirodalomból nyert információk tudományos módszerekkel történő szintézisei, amelyek részletes, alapos kutatómunka alapján tartalmazzák a kiválasztott adatbázisokban megjelent tudományos eredményeket egy adott témával kapcsolatban.[12]

A cikkek beazonosítása, kiválasztása és elemzése az alábbi lépések mentén történt, a módszer lépéseit az 1. ábra mutatja be.

Adatbázisok: a vizsgálatba a Google Scholar, a Web of Science és a Scopus adatbázisokban megtalálható cikkek szolgáltak a keresés alapjául.

[10] Sandeep Kumar Sood – Navin Kumar – Munish Saini: Scientometric Analysis of Literature on Distributed Vehicular Networks: VOSViewer Visualization Techniques. *Artificial Intelligence Review,* (2021), 1–33.

[11] Alberto Martín-Martín et al.: Google Scholar, Web of Science, and Scopus: A Systematic Comparison of Citations in 252 Subject Categories. *Journal of Informetrics,* 19. (2018), 4. 1160–1177; Jean-François Gehanno – Laetitia Rollin – Stefan Darmoni: Is the Coverage of Google Scholar Enough to be Used Alone for Systematic Reviews. *BMC Medical Informatics and Decision Making,* 13. (2013), 7. 1–5.

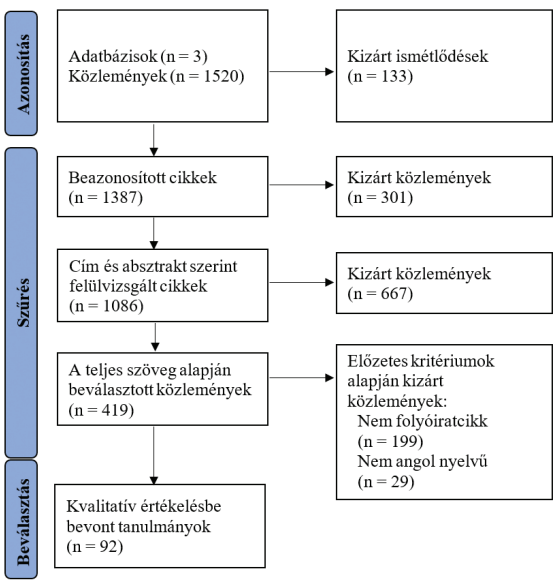
[12] Kamarási Viktória – Mogyorósy Gábor: Szisztematikus irodalmi áttekintések módszertana és jelentősége. Segítség a diagnosztikus és terápiás döntésekhez. *Orvosi Hetilap,* 156. (2015), 38. 1523–1531; Matthew J. Page et al.: The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *British Medical Jorunal,* 372. (2021), n71.

A keresés kulcsszavának kiválasztása: az elemzés során az alábbi kifejezést alkalmaztuk: biztonságtudatosság („security awareness"). Mivel a felsorolt adatbázisokban főként angol nyelvű publikációk találhatók, így a kereséshez a kulcsszó angol nyelvű változatát használtuk, amelyet idézőjelek használata mellett alkalmaztunk, ezzel is minimalizálva a keresési feltételeknek nem megfelelő találatok számát. Mivel a kutatási terület legújabb eredményeinek elemzése a jelen tanulmány célja, ezért az elmúlt kilenc évben publikált, angol nyelven íródott és lektorált folyóiratcikkek képezték a fókuszt. Az online adatbázisokban lefolytatott keresés 1520 találatot eredményezett a korábban említett kifejezésre.

Kizáró kritériumok összegyűjtése: ismétlődéseket, biztonságtudatosság hatásain kívül eső tanulmányokat, nem a humán faktorra vonatkozó biztonságtudatosságot mérő, illetve az azt befolyásoló tényezőket vizsgáló cikkeket, a folyamatban levő kutatásokat, a biztonságtudatosság technológiai, illetve oktatási oldalról megközelítő tanulmányokat, valamint a 2012 előtt, illetve 2020 után publikált elemzéseket, továbbá a nem elérhető értekezéseket kizáró kritériumokként fogalmaztuk meg. A cím, az absztrakt és a kulcsszavak szűrése során 133 ismétlődést és 301 témán kívül eső publikációt azonosítottunk. Az ismétlődések esetében olyan publikációkról van szó, amelyek többször fordultak elő, aminek oka abban keresendő, hogy három különböző adatbázisból kérdeztük le az adatokat.

Az átvizsgálás során beválogatott közlemények kiválasztása: a kizáró kritériumok alapján kiszűrt publikációk eltávolítása után 419 cikk maradt a teljes vizsgálatra.

A kvalitatív értékelésben részt vevő publikációk kiválasztása: a teljes átvizsgálás során 92 cikket választottunk ki, amelyek a minőségi értékelés alapját képezték.



1. ábra

A szisztematikus irodalmi áttekintés folyamatábrája

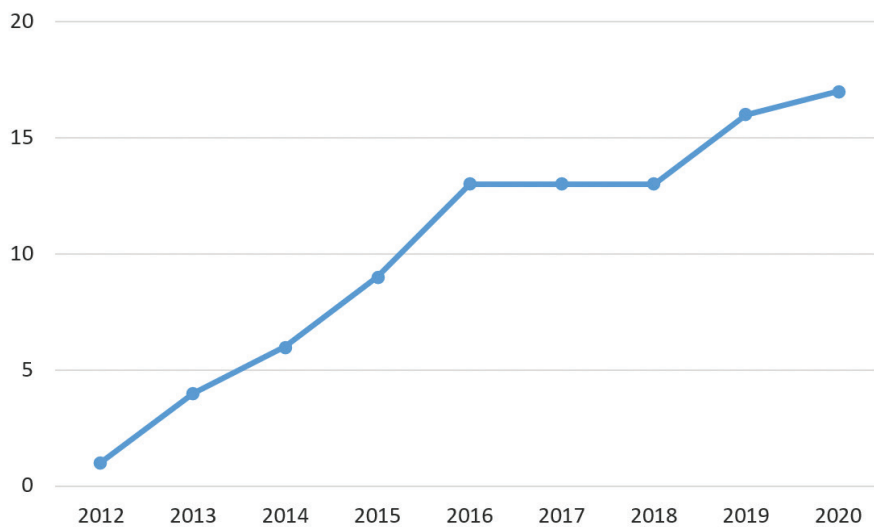
Forrás: a szerzők szerkesztése PRISMA ajánlás alapján

3.2. Adatkinyerés folyamata

A kiválasztott cikkek kvalitatív értékelése után az adatok kiválasztása és kódolása során rögzítettük az alapvető információkat, mint a szerzők neve, az első szerző országa, a publikálás éve, a folyóirat megnevezése, a publikáció nyelve. Ezt követte a témában megjelent közlemények vizsgálata területi eloszlás és megjelenési év alapján. Majd a megjelent publikációk kivonatának átvizsgálása, amely során a publikációkban alkalmazott kutatási módszerek feltárása történt. A beazonosított cikkek áttekintése után azokat az empirikus eredményeket rögzítettük, amelyek kapcsolatban állnak az emberi tényezővel.

4. A szisztematikus irodalmi áttekintés eredményei

A fejezet célja meghatározni a téma elhelyezkedését és beágyazottságát a nemzetközi irodalomban. A biztonságtudatosság humán aspektusait vizsgáló szakirodalmak köre nagymértékben növekszik, amint azt a 2. ábra is mutatja. A kvalitatív elemzésbe beválasztott cikkek alapján a vizsgált kilencéves időszakban évről évre növekedett a témában megjelent publikációk száma. A növekedés olyan mértékűvé vált az elmúlt években, hogy a vizsgált tanulmányok fele a vizsgált időszak utolsó három évében jelent meg, továbbá a téma beágyazottságára növekvő trend jellemző. A téma irodalmának nagy részét az informatikai és gazdasági-menedzsment folyóiratok közlik, azonban oktatás tematikájú területek is képviseltetik magukat.



2. ábra

Az elemzett cikkek számának alakulása 2012–2020 között

Forrás: a szerzők szerkesztése a minta adatai alapján

A biztonságtudatosság kapcsán keletkező kutatások tekintetében az Egyesült Államok, Törökország és Ausztrália emelkedik ki a publikációk számát tekintve (1. táblázat), ezt követi az Egyesült Királyság. Az elemzésekben vizsgált országok megjelenésének számossága azt mutatja, hogy a nemzetközi irodalomban az Egyesült Államok mellett Európa és Ázsia is jelentős figyelmet fordít a témára. Az eredményekből az is látható, hogy számos fejlődő ország igyekszik a biztonságtudatosságot és az emberi tényező kapcsolatát minél jobban megérteni. Azonban szakirodalmi publikációkat figyelembe véve az látható, hogy a közép-európai, kelet-európai, dél-amerikai és közép-ázsiai régiók a témában nem, vagy kis mértékben végeznek kutatásokat.

1. táblázat

Az elemzett országok 10 legtöbbet publikált eleme

Forrás: a szerzők szerkesztése a minta adatai alapján

	Ország	**N**
1.	USA	13
2.	Törökország	9
3.	Ausztrália	9
4.	UK	7
5.	Malajzia	6
6.	Dél-afrikai Köztársaság	5
7.	Horvátország	3
8.	Indonézia	3
9.	Dél-Korea	3
10.	Svédország	2

A teljesség igénye nélkül a következőkben bemutatjuk a főbb kutatási eredményeket a vizsgált szakirodalomból, amelyet a 2. táblázat foglal össze. A táblázatban az adott empirikus megállapításokat az elemzett publikációkban előforduló gyakorisága alapján tüntettük fel, a táblázat harmadik oszlopa az adott megállapítással foglalkozó cikkek számát jelöli.

A nemzetközi szakirodalom kutatási eredményeit áttekintve az látható, hogy a kutatók számos aspektusból igyekeznek a témában megközelíteni a biztonságtudatosságot befolyásoló emberi tényezőket. A legtöbb kutatás (29 db) az emberek szociodemografikus jellemzőire fókuszál, mint a nem, a kor, a jövedelem vagy az iskolázottság. E mellett még nagy hangsúlyt kapott a személyiségjegyek (16 db) vizsgálata is, mint hogy az adott illető mennyire introvertált, miként kezeli a stresszt és mennyire rugalmas. A kutatásba beválasztott publikációk között vannak olyanok is, amelyek jelenleg még a kevésbé vizsgált megközelítések táborába tartoznak, ilyen a biztonságtudatosság digitális írástudással való kapcsolata (8 db), valamint a közösségimédia-felületek használatához köthető jelenség, a FoMO *(fear of missing out)* befolyásoló hatása is (1 db).

2. táblázat

A vizsgált szakirodalom jelentősebb eredményei

Forrás: a szerzők szerkesztése a minta adatai alapján

	Empirikus megállapítások	**N**
1	A demográfiai (kor, nem, iskolai végzettség, lakhely, foglalkozás, munkában eltöltött évek száma) tényezők hatással vannak az egyén biztonságtudatossági szintjére.[13]	29
2	A személyiségjegyek összefüggésben állnak az egyén biztonságtudatosságával és magatartásával.[14]	14
3	A magasabb digitális írástudás magasabb biztonságtudatossággal jár együtt.[15]	14
4	A vállalaton belüli biztonsági irányelvek és a vállalati kultúra pozitív kapcsolatban állnak a biztonságtudatossággal.[16]	13
5	A biztonságtudatosságra vonatkozó tudás és magatartás eltérő.[17]	7
6	A felhasználók alábecsülik a biztonsági incidenseknek való kitettségüket, illetve nincsenek tisztában, hogy kihez fordulhatnak, ha megtörténik az incidens.[18]	6

[13] Atila Bostan – İbrahim Akman: Impact of Education on Security Practices in ICT. *Tehnički Vjesnik,* 22. (2015), 1. 161–168; Mehmet Tekerek – Adem Tekerek: A Research on Students' Information Security Awareness. *Online Submission,* 2. (2013), 3. 61–70; Christian Happ – André Melzer – Georges Steffgen: Trick with Treat – Reciprocity Increases the Willingness to Communicate Personal Data. *Computers in Human Behavior,* 61. (2016), 372–377.

[14] Ivana Borić Letica: Some Correlates of Risky User Behavior and ICT Security Awareness of Secondary School Students. *International Journal of Electrical and Computer Engineering Systems,* 10. (2019), 2. 85–89; Jaime Ortiz et al.: The Contradiction between Self-protection and Self-presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017), 406–416; Agata McCormac et al.: The Effect of Resilience and Job Stress on Information Security Awareness. *Information & Computer Security,* 26. (2018), 3. 277–289.

[15] Peter Sasvári – András Nemeslaki – Rauch Wolf: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Military and Public Management Science,* 14. (2015), 1. 63–78; Özgün Ünal: During COVID-19, Which is More Effective in Work Accident Prevention Behavior of Healthcare Professionals: Safety Awareness or Fatalism Perception? *Work,* 67. (2020), 4. 783–790.

[16] Lee Hadlington – Kathryn Parsons: Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior, and Social Networking,* 20. (2017), 9. 567–571; Ashleigh Wiley – Agata McCormac – Dragana Calic: More than the Individual: Examining the Relationship between Culture and Information Security Awareness. *Computers & Security,* 88. (2020), 101640; Duy Dang-Pham – Siddhi Pittayachawan – Vince Bruno: Why Employees Share Information Security Advice? Exploring the Contributing Factors and Structural Patterns of Security Advice Sharing in the Workplace. *Computers in Human Behavior,* 67. (2017), 196–206.

[17] Hanieh Yaghoobi Bojmaeh: Mediating Role of Information System Security Awareness in the Relationship between Self-Efficacy, Security Practice and Information System Security Behavior. *International Journal of Science and Engineering Applications,* 4. (2015), 6. 361–365; Zakaria I. Saleh – Ahmad Mashhour: Evaluating Security Awareness Impact on Perceived Risk and Trust: The Case of Social Networks. *International Journal in IT & Engineering,* 4. (2016), 5. 99–110.

[18] Awil Ahmed Mohamed – Othman Ibrahim – Mehrbakhsh Nilashi: The Security Awareness Framework for Social Network Sites Facebook: Case Study in Universiti Teknologi Malaysia. *Journal of Soft Computing and Decision Support Systems,* 2. (2015), 3. 1–8; Puspita Kencana Sari – Candiwan Candiwan: Measuring Information Security Awareness of Indonesian Smartphone Users. *Telkomnika,* 12. (2014), 2. 493–500; Adedayo Williams – Akanmu Semiu Ayobami: Relationship between Information Security Awareness and Information Security Threat. *International Journal of Research in Commerce,* IT & Management, 3. (2013), 8. 115–119.

	Empirikus megállapítások	N
7	Az egyén gondolkodásmódja és információmegosztási hajlandósága hatással van a biztonságtudatossági szintre.[19]	6
8	A biztonsági incidensekkel való tapasztalat pozitívan befolyásolja a biztonságtudatossági szintet.[20]	2
9	A FoMO *(fear of missing out)* negatívan befolyásolja az egyén információbiztonság-tudatosságát.[21]	1

A 3. táblázatban az elemzett 92 publikáció látható aszerinti bontásban, hogy mely célcsoportot, mintát vizsgálta, és mik voltak a kutatás céljai, továbbá milyen módszerrel vizsgálták azt, valamint hogy számszakilag mennyi publikáció tartozik az adott csoportba.

Az alábbi táblázatból láthatjuk, hogy a vizsgálatba bevont publikációk nagy része (40 db; 43,5%) a munkavállalókra vagy munkatapasztalattal rendelkező egyénekre fókuszált. Ezeknek a kutatásoknak a vizsgálati fókuszában áll az elemzett minta biztonságtudatossági szintjének feltérképezése, illetve hogy milyen tényezők (életkor, iskolázottság, jövedelem stb.) hatnak rá, hogyan lehet növelni ezt a szintet, milyen munkahelyi körülmények (vezetői stílus, vállalati policy) tudják szintén befolyásolni, valamint, hogy maga az egyén viselkedésmódja, gondolkodása, problémamegoldó képessége és szociális készségei miként határozzák meg. Mindezeknek a tesztelésére az alkalmazott módszerek között megtalálható a kérdőív alkalmazása, interjú lefolytatása, valamint a kísérlet.

A kutatók által másik gyakran vizsgált minta a tanulók csoportja (33 db), mind az egyetemisták (27 db), mind az általános és középiskolás (6 db) korosztály. A két csoport között feltűnő különbség, hogy míg a fiatalabb korosztály tagjait a biztonságtudatossági szintjük és a kapcsolódó viselkedésük vizsgálata kapcsán elemezték, addig az egyetemisták esetében a kockázatok mérséklése, valamint a használati szokások feltérképezése és a tudásmegosztási hajlandóság is a vizsgálat tárgyát képezte.

Érdekességként megemlítendő, hogy a mobil-, illetve okostelefon-használók körében végzett kutatások száma a legalacsonyabb (4 db) a vizsgált mintában, valamint csak az egyének biztonságtudatossági szintjének mérésére koncentrál, amelyet kérdőívvel vizsgáltak.

[19] Gizem Öğütçü – Özlem Müge Testik – Oumout Chouseinoglou: Analysis of Personal Information Security Behavior and Awareness. *Computers & Security,* 56. (2016), 83–93; Charlette Donalds – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020), 102056; Wasim Qazi – Syed Ali Raza – Komal Akram Khan: The Contradiction between Self-protection and Self-presentation on Knowledge Sharing Behaviour: Evidence from Higher Education Students in Pakistan. *International Journal of Knowledge and Learning,* 13. (2020), 3. 246–271.

[20] Pelin Bolat – Gizem Kayişoğlu: Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. *Journal of ETA Maritime Science,* 7. (2019), 4. 344–360; Bartlomiej Hanus – John C. Windsor – Yu Wu: Definition and Multidimensionality of Security Awareness. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* 49. (2018), 49. 103–133.

[21] Lee Hadlington – Jens Binder – Natalia Stanulewicz: Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender. *Cyberpsychology, Behavior, and Social Networking,* 23. (2020), 7. 459–464.

3. táblázat

A vizsgált szakirodalom kutatási céljai és vizsgált mintái

Forrás: a szerzők szerkesztése a minta adatai alapján

Minta	Kutatási célok	Módszer	N
munkavállalók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők biztonságtudatosságot mérő eszköz létrehozása, tesztelése biztonságtudatosság növelését célzó programok, tréningek hatása a biztonságtudatosságra a munkahelyi környezet hatása a biztonságtudatosságra az egyén személyiségjegyei, kockázatvállalási hajlama miként befolyásolja a biztonságtudatosságot okoseszközök használatához kapcsolódó viselkedés megismerése információbiztonsági tudásmegosztási hajlandóság mérése	kérdőív, interjú, kísérlet	40
egyetemisták	információbiztonsági kockázatok mérséklése, lehetőségeinek azonosítása biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők a biztonságtudatosságról alkotott elképzelések feltárása biztonságtudatosságot mérő eszköz létrehozása, tesztelése információbiztonsági tudásmegosztási hajlandóság mérése digitális/okoseszközök használati mintázata okoseszközök használatához kapcsolódó viselkedés megismerése	kérdőív	27
lakosság vagy vegyes csoport	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők biztonságtudatosságot mérő eszköz létrehozása, tesztelése biztonságtudatosság növelését célzó programok, tréningek hatása a biztonságtudatosságra	kérdőív, kísérlet	9
általános vagy középiskolás tanulók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők okoseszközök használatához kapcsolódó viselkedés megismerése	kérdőív	6
közösségimédia-felhasználók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők biztonságtudatosságot mérő eszköz létrehozása, tesztelése közösségimédia-oldalak használatához köthető kockázatok észlelésének mérése információbiztonsági, tudásmegosztási hajlandóság mérése	kérdőív	6
mobiltelefon-használók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők	kérdőív	4

5. Következtetések

Jelen kutatás célja a biztonságtudatosság szisztematikus áttekintése volt. A tanulmány azt is megvizsgálta, hogy a biztonságtudatosság és az ember kapcsolatát mely országok kutatják a legnagyobb részben, valamint hogy miként változott a kutatási téma az elmúlt években. Figyelembe véve a tanulmányban bemutatott empirikus

irodalmat és eredményeit, az látható, hogy az egyén biztonságtudatosságát számos tényező befolyásolhatja. Ezek a befolyásoló tényezők lehetnek a szociodemografikus tényezők, mint a nem, a kor, az iskolázottság, vagy a jövedelem, lakhely, azonban számos olyan tényező is akad, amelyek kevésbé egzaktak, illetve azok meghatározása, mérése sem egyszerű. Egyrészt ilyen az egyén attitűdje, én-hatékonysága és egyéb más személyiségjegyek, vagy akár maga a szervezeti kultúra. Azonban nem árt figyelembe venni, hogy e befolyásoló tényezők hatása régiónként, kultúránként változhat.

A biztonságtudatosságot befolyásoló emberi tényezők és az ezt vizsgáló kutatások feltérképezésére azért volt szükség, mert így képet kaphatunk a tématerület aktuális állásáról, illetve eredményeiről. Ezáltal kirajzolódhat előttünk, hogy mik azok a tényezők, amelyekre egy-egy tréning, vagy a biztonságtudatosság felmérése során érdemes hangsúlyt fektetni. Másik szempontból pedig hozzájárul a biztonságtudatosság és a már kapcsolódó társtudomány-területek feltérképezéséhez, vagy akár egy teljesen új megközelítési módon, más tudományterületről érkező kutatást vezethet elő. Ezt alapul véve a kutatás következő szakaszában érdemes lehet megvizsgálni a biztonságtudatossággal foglalkozó publikációk esetében kialakult hálózatokat is mind a kutatói együttműködések, hivatkozások, mind a kulcsszavak tekintetében.

Továbbá megfontolandó a következő kutatások során más adatbázisokat is bevonni a szélesebb körű ismeretek feltérképezésére, valamint az egyes publikációk közötti kapcsolatok feltérképezésére is.

6. Összefoglalás

Ebben a tanulmányban a PRISMA-módszertant alkalmaztuk, amely során a kutatás célja volt többek között a minél szélesebb és alaposabb összegyűjtése a fókuszt képező tanulmányoknak. Annak ellenére, hogy az elemzés főként a nemzetközi adatbázisokra koncentrált, illetve a folyóirat-publikációkra, és ezáltal biztosítva van a bevont tanulmányok minősége, a vizsgált minta alacsony száma miatt felvetődhet a kérdés, érdemes volt-e ilyen szigorú megkötéseket alkalmazni. Ezt figyelembe véve a jövőre nézve érdemes megfontolni a szigorú kritériumok enyhítését, azaz a konferenciatanulmányok és más adatbázisok bevonását, ezáltal biztosítva a szélesebb nemzetközi palettát.

A szakirodalmi áttekintésben az elmúlt kilenc évben keletkezett empirikus tanulmányok felhasználásával történt a biztonságtudatosság emberi vonzatainak bemutatása. Az eredmények alapján elmondható, hogy bár a tématerület viszonylag új keletű, számos kutatás zajlik, amelyek mind igyekeznek csökkenteni az emberi hibából, óvatlanságból bekövetkező hibák mértékét, azáltal, hogy felfedik, milyen tényezők játszanak szerepet a mulasztások kialakulásában és bekövetkezésében.

Jelen kutatás korlátai közé sorolható, hogy a kutatott tématerület feltérképezését, annak helyzetét és az eddigi kutatási irányok, illetve eredmények megismerését célozta, ezáltal segítve a kiválasztott tématerületen való mélyebb kutatások előkészítését mind további tudománymetriai, mint pedig primer adatok elemzésével.

Bár a releváns szakirodalom felkutatására szigorú megközelítést alkalmaztunk, a felhasznált keresőkifejezés és az azonosított szakirodalom tekintetében vannak

korlátok. Csak angol nyelvű keresőkifejezést használtunk. Más nyelvű publikációkat nem vizsgáltunk. Ezenkívül a keresőkifejezést előre meghatároztuk, és nem induktív módon alakítottuk ki. A későbbiekre tekintettel egy második keresési folyamatot is kell végezni az irodalomelemzés során összegyűjtött kifejezésekkel, hogy további, a jelen szakirodalmi áttekintés szempontjából releváns szakírásokat találjunk. A nem lektorált publikációk (például könyvek, reportok) kizárásával csak az ellenőrzött minőségű publikációk kerültek be az elemzési folyamatba. Ennek ellenére úgy véljük, hogy a könyvek is tartalmazhatnak értékes konferenciaanyagokat, kutatásokat, amelyek hiányozhatnak ebből a szakirodalmi áttekintésből.

Felhasznált irodalom

Bada, Maria – Angela Sasse – Jason R. C. Nurse: *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* In International Conference on Cyber Security for Sustainable Society. United Kingdom, Coventry University, 2015. 118–131.

Bianchi, Daniele – Onur Kemal Tosun: Cyber attacks and Stock Market Activity. *International Review of Financial Analysis,* 76. (2019), 101795. Online: https://doi.org/10.1016/j.irfa.2021.101795

Bojmaeh, Hanieh Yaghoobi: Mediating role of Information System Security Awareness in the relationship between Self-Efficacy, Security Practice and Information System Security Behavior. *International Journal of Science and Engineering Applications,* 4. (2015), 6. 361–365. Online: https://doi.org/10.7753/IJSEA0406.1006

Bolat, Pelin – Gizem Kayişoğlu: Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. *Journal of ETA Maritime Science,* 7. (2019), 4. 344–360. Online: https://doi.org/10.5505/jems.2019.85057

Borić Letica, Ivana: Some Correlates of Risky User Behavior and ICT Security Awareness of Secondary School Students. *International Journal of Electrical and Computer Engineering Systems,* 10. (2019), 2. 85–89. Online: https://doi.org/10.32985/ijeces.10.2.4

Bostan, Atila – İbrahim Akman: Impact of Education on Security Practices in ICT. *Tehnički Vjesnik,* 22. (2015), 1. 161–168. Online: https://doi.org/10.17559/TV-20140403122930

Capgemini Consulting: *Information Security Benchmarking 2017.* Report. (2017). Online: www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/11/information-security-benchmark-2017.pdf

Dang-Pham, Duy – Siddhi Pittayachawan – Vince Bruno: Why Employees Share Information Security Advice? Exploring the Contributing Factors and Structural Patterns of Security Advice Sharing in the Workplace. *Computers in Human Behavior,* 67. (2017), 196–206. Online: https://doi.org/10.1016/j.chb.2016.10.025

Donalds, Charlette – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020), 102056. Online: https://doi.org/10.1016/j.ijinfomgt.2019.102056

Frost & Sullivan: *Cybersecurity Threats to Cost Organisations in Asia Pacific US$1.75 Trillion in Economic Losses* (2018. május 18.). Online: https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/

Gehanno, Jean-François – Laetitia Rollin – Stefan Darmoni: Is the Coverage of Google Scholar Enough to be Used Alone for Systematic Reviews. *BMC Medical Informatics and Decision Making,* 13. (2013), 7. 1–5. Online: https://doi.org/10.1186/1472-6947-13-7

Hadlington, Lee – Jens Binder – Natalia Stanulewicz: Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender. *Cyberpsychology, Behavior, and Social Networking,* 23. (2020), 7. 459–464. Online: https://doi.org/10.1089/cyber.2019.0703

Hadlington, Lee – Kathryn Parsons: Can Cyberloafing and Internet Addiction Affect Organisational Information Security? *Cyberpsychology, Behavior, and Social Networking,* 20. (2017), 9. 567–571. Online: https://doi.org/10.1089/cyber.2017.0239

Hanus, Bartlomiej – John C. Windsor – Yu Wu: Definition and Multidimensionality of Security Awareness. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* 49. (2018), 49. 103–133. Online: https://doi.org/10.1145/3210530.3210538

Happ, Christian – André Melzer – Georges Steffgen: Trick with Treat – Reciprocity Increases the Willingness to Communicate Personal Data. *Computers in Human Behavior,* 61. (2016), 372–377. Online: https://doi.org/10.1016/j.chb.2016.03.026

IBM: Cost of a Data Breach Report (2019). Online: https://doi.org/10.1016/S1361-3723(19)30081-8

Kamarási Viktória – Mogyorósy Gábor: Szisztematikus irodalmi áttekintések módszertana és jelentősége. Segítség a diagnosztikus és terápiás döntésekhez. *Orvosi Hetilap,* 156. (2015), 38. 1523–1531. Online: https://doi.org/10.1556/650.2015.30255

Martín-Martín, Alberto – Enrique Orduna-Malea – Mike Thelwall – Emilio Delgado López-Cózar: Google Scholar, Web of Science, and Scopus: A Systematic Comparison of Citations in 252 Subject Categories. *Journal of Informetrics,* 19. (2018), 4, 1160–1177. Online: https://doi.org/10.1016/j.joi.2018.09.002

McCormac, Agata – Dragana Calic – Kathryn Parsons – Marcus Butavicius – Malcolm Pattinson – Meredith Lillie: The Effect of Resilience and Job Stress on Information Security Awareness. *Information & Computer Security,* 26. (2018), 3. 277–289. Online: https://doi.org/10.1108/ICS-03-2018-0032

Mohamed, Awil Ahmed – Ibrahim, Othman – Nilashi, Mehrbakhsh: The Security Awareness Framework for Social Network Sites Facebook: Case Study in Universiti Teknologi Malaysia. *Journal of Soft Computing and Decision Support Systems,* 2. (2015), 3. 1–8. Online: www.jscdss.com/index.php/files/article/view/33

Ortiz, Jaime – Shu-Hao Chang – Wen-Hai Chih – Chia-Hao Wang: The Contradiction Between Self-protection and Self-presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017), 406–416. Online: https://doi.org/10.1016/j.chb.2017.07.031

Öğütçü, Gizem – Özlem Müge Testik – Oumout Chouseinoglou: Analysis of Personal Information Security Behavior and Awareness. *Computers & Security,* 56. (2016), 83–93. Online: https://doi.org/10.1016/j.cose.2015.10.002

Page, Matthew J. – Joanne E. McKenzie – Patrick M. Bossuyt – Isabelle Boutron – Tammy C. Hoffmann – Cynthia D. Mulrow – Larissa Shamseer – Jennifer M. Tetzlaff – Elie A. Akl – Sue E Brennan et al.: The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *British Medical Jorunal,* 372. (2021), n71. Online: https://doi.org/10.1136/bmj.n71

PwC: *Information Security Breaches Survey* (2015). Online: www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Qazi, Wasim – Syed Ali Raza – Komal Akram Khan: The Contradiction between Self-protection and Self-presentation on Knowledge Sharing Behaviour: Evidence from Higher Education Students in Pakistan. *International Journal of Knowledge and Learning,* 13. (2020), 3. 246–271. Online: https://doi.org/10.1504/IJKL.2020.10032181

Saleh, Zakaria I. – Ahmad Mashhour: Evaluating Security Awareness Impact on Perceived Risk and Trust: The Case of Social Networks. *International Journal in IT & Engineering,* 4. (2016), 5. 99–110.

Sari, Puspita Kencana – Candiwan Candiwan: Measuring Information Security Awareness of Indonesian Smartphone Users. *Telkomnika,* 12. (2014), 2. 493–500. Online: https://doi.org/10.12928/TELKOMNIKA.v12i2.2015

Sasvári, Péter – András Nemeslaki – Wolf Rauch: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Military and Public Management Science,* 15. (2015), 1. 63–78. Online: https://doi.org/10.32565/aarms.2015.1.6

Sood, Sandeep Kumar – Navin Kumar – Munish Saini: Scientometric Analysis of Literature on Distributed Vehicular Networks: VOSViewer Visualization Techniques. *Artificial Intelligence Review,* (2021), 1–33. Online: https://doi.org/10.1007/s10462-021-09980-4

Tekerek, Mehmet – Adem Tekerek: A Research on Students' Information Security Awareness. *Online Submission,* 2. (2013), 3. 61–70. Online: https://doi.org/10.19128/turje.181065

Ünal, Özgün: During COVID-19, Which is More Effective in Work Accident Prevention Behavior of Healthcare Professionals: Safety Awareness or Fatalism Perception? *Work,* 67. (2020), 4. 783–790. Online: https://doi.org/10.3233/WOR-203327

Vom Brocke, Jan – Christian Buddendick: Security Awareness Management – Konzeption, Methoden und Anwendung. In Otto K. Ferstl – Elmar J. Sinz – Sven Eckert – Tilman Isselhorst (szerk.): *Wirtschaftsinformatik 2005. Heidelberg,* Physica, 2005. 1227–1246. Online: https://doi.org/10.1007/3-7908-1624-8_64

Webster, Jane – Richard T. Watson: Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly,* 26. (2002), 2. 13–23.

Wiley, Ashleigh – Agata McCormac – Dragana Calic: More than the Individual: Examining the Relationship between Culture and Information Security Awareness.

Computers & Security, 88. (2020), 101640. Online: https://doi.org/10.1016/j.cose.2019.101640

Williams, Adedayo – Akanmu Semiu Ayobami: Relationship between Information Security Awareness and Information Security Threat. *International Journal of Research in Commerce,* IT & Management, 3. (2013), 8. 115–119.

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 101–112.
DOI: 10.32567/hm.2021.4.8

Bihaly Barbara[1]

Az elektronikai hadviselés eszközei az információs és kibertérműveletek támogatásában az ukrán konfliktus példáján keresztül

Electronic military instruments in support of information and cyberspace operations through the example of the ukrainian conflict

A világ minden eddiginél jobban függ az elektronikai (információs) rendszerektől, ennélfogva az egyre kifinomultabb elektronikai hadviselés, valamint a kibertér- és információs műveletek egyre nagyobb hangsúlyt kapnak az érdekérvényesítés során. Oroszország jelentős jártasságot mutatott e területeken, különösen az ukrajnai válság idején. Oroszország tartós információs műveleti kampányt folytat a geopolitikai érdekszférájában. Aggodalomra ad okot ugyanakkor az EW és a kibertérműveleti képességek potenciális hatása az erők operatív hatékonyságára és túlélőképességére, ha valaha is konfrontáció lép fel.

Kulcsszavak: elektronikai hadviselés, információs műveletek, Ukrajna

The world is more than ever dependent on electronic (information) systems, hence the increasing sophistication of electronic warfare, cyber and information operations with increasing emphasis on advocacy. Russia has shown considerable expertise in these areas, especially during the crisis in Ukraine. Russia is conducting a sustained information operations campaign in its geopolitical sphere of interest. At the same time, the potential impact of EW and cyber capabilities on the operational efficiency and survival of forces, should confrontation ever arise, is a cause for concern.

Keywords: electronic warfare, information operation, Ukraine

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktori hallgató, e-mail: bihaly.barbara@hm.gov.hu

1. Bevezetés

Oroszország már a bolsevik hatalomátvétel óta használja a dezinformációs műveleteket, és az 1970-es évek óta tanulmányozza, hogyan lehet szoftveresen támadó műveletet végrehajtani. A hadsereg információs térben betöltött szerepének orosz megértése sokkal szélesebb, mint a nyugati modellben. A nyugati gondolkodásmódban a „kibertér" a kulcsfogalom, amely jobban megfelel a katonai környezetnek. Az orosz hadművészet azonban az „információs tér" fogalmát használja, amelyet társadalmi, politikai és civilizációs fenyegetések összefüggésében hoznak fel. Az orosz hadsereg tevékenységének, „információs" jellegének hangsúlyozásával és nem „kiber" jellegével a stratégák az információkra, valamint az általa kiváltott politikai agitációra és mozgósításra összpontosítanak, ami összhangban áll az információk saját személyzetükre és polgári lakosságára gyakorolt hatásával. A szovjet idők óta egy másik tényező, amely súlyosan rányomta bélyegét az orosz stratégiákra, az a tény, hogy Oroszország mindig élesen érzékelte és igyekezett ellensúlyozni technikai és gazdasági alacsonyabb rendűségét azáltal, hogy az aszimmetrikus stratégiákat szisztematikusan feltárta és integrálta a műveleteibe. A legtöbb stratéga hangsúlyozza, hogy az orosz rádióelektronikai harc (oroszul: радиоэлектронная борьба, РЭБ; NATO-meghatározás szerint: electronic warfare, EW) és információs műveleti koncepciók mind a technikai, mind a pszichológiai képességek mesteri kombinációi, a stratégiai céloknak vannak alárendelve azért, hogy túlerőt képezzenek és visszatartsák az ellenérdekelt felet a támadástól.[2]

Oroszország fő fókusza a kutatás-fejlesztés a hadseregen belül, és mindenekelőtt az új mélyreható fegyverek és a fejlett C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance, magyarul: vezetés, irányítás, kommunikáció, számítógépek, hírszerzés, megfigyelés és felderítés) eszközeinek fejlesztése. Ennek ellenére a jelenlegi szelektív befektetési stratégia és a sebezhetőségek körültekintő elemzése megfelelő erőforrások hiányában is lehetővé teheti Oroszország számára, hogy ismét beszálljon a fegyverkezési versenybe, sőt felülmúlja a nyugati erőket bizonyos műveleti résekben – például az információs/(rádió)elektronikai hadviselésben.[3] Az orosz РЭБ-képesség, szemben a nyugati hasonszőrű képességekkel, a hadviselés informatikai-technikai eszközeinek egyik legfontosabb támogatójává vált.

A tanulmány célja bemutatni, hogy az elektronikai hadviselés eszközei milyen módon képesek támogatni az információs és kibertérműveleteket; mindezt az ukrán konfliktus példáján keresztül kívánom elemezni.

2. Az elektronikai hadviselés és funkciói

Az elektronikai hadviselés a modern konfliktusok egyik legtitkosabb és ennélfogva talán legkevésbé megértett aspektusa, gyakran pontatlanul összegzik, mint az ellenfél elektronikai rendszerei korlátozásának képességét. Ennél azonban sokkal többről van

[2] Dévai Dóra: An Overview of the Development of the Russian Information Warfare Concept Part 2. *Hadtudományi Szemle,* 13. (2020), 2. 5–12.

[3] Jolanta Darczewska: Russia's Armed Forces on the Information War Front, Strategic Documents. *OSW Studies (Center for Eastern Studies),* (2016), 57. 1–50.

szó. A hírszerzés az adatbázis építésétől, a műveleti területen való megtévesztésen át az ellenfelek elektronikai rendszerei működésének akadályozásáig, zavarásáig és a működés teljes ellehetetlenítéséig az EW széles körű lehetőséget kínál a döntő fölény megszerzésére. Lényeges, hogy ez az előny a földfelszíntől az űrbe telepített rendszerekig elérhető az elektromágneses spektrum (electromagnetic spectrum, EMS) kihasználásával. Az РЭБ konvergál a kibertér- és információs műveletekkel, hatékony és rugalmas eszközöket kínál a katonai hatás elérésére és az információs tér uralására, több egyidejű támadási vektor révén.

Definíciószerű megfogalmazás szerint az „elektronikai hadviselés: a műveleti (hadműveleti, harc-) támogatás fajtája. Azon tevékenységek összessége, amelyek az elektromágneses spektrum ellenség által történő felhasználásának meghatározására, felderítésére, csökkentésére vagy megakadályozására, illetve az elektromágneses energia és az irányított energia felhasználására, az elektromágneses spektrum saját célú felhasználására, valamint az ellenség vezetési és irányítási rendszerei támadásának támogatására, a saját csapatok védelmére irányulnak".[4]

Hazánkban az elektronikai hadviselés külön dedikált doktrínával rendelkezik, amely szerint e tevékenység fogalma: „[O]lyan 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."[5]

Ezekből a fogalmi meghatározásokból következtethetően az elektronikai hadviselésnek három funkcionális területe van: elektronikai támogatás, elektronikai ellentevékenység és elektronikai védelem. Az ehhez a három területhez tartozó feladatok is levezethetők. Az elektronikai támogatáshoz tartozó feladatok alatt értjük az elektromágneses spektrumban történő veszélyjelzés, a felderítés és célazonosítás képességekhez való hozzájárulást, valamint a rádióelektronikai felderítés tevékenység támogatását. Az elektronikai ellentevékenység feladatai alatt értjük a légierő műveleteiben a repülőgépek önvédelmi elektronikai hadviselési feladatait, kötelékoltalmazást (zavarást), az ellenséges légvédelem lefogását; szárazföldi tevékenység esetén ezek a feladatok lehetnek a szemben álló fél kommunikációs eszközeinek, radarjainak vagy akár navigációs eszközeinek zavarása vagy megtévesztése. Elektronikai védelem esetében a saját eszközrendszerek védelme, a csapatok közvetlen vagy közvetett oltalmazása, illetve a vezeték nélküli távirányítással működő improvizált robbanóeszközök zavarása a feladat.[6]

Az orosz meghatározást két, az orosz РЭБ-csapatokon belül és a Voronyezsi Légierő Akadémián működő РЭБ Osztálynál szolgáló ezredes foglalta össze egy 2017-ben megjelent cikkben: „A rádióelektronikai harc összehangolt tevékenységek és cselekvések összessége, amely magában foglalja a kontradiktórius rádióelektronikai és információ-technológiai objektumok elleni rádióelektronikai támadásokat, a rádióelektronikai és információs-technológiai objektumok rádióelektronikai védelmét,

[4] Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás. MH Vezetési és Doktrinális Központ, 2012.
[5] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 2. kiadás, 2015.
[6] Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232.

a műszaki felderítéssel szembeni ellenintézkedéseket és a rádióelektronikai információs támogató intézkedéseket."[7]

A korábbi szovjet *Katonai Enciklopédia* meghatározása szerint az РЭБ: „[O]lyan intézkedések összessége, amelyeket a kontradiktív rádióelektronikai berendezések és rendszerek rádiófrekvenciájának azonosítása és későbbi zavarása, valamint a saját erők rádióelektronikai berendezéseinek és rendszereinek védelme érdekében hoznak."[8]

Bár első olvasásra ez az első, 1984-es szovjet meghatározás meghökkentően hasonló a jelenleg érvényben lévő magyar doktrinális megfogalmazáshoz, de a magyar meghatározásban az elektromágneses környezet mint fogalom használata sokkal szélesebb felhasználásra enged következtetni, mint csupán a szovjetek által használt „rádióelektronikai" kifejezés. Ugyanakkor az új, 2017-es orosz meghatározás már utal a teljes „információs térre", amely a magyar definíciónál is tágasabb mozgásteret engedélyez a műveletek számára. Tehát alapvetően, annak ellenére, hogy a mai napig a rádióelektronikai harc kifejezést használják, minden vezeték nélküli eszköz használatát/zavarását értik ezalatt.

A szovjet РЭБ az 1980-as években támadó és védekező РЭБ-intézkedésekre volt felosztva, tehát feladatrendszerük szerint létezett „rádióelektronikai elnyomás" (Радио Электронные по-давление) és „rádióelektronikai védelem" (радиоэлектронная защита). A cél észlelésének és a célmegjelölésnek a folyamatát nem hagyták ki a definícióból, hanem inkább elválaszthatatlanul kezelték a támadó és védekező РЭБ-intézkedésektől.

1990-re a szovjet haditengerészeti szótárban az РЭБ meghatározása néhány, főleg „kozmetikai" változáson ment keresztül. Az 1990-es definíció szerint: „A rádióelektronikai harc olyan intézkedések és tevékenységek összessége, amelyek időben, célokban és feladatokban kapcsolódnak egymáshoz, és amelyeket a csapatok (erők) hajtanak végre az ellenséges rádióelektronikai berendezések és rendszerek felderítése és későbbi (bármilyen típusú fegyverrel történő) megsemmisítése, megszüntetése vagy rádióelektronikai elnyomása érekében, valamint az erők saját rádióelektronikai berendezéseinek és rendszereinek elektronikai védelme céljából. Az РЭБ harci támogató funkció."[9]

A 2017-es meghatározás számos tekintetben eltér a korábbi szovjet és orosz definícióktól. Az első és a leginkább szembetűnő különbség az, hogy további külön területekre osztják az РЭБ-t, hisz külön veszik a műszaki felderítést és az információ elleni tevékenységet, valamint a rádióelektronikai információtámogató intézkedést. Másrészről, a hagyományos РЭБ támadó oldalát, a „rádióelektronikai elnyomást" rádióelektronikai támadás váltja fel. Ily módon a támadó РЭБ-fegyverek sokféleségét kibővítették olyan eszközökkel, amelyek képesek elpusztítani az elektronikai berendezéseket. Ennek megfelelően a radióelektronikai védelemben szereplő intézkedések köre is kibővült. Harmadszor, a korábbi „rádióelektronikai berendezések és rendszerek" információtechnológiai eszközökkel való helyettesítésével a védelemre szoruló saját eszközök és célpontok típusainak köre, amelyekre РЭБ-intézkedések vonatkozhatnak,

[7] V. F. Guzenk – A. L. Morarescu: *Radioelektronnaia borba. Sovremennoe soderzhanie. Tematicheskiy Sbornik. Radioelektronnaia borba v vooruzhennykh silakh Rossiiskoi Federatsii.* Moszkva, Informatsionnyi Most, 2017.

[8] *Military Encyclopaedia: Voennyi Entsiklopedicheskii Slovar.* Moscow, Voennoe Izadatelstvo, 1984.

[9] *Naval Dictionary: Voenno-morskoi Slovar.* Moscow, Voennoe Izadatelstvo, 1990.

kibővültek. Az РЭБ célpontjai tehát nem korlátozódnak az EMS-ben közvetlenül aktív berendezésekre és rendszerekre, például rádiókommunikációs berendezésekre, radarra, elektrooptikai érzékelőkre és így tovább. Az olyan mögöttes rendszerek, mint a számítógépek, az adattároló és az energiaellátó rendszerek, szintén célpontok az РЭБ definíciójának értelmében.

Azt is fontos itt megemlíteni, hogy az eredeti orosz kifejezés, mint „rádióelektronikai harc" a mai napig tartja magát a hivatalos orosz szövegekben, bár a teljes EMS működési tartományt értik alatta, holott az nyilvánvalóan túlmutat a rádiófrekvencián és az ahhoz a hullámhosszhoz tartozó eszközök használatán.

3. Orosz elektronikai hadviselés az ukrán válság során

Az ukrán hadsereg komoly segítséget kapott az Egyesült Államoktól az orosz–ukrán konfliktus során, cserébe az ukrán tapasztalatokat az USA feldolgozta és kielemezte. Az amerikai fél arra a következtetésre jutott elemzései során, hogy „az orosz fél komoly fejlesztéseket hajtott végre a fegyveres erejének modernizációja terén, amely során az elektronikai hadviselési képességek is hatalmas fejlődést mutatnak. Az orosz hadsereg megtartotta, sőt fejlesztette a hagyományos elektronikai hadviselési erőit, ezen belül kiemelt figyelmet fordítottak a rádiózavaró, navigációs eszközöket zavaró, illetve egyéb szárazföldi elektronikai eszközök, valamint rádiólokációt zavaró képességeik fejlesztésére".[10]

Oroszország jelentős beruházásokat hajtott végre az РЭБ-képességek fejlesztésében a 2008-as katonai reformok óta.[11] A РЭБ mára olyan mélyen integrálódott az orosz szárazföldi erőkbe, hogy már nem hajtanak végre úgy műveletet, hogy meg ne jelenne benne az РЭБ mint képesség. Oroszország ukrajnai műveleteit az РЭБ, a kibertér- és az információs műveletek szinergikus alkalmazása támasztja alá, amely az alábbiak szerint jellemezhető.

Az offenzív РЭБ-taktikák között szerepel több elektronikai támadó rendszer alkalmazása az EMS több tartományának egyidejű zavarása, ezáltal lerontva és ellehetetlenítve a globális navigációs műholdas rendszerek (*Global Navigation Satellite System,* GNSS), valamint a harcászati rádió-, mobil és műholdas kommunikáció hozzáférését. Az offenzív РЭБ-taktika különösen jól alkalmazható a hibrid hadviselésben, mivel az РЭБ-rendszerek úgy hangolhatók, hogy finom és kevésbé eszkalatív, nem kinetikus hatásokat hozzanak létre viszonylag rejtett módon, például úgy, hogy átmenetileg ellehetetlenítik a kommunikációt.[12]

Az ukrán védelmi minisztérium megerősítette, hogy Oroszország ezeket a taktikákat alkalmazza a harctéren. Például Oroszország által a Donbas régióban telepített Protek R-330Zh Zhytel rendszer képes a VHF, UHF és L sávokban működő ukrán kommunikációs rendszerek észlelésére, iránymérésére és megzavarására. Egy másik példa az orosz Leer-3 RB-341 rendszer, amely legfeljebb három Orlan-10 pilóta nélküli

[10] Kovács (2017): i. m. 221.
[11] Roger N. McDermott: *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Tallinn, International Centre for Defence and Security, 2017. 5–11.
[12] US Army Asymmetric Warfare Group: *Russian New Generation Warfare Handbook*. Version 1, 2016. 17.

repülőgépet (*unmanned aerial vehicle*, UAV) alkalmaz, és az orosz erők a mobil kommunikációs hálózatok megzavarására használták Ukrajnában.[13]

Az ukrán biztonsági erők által a válság korai szakaszában használt harcászati rádiók különösen veszélyeztetettek voltak az orosz elektronikai támadási rendszerekkel szemben. Ukrajna azonban azóta átállt a zavarásnak ellenállóbb, frekvenciaugratásos Harris rádiókra. Ezek a tulajdonságok arra kényszeríthetik a szemben álló felet, hogy új technikákat alkalmazzon, sokkal közelebb vonva őket a harcérintkezés vonalához, ezáltal kiszolgáltatottabbá téve rendszereit az ellentámadással szemben.

Oroszország az ukrán pilóta nélküli légi hírszerző, megfigyelő és felderítő (*intelligence, surveillance and reconnaissance,* ISR) platformokat is megcélozta. Csak 2015 és 2017 között az ukrán biztonsági erők közel 100 UAV-ot veszítettek az orosz GNSS zavaró technikák miatt, ami rontotta az időbeli kritikus hírszerzés képességét az orosz erőkkel kapcsolatban.[14]

Oroszország passzív elektronikai támogatással (*electronic support measures,* ESM) folytatott műveleteket, és rádiófelderítő rendszereket használt az információ összegyűjtésére és a szituációs helyzetkép megszerzésére az ukrán harcászati rádiók, személyi mobil eszközök és radarrendszerek jeleinek felderítésével. Az orosz SIGINT (*signal intelligence,* vagy сигнальная разведка) tevékenységek különösen hatékonyak voltak az ukrán erők által használt, régi titkosítás nélküli kommunikációs eszközök felderítésére.[15] Továbbá Oroszország aktív elektronikai érzékelő képességeket is felhasznált a régió ukrán erőinek megfigyelésére.[16]

A helyzetismeret megszerzése mellett Oroszország az РЭБ-rendszereket is felhasználta az ukrán erők precíziós célmegjelölésére. A kommunikációs zavarások időszakában az, hogy nem képesek a régi harcászati rádiókat használni, arra kényszerítette az ukrán katonákat, hogy személyes mobileszközeiket használják. Ezt az orosz hadsereg kihasználta, mivel könnyedén hozzáfért a mobilok geolokációs adataihoz, ezzel segítve a tűzvezetés precizitását.[17]

Összegezve, a Leer-3 rendszer részeként működő orosz Orlan-10 UAV-okhoz tervezett SIGINT-művelet során az orosz csapatok képesek voltak a bázisállomásokról származó adatok elfogására, hozzáférést biztosítva a mobileszközök geolokációjához, és ezt a helyinformációt megoszthatták más erőkkel. Következésképpen a rejtett célpontú földrajzi helymeghatározási képességek és a tüzérség integrációja meghatározó előnyt biztosított az orosz erőknek az ukrán szárazföldi erőkkel szemben.

[13] Duncan McCrory,: Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States. *The RUSI Journal,* 165. (2020), 7. 34–44.

[14] Joseph Trevithick: Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus". *The Drive,* 2019. október 30.

[15] Yuir Lapaiev: Ukraine as Clandestine Testing Ground for Russian Electronic Warfare. *Eurasia Daily Monitor,* 15. (2018), 157.

[16] Patrick Tucker: Exclusive: US Intelligence Officials and Satellite Photos Detail Russian Military Buildup on Crimea. *Defense One,* 2019. június 12.

[17] McCrory (2020): i. m.

4. Hogyan támogatták a rádióelektronikai harc eszközei az információs és kiberműveleteket az ukrán válság során?

Az orosz kormányzati és tudományos körökben az információ a nagyhatalom formájának és forrásának tekinthető. Ez igaz volt jóval az internet és a kibertér megjelenése előtt – ami nem változtatta meg az orosz információs háború stratégiáját, hanem csak annak taktikáját.[18]

Ennek az orosz perspektívának a logikus következménye az orosz „információs tér" (информационное пространство) határainak meghatározása és védelme, és ez a filozófia könnyen megtalálható az orosz doktrínákban, stratégiákban és tevékenységekben – például az ukrán konfliktus során végzett műveletekben is. Viszont az orosz perspektívának nincs meghatározása az információs, illetve kiberműveletekre, sokkal inkább csinálják, mint beszélnek róla.

Az orosz szóhasználatok (információs tér és információbiztonság kibertér és kiberbiztonság helyett) tökéletesen rámutatnak arra az összefüggésre, hogy az információs tér egy mindent lefedő műveleti tartomány, amelyben eszközként használhatók a rádióelektronikai harc eszközei, és magában foglalja a kiberteret, valamint a kibertérben zajló műveleteket.

Ennek eredménye az, hogy nem csupán támogató funkcióként értelmezik az információs és kibertérműveleteket, hanem egyenrangú műveletekként.[19]

Ezért teljesen természetes, hogy Oroszország információs műveleteket alkalmazott Ukrajnában: az „Euromaidan" tüntetések kezdetétől a Krím annektálásáig és a kelet-ukrajnai hadműveletek dimenziójaként. És az sem meglepő, hogy az internet korszakában Moszkva hatékony taktikát dolgozott ki az információs hadviselés virtuális térben történő alkalmazására.[20]

Oroszország 2020-as nemzetbiztonsági stratégiája kimondja, hogy a „nacionalista, szeparatista, radikális vallások" veszélyt jelentenek a nemzetállamokra, és hogy most fokozódik a „globális információs harc". A dokumentum ennek a fenyegetésnek az ellensúlyozását javasolja az „igaz" információk terjesztését az orosz állampolgárok számára, többek között a közösségi médiát felölelő natív internetes platformok népszerűsítésével.[21]

Ami a kibertér (orosz felfogás szempontjából információs tér) fontosságát illeti, számos hivatalos dokumentum írja le a számítógépes hálózati műveleteket az orosz információbiztonság szerves részeként, többek között: az Orosz Föderáció információbiztonsági doktrínája, az Orosz Föderáció fegyveres erőinek információs térben végzett tevékenységével kapcsolatos koncepcionális nézetek és az Orosz Föderáció állampolitikájának alapelvei a nemzetközi információbiztonság területén.

[18] Margarita Levin Jaitner: Russian Information Warfare: Lessons from Ukraine. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, NATO CCD COE, 2015. 87–94.
[19] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus. 2018. 198.
[20] Jaitner (2015): i. m. 87–94.
[21] Az Orosz Föderáció Biztonsági Tanácsa. Стратегия национальной безопасности Российской Федерации до 2020 года. (Orosz Nemzeti Biztonsági Stratégia 2020).

Oroszországban a kiberbiztonság az információbiztonságnak van alárendelve, amely lehetővé teszi a nemzetbiztonsági tervezők számára, hogy mind a műszaki, mind a kognitív adatokat felügyeljék.

A konfliktusok tendenciája azt mutatja, hogy a polgári kommunikációs technológiának egyre nagyobb hatása van a konfliktusokban, és hogy az alacsony technológiájú, rögtönzött rendszerek ugyanolyan hatékonynak bizonyulnak, mint a csúcstechnológiájú katonai megfelelői. A kereskedelmi kommunikációs technológia konfliktusokban való elterjedésével és a katonai felszerelések nem állami szereplők általi használatával az РЭБ-nek egyre többféle fenyegetéssel kell szembenéznie, a legkülönfélébb technológiai szintektől. Az információs és kommunikációs technológiák konvergenciája a hadviselés formái határainak elmosódását eredményezi, ami nagyobb lehetőségeket és igényt kínál az РЭБ számára az információs térrel való együttműködésre.

Előfordulhat, hogy az РЭБ eszközeinek támogatnia kell a biztonsági műveleteket, továbbfejlesztett képességeket biztosítva számukra a mobiltelefonok és egyéb eszközök nyomon követésére, vagy más fenyegetések elleni védelemre. Új РЭБ-technológiákat fejlesztenek és a meglévő rendszereket adaptálják annak érdekében, hogy ellenintézkedéseket hozzanak egy kiszámíthatatlan világban, ahol a konfliktusok egyik napról a másikra változhatnak.[22]

Az orosz hadseregen belüli kutatók közötti diszkurzus is arra a következtetésre jutott, hogy a számítástechnika terén elért haladás a hadviselés új generációját hozta el, amelynek lényege a kibertérben elérendő abszolút információs fölény.[23] Nevezetesen: bármely kívánt befolyásolási zónán belül idetartoznak a technikai adatok és a kognitív információk, valamint a pszichológiai műveletek elleni támadás és védekezés egyaránt.

Ivan Vorobjev vezérőrnagy és Valerij Kiselyov ezredes azt írta, hogy az információ „nemcsak a tűzerő, a támadás, a manőver kiegészítője, hanem mindezeket átalakítja és egyesíti".[24] Szergej Csekinov ezredes és Szergej Bogdanov altábornagy még ennél is tovább megy: „Ma az információs befolyás eszközei olyan tökéletesre lettek fejlesztve, hogy stratégiai feladatokat tudnak megoldani."[25]

Oroszország az ukrajnai válság során átfogó információs műveleti kampányt folytatott és folytat a közvélemény befolyásolásának és az információs tér megzavarásának érdekében. Az orosz információs műveletek egyértelmű célja volt, hogy befolyásolja, összezavarja és demoralizálja az állampolgárokat, narratívájában gyakran keveredtek az igaz és hamis információk, hogy elfogadhatónak tűnjenek és illeszkedjenek a „közönség" korábban létező világképéhez.

Oroszország jelentős erőfeszítéseket tett e kampány érdekében: a *Bellingcat* jelentése szerint az orosz trollok mintegy 65 ezer tweetet tettek közzé nagyjából 24 órával a Malaysia Airlines MH-17 lelövése után, Ukrajnát okolva a tragédiáért.[26]

[22] B. Van Niekerk – M. Maharaj: The Future Roles of Electronic Warfare in the Information Warfare Spectrum. *Journal of Information Warfare,* 8. (2009), 3. 1–13.
[23] Jaitner (2015): i. m. 88.
[24] I. Vorobyov – V. Kiseljov: Russian Military Theory: Past and Present. *Military Thought,* (2013), 3.
[25] Sergei G. Checkinov – Sergei A. Bogdanov: Asymmetrical Actions to Maintain Russia's Military Security. *Military Thought,* (2010), 1.
[26] Bellingcat Podcast: *MH-17, Episode 2 Guide: A Pack of Lies* (2019. július 24.).

A Krím annektálása során az orosz erők kilenc ukrán tévécsatornát kapcsoltak le a krími műsorszóró állomásokon, továbbá az ukrán csatornákat az orosz tévéadások váltották fel Donyeckben. Az orosz propaganda példái közé tartoznak azok a nyilatkozatok, miszerint a Krímben élő orosz etnikai lakosságot súlyos ultranacionalista fenyegetés érte, és tagadták, hogy Oroszország részt venne a krími eseményekben.[27]

Másrészről Oroszország РЭБ-eszközökkel is támogatta az információs műveleteit. Az ukrán hadügyminisztérium jelentései szerint Oroszország a Leer-3 rendszert használta az ukrán katonák demoralizálásának megkísérléséhez, fenyegető szöveges üzenetek küldésével közvetlenül személyes mobileszközeikre.[28]

Az orosz támadó kibertérműveletek Ukrajnában magukban foglalják a kémkedést, az információs műveletek támogatását és a fizikai hatások kiváltását is. Egy ilyen jellegű kampánynak az a célja, hogy széles körű zavart okozzon, információs előnyt szerezzen és demoralizálja az ukrán biztonsági erőket. Ez magában foglalja az elosztott túlterheléses támadásokat, a kormányzati weboldalak elérésének ellehetetlenítését, a mobilhálózatok megzavarását, a kormány szavazatszámláló rendszerébe való beavatkozást és az idegen zászló alatti műveleteket. Az ilyen jellegű műveletek együttesen támadják a kibertér három rétegét: a fizikai, a logikai és a kiberszemélyiség réteget.

Az ukrán hadügyminisztérium jelentése szerint az orosz erők képesek voltak távolról letiltani az orosz gyártmányú harcászati rádiókat, amelyeket az ukrán biztonsági erők használtak 2015-ben. Ezt úgy érték el, hogy a kibertéren keresztül kiiktatták a beágyazott hibamentes funkciókat.[29]

A fentin kívül a GRU, az orosz katonai hírszerző ügynökség állítólag számos más offenzív kibertérműveletet is szervezett Ukrajnában. Ez magában foglalta a 2015-ös nagy intenzitású, összehangolt támadásokat is, amelyek tönkretették a kormányzati információs rendszerek adatait, letiltották az ATM-eket és megzavarták a közlekedési rendszereket. Ennek csúcspontja volt az a nyilvánosan dokumentált számítógépes támadás egy elektronikai hálózat ellen, 2015. december 23-án, amelynek következtében áramkimaradás következett be,[30] mintegy 225 000 ukránt érintve.[31]

Ugyanakkor, az oroszok által vezetett információs műveletek Ukrajnában jóval a tárgyalt konfliktus előtt megkezdődtek. Az ukrán biztonsági szolgálat (SBU) figyelmeztetést adott ki, hogy a kormányzati szervereket és tisztviselőinek számítógépeit 2010 óta orosz kémkedésre szánt kártevők (különböző nevén „Snake", „Uroboros" vagy „Turla") célozták meg.[32]

Checkinov és Bogdanov rámutatnak – a Krím annektálása és Ukrajna jelenlegi destabilizálása következtében –, hogy az információk felhasználhatók a kormányzat

[27] Michael Kofman et al.: *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Santa Monica, CA, RAND Corporation, 2017. 13.

[28] Borys Krementskyi: Hybrid Warfare in Ukraine EW Domain. 2019. szeptember 12. 20.

[29] Trevithick (2019): i. m.

[30] DDOS támadás az áramellátó ellen az Ivano-Frankovszki körzetben. Pontosan egy évre rá, ugyanezzel a módszerrel, ugyanez megtörtént Kijev egyik északi kerületében, és párhuzamosan kiiktatták a nemzeti légitársaság (MAU) jegyeladási rendszerét.

[31] David E. Whitehead et al.: *Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies*. Power and Energy Automation Conference, Washington, 2017. március 21–23.

[32] InfoSecurity Magazine: *Snake Cyber-espionage Campaign Targetting Ukraine is Linked to Russia* (2014. március 14.).

dezorganizálására, a kormányellenes tüntetések megszervezésére, az ellenfelek megtévesztésére, a közvélemény befolyásolására és az ellenfél ellenállási akaratának csökkentésére. Továbbá kritikus fontosságú, hogy az ilyen tevékenységek a hagyományos katonai műveletek előtt megkezdődjenek.[33]

A fent említett kutatók ugyanakkor nem veszik figyelembe azt a kritikát, miszerint különbséget kell tenni a technikai és a kognitív adatok elleni támadások között. Az Orosz Föderáció következő nemzetbiztonsági stratégiájának tervezete is problematizálja a nyugati és orosz definíciós különbségeket.

5. Következtetések

A sikeres felderítés stratégiai hatással lehet. Háborús körülmények között közvetlenül kapcsolódhat az információs fölény megszerzésének vágyához a harctéren, és néha könnyen társítható a folyamatban lévő katonai műveletekhez.

A hadviselés során mindig szoros kapcsolat állt fenn az információs műveletek és a hagyományos katonai műveletek között. Krímben az események teljes menetét – a parlament átvételétől a vitatott népszavazásig és a Krím orosz annektálásáig – az információáramlás ellenőrzésének kifinomult módszertana támogatta. Az orosz műveletek kiterjedtek a kommunikáció teljes spektrumára mind a kinetikus, mind az információs térben (és kibertérben).

Oroszország magas szintű jártasságot mutatott az РЭБ, a kiber- és információs műveletek szinergikus alkalmazásában. Ez az elemzés Ukrajnára összpontosított, kiemelve Oroszország e több területre kiterjedő képességeinek alkalmazását az ukrán erőkkel kapcsolatos hírszerzéshez, a navigációs és kommunikációs rendszerek befolyásolásához, az ukrán katonák közvetlen támadásához a mobil hírközlés rejtett földrajzi elhelyezkedése révén, a kritikus nemzeti infrastruktúra letiltásához és a társadalmi és politikai kohézió aláásásához.

Ezeket a komplex, több területet átfogó képességeket, amelyek Oroszországnak meghatározó katonai előnyt biztosítottak az ukrajnai válság idején, később Szíriában továbbfejlesztették, és jelenleg is továbbfejlesztik aszimmetrikus válaszként a kifinomult nyugati katonai képességekre.

Felhasznált irodalom

Bellingcat Podcast: *MH-17, Episode 2 Guide: A Pack of Lies* (2019. július 24.). Online: www.bellingcat.com/resources/podcasts/2019/07/24/bellingcat-podcast-mh17-episode-2-guide-a-pack-of-lies/

Checkinov, Sergei G. – Sergei A. Bogdanov: Asymmetrical Actions to Maintain Russia's Military Security. *Military Thought,* (2010), 1.

[33] Sergei G. Checkinov – Sergei A. Bogdanov: The Art of War in the Early 21st Century: Issues and Opinions. *Military Thought,* 24. (2015), 11. 26–38.

Checkinov, Sergei G. – Sergei A. Bogdanov: 'The Art of War in the Early 21st Century: Issues and Opinions. *Military Thought,* 24. (2015), 11. 26–38.
Darczewska, Jolanta: Russia's Armed Forces on the Information War Front, Strategic Documents. *OSW Studies (Center for Eastern Studies),* (2016), 57. 1–50. Online: www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf
Dévai Dóra: An Overview of the Development of the Russian Information Warfare Concept: Part 2. *Hadtudományi Szemle,* 13. (2020), 2. 5–12. Online: https://doi.org/10.32563/hsz.2020.2.1
Guzenko, V. F. – A. L. Moraresku: *Radioelektronnaia borba. Sovremennoe soderzhanie. Tematicheskiy Sbornik. Radioelektronnaia borba v vooruzhennykh silakh Rossiiskoi Federatsii.* Informatsionnyi Most, Moszkva, 2017. 14–15.
Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.
Infosecurity Magazine: *Snake Cyber-Espionage Campaign Targetting Ukraine is Linked to Russia* (2014. március 11.). Online: www.infosecurity-magazine.com/news/snake-cyber-espionage-campaign-targetting-ukraine/
Jaitner, Margarita: Russian Information Warfare: Lessons from Ukraine. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, NATO CCD COE, 2015. 87–94.
Krementskyi, Borys: *Hybrid Warfare in Ukraine EW Domain.* 2019. szeptember 12. Online: www.dsei.co.uk/__media/libraries/global-theatre/Borys-KREMENETSKYI.pdf
Kofman, Michael– Katya Migacheva – Brian Nichiporuk – Andrew Radin – Olesya Tkacheva – Jenny Oberholtzer: *Lessons from Russia's Operations in Crimea and Eastern Ukraine.* Santa Monica, CA, RAND Corporation, 2017. Online: https://doi.org/10.7249/RR1498
Kovács László. Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232. Online: https://doi.org/10.32567/hm.2017.1.17
Lapaiev, Yuir: Ukraine as Clandestine Testing Ground for Russian Electronic Warfare. *Eurasia Daily Monitor,* 15. (2018), 157. Online: https://jamestown.org/program/ukraine-as-clandestine-testing-ground-for-russian-electronic-warfare/
Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás. MH Vezetési és Doktrinális Központ, 2012.
Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 2. kiadás. 2015.
McCrory, Duncan: Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States. *The RUSI Journal,* 165. (2020), 7. 34–44. Online: https://doi.org/10.1080/03071847.2021.1888654
McDermott, Roger N.: *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum.* Tallinn, International Centre for Defence and Security, 2017. Online: https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf
Military Encyclopaedia: Voennyi Entsiklopedicheskii Slovar. Moscow, Voennoe Izadatelstvo, 1984.
Naval Dictionary: Voenno-morskoi Slovar. Moscow, Voennoe Izadatelstvo, 1990.
Az Orosz Föderáció Biztonsági Tanácsa: Orosz Nemzeti Biztonsági Stratégia. 2021. Online: http://publication.pravo.gov.ru/Document/View/0001202107030001

Trevithick, Joseph: Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus". *The Drive,* 2019. október 30. Online: www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus

Tucker, Patrick: Exclusive: US Intelligence Officials and Satellite Photos Detail Russian Military Buildup on Crimea. *Defense One,* 2019. június 12. Online: www.defenseone.com/threats/2019/06/exclusive-satellite-photos-detail-russian-military-buildup-crimea/157642/

US Army Asymmetric Warfare Group: *Russian New Generation Warfare Handbook.* Version 1, 2016. Online: https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf

Van Niekerk, B. – M. Maharaj: The Future Roles of Electronic Warfare in the Information Warfare Spectrum. *Journal of Information Warfare,* 8. (2009), 3. 1–13. Online: www.jstor.org/stable/26486763

Vorobyov, I. – V. Kiseljov: Russian Military Theory: Past and Present. *Military Thought,* (2013), 3.

Whitehead, David E. – Kevin Owens – Dennis Gammel – Jess Smith: *Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies.* Power and Energy Automation Conference, Washington, 2017. március 21–23. Online: https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 113–132.
DOI: 10.32567/hm.2021.4.9

Krasznay Csaba,[1] Deák Veronika[2]

Adatbiztonsági informatikai alapismeretek átadásának vizsgálata egy szakirányú továbbképzés keretében

Evaluating the Basic Knowledge Transfer of Data Security in a Postgraduate Specialist Training Course

A közszolgálati kiberbiztonság fejlesztését célzó felsőoktatási képzés során elengedhetetlen az informatikai alapismeretek átadása a hallgatók számára.

Az ilyen típusú képzésekre jelentkező hallgatók jelentős része nem képzett informatikus, így esetükben nem feltételezhető a mélyebb műszaki, technikai, informatikai alapismeretek megléte. Egy ilyen típusú képzés kialakítása során figyelni kell arra, hogy a hallgatóság megértse és képes legyen feldolgozni, elsajátítani az átadott ismereteket.

Jelen tanulmány az informatikai alapismeretek átadásához egy már meglévő tantárgy tematikáját, az általa átadott ismeretanyag hatékonyságát, helyességét, az esetleges hiányosságait vizsgálja, és javaslatot fogalmaz meg, hogyan lehet azt a közszolgálati kiberbiztonsági képzésbe beilleszteni.

Kulcsszavak: **közszolgálat, kiberbiztonság, képzés, informatika, alapismeretek, készségek, képességek, tudásátadás, hatékonyság**

In case of a training programme which aims to improve cyber security in the public service it is required to transfer basic knowledge of information technologies to the attendees.

[1] Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézet, intézetvezető, egyetemi docens, e-mail: krasznay.csaba@uni-nke.hu

[2] Nemzeti Közszolgálati Egyetem adatvédelmi tisztviselő; Katonai Műszaki Doktori Iskola, doktori hallgató, e-mail: deak.veronika@uni-nke.hu

Generally, only a small part of the attendees on such training programmes are qualified computer science experts. Hence, we can assume that the rest of the students lack a deeper engineering and technical knowledge on this field. However, it is a challenging task to educate such students in a way they can understand and use the transferred knowledge.

In this paper, we evaluate the results of an existing course in the field of information technologies that can be a basis for a similar course in the cybersecurity training programme for public service. We investigate the effectiveness, correctness and insufficiency of the knowledge transfer. Finally, we propose improvements and changes to be able to integrate such courses into a cybersecurity training programme for public service.

Keywords: **public service, cybersecurity, training programme, computer science, skills, knowledge transfer, effectiveness**

1. Bevezetés

A közszolgálati kiberbiztonság fejlesztését célzó képzés során elengedhetetlen az informatikai alapismeretek átadása a hallgatók számára. Az elmúlt évek eseményei azt mutatják, hogy a közszolgálat a kibertámadások kedvező célpontjaként értelmezhető, így különösen nagy hangsúlyt kell fektetni a lehetséges támadási alternatívák megismerésére és alkalmazhatóságára a hatékony védelem kialakítása érdekében.

A közszolgálati kiberbiztonság kialakításához és folyamatos fejlesztéséhez elengedhetetlen a közszolgálatban dolgozó személyek kibervédelmi ismereteinek bővítése. Ezt célozza a közszolgálati kiberbiztonsági képzés,[3] amelynek megalkotása tudományos módszerek alapján történik. Ennek egyik fő feladata a képzéshez szükséges főbb alapismeretek feltérképezése és hatékony tudástranszfer bizonyítása.

A jelenlegi IT-szektorban jelentkező szakemberhiány indokolttá teszi a közszolgálat képzési programjának kidolgozását a kiberbiztonság fejlesztése érdekében. A közszolgálati kiberbiztonsági képzés alapvetően azoknak a közszolgálatban dolgozó, nem informatikai végzettségű személyeknek szól, akik nem rendelkeznek a szükséges kibervédelmi alapismeretekkel, nem mozognak a témában otthonosan, a cél, hogy megfelelő felkészítést kapjanak a hatékony és eredményes védelem kialakítása, a különféle kiberfenyegetések megelőzése, illetve a már bekövetkezett események elhárítása érdekében.

A kibervédelmi képesség kialakításához szükséges készségek, képességek meghatározásának részét képezi azon informatikai alapismeretek azonosítása, amelyek nélkülözhetetlenek a hatékony közszolgálati kiberbiztonság elérése érdekében. Az informatikai alapismeretek meghatározása egy, már folyamatban lévő, rokon területen megvalósított képzés keretében oktatott tantárgy hatékonyságának elemzésével

[3] Jelen tanulmánynak nem célja a közszolgálati kiberbiztonsági képzés részletes bemutatása.

történik, amelynek tematikája esetlegesen felhasználható a közszolgálati kiberbiztonsági képzéshez.

Ennek igazolására az alábbi hipotéziseket állítottuk fel:

H1. A tantárgy keretein belül hatékony volt a tudástranszfer.

H2. A tantárgy tematikája megfelelően fedi a szükséges informatikai alapismereteket.

H3. Definiálható egy szempontrendszer, amely alapján osztályozható, hogy a témakörök során átadott tudás kellően részletes-e.

H4. A tantárgy felhasználható a kiberbiztonsági képzés során.

1.1. Kutatási módszertan

A fentebb említett hipotézisek megválaszolására az alábbi módszereket használtuk fel.

A H1 hipotézis esetén minden témakör oktatása előtt és után a hallgatók tesztet töltöttek ki. A hatékonyságot pedig úgy definiáltuk az egyes témakörök esetén, hogy vettük az oktatás előtt és után mért helyes válaszok százalékos arányának különbségét:

$$hatékonyság_{témakör}[\%] = \left\{\frac{helyes\ válaszok_{témakör}^{oktatás\ után}}{összes\ teszt\ kérdés_{témakör}} - \frac{helyes\ válaszok_{témakör}^{oktatás\ előtt}}{összes\ teszt\ kérdés_{témakör}}\right\} \times 100 \quad (1)$$

A H2 hipotézis esetén azt vizsgáltuk, hogy az oktatott ismeretanyag elegendő-e a *NICE Cybersecurity Workforce Framework*[4]-ben meghatározott képességek elsajátítására és a *Certified Information Systems Security Professional* (CISSP) képesítés[5] megszerzésére. A NICE Frameworköt és a CISSP-képesítés tartalmát a 2. pontban részletesen kifejtjük.

A H3 hipotézis során olyan szempontrendszert kell definiálni, amely a H1-ben meghatározott hatékonyság alapján osztályozni tudja az egyes témaköröket az alábbiak tekintetében:

- mélyebb tudás átadása szükséges,
- a témakör kellően részletes,
- a témakör egyszerűsítése szükséges.

A H4 hipotézis igazolására a H1, H2 és H3 hipotézisek eredményét vesszük alapul. Amennyiben a vizsgált tantárgy felhasználható, bemutatjuk, hogy milyen változtatások szükségesek a közszolgálati kiberbiztonsági képzésbe történő integrálásához.

[4] A NICE Keretrendszer a NIST *(National Institute of Standards and Technology)* egy speciális kiadványa, amely a kiberbiztonsághoz kapcsolódó munkaköröket kategorizálja, valamint többek között kifejti és leírja a kiberbiztonsági munkakörök tartalmát és ezen munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket. Bővebb információ a következő weboldalon található: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[5] A *Certified Information Systems Security Professional* (CISSP, más néven minősített információs rendszer biztonsági szakember) képzése az informatikai rendszerek technikai kérdéseinek biztonsági vonatkozásairól szól. Bővebb információ a következő weboldalon található: www.isc2.org/Certifications/CISSP#

1.2. Struktúra

A második pontban bemutatjuk az előbbiekben említett NICE Framework és CISSP tartalmát, elemeit és a képzéshez fűződő kapcsolatát, valamint a kapcsolódó munkákat. A harmadik pontban a mérések körülményeit és az alkalmazott módszertant fejtjük ki. A negyedik pont tartalmazza a mérések eredményeinek általános és egyes témakörök szerinti áttekintését, valamint kiértékelését. Az ötödik pontban a témakörök osztályozását, az általunk definiált szempontrendszert, majd a hatodik pontban az eredmények alapján levonható következtetéseket ismertetjük, amelyet az utolsó pontban az összegzés, a jövőbeni tervek, a mérések lehetséges folytatása követ.

1.3. Előzetes következtetések

Meggyőződésünk, ha a bemutatott hipotéziseket megfelelően alá tudjuk támasztani, akkor az megfelelő alapot biztosíthat a közszolgálati kiberbiztonsági képzés és más képzések fejlesztéséhez kapcsolódóan.

2. Kapcsolódó munkák

Ahhoz, hogy a jelen tanulmányban ismertetett tudástranszfer hatékonyságmérés minden részletre kiterjedő értékelése megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata. A jelen mérés alapjául szolgáló célcsoport részére átadott tudás alapját képező képességek, készségek halmazát a hasonló képzések követelményeinek vizsgálatával határoztuk meg.

2.1. Hazai közigazgatásban végzett kutatások

Elsősorban olyan tanulmányokat elemzünk, amelyekben hasonló kutatást végeztek el, illetve a kiberbiztonsági képzésfejlesztés, a kiberbiztonsági és kibervédelmi képességek fejlesztését vizsgálják. Az irodalomkutatás során feltárt tanulmányok közül mindenképp ki kell emelni az Illésy Miklós, Nemeslaki András, Som Zoltán által elkészített *Elektronikus információbiztonság-tudatosság a magyar közigazgatásban* című publikációt. A szerzők a magyar közigazgatás információbiztonsággal kapcsolatos tudatosságát térképezték fel egy szakértői interjúsorozattal, illetve egy köztisztviselői kérdőíves megkérdezéssel, amelyet leíró statisztikai módszerekkel elemeztek.[6]

A tanulmányban részletezett interjúk megerősítették, hogy a rohamos technológiai fejlődéshez történő alkalmazkodást nagymértékben befolyásolhatja az információbiztonsággal kapcsolatos humánerőforrás-fejlesztés információbiztonsági vezetői és alkalmazotti szinteken egyaránt. A szerzők által elvégzett kérdőív kimutatta azokat

[6] Illésy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. *Információs Társadalom,* 14. (2014), 1. 52–73.

a területeket, amelyek alapján láthatóvá váltak az ellentmondások az információbiztonság-tudatosság megítélésében. A tanulmány tapasztalatai azt mutatják, hogy elengedhetetlen az információbiztonság-tudatosság folyamatos fejlesztése a kibertérből érkező fenyegetések megakadályozása, elhárítása érdekében.[7]

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.[8]

2.2. National Initiative for Cybersecurity Education (NICE) Framework

A hatékony és eredményes tudásátadás eléréséhez nem csak a hasonló méréseket szükséges vizsgálni, nélkülözhetetlen azon képességek, készségek meghatározása, amelyeket át szeretnénk adni a célcsoport számára. E halmaz megállapításához a korábbiakban említett National Initiative for Cybersecurity Education (NICE) Frameworkben részletezett ismereteket vettük alapul. A NICE Keretrendszer meghatározza az elsajátítandó kiberbiztonsági tudást, készségeket, képességeket és feladatokat az egyes kiberbiztonsággal kapcsolatos munkakörökhöz.[9] Ez a keretrendszer kiváló alapként szolgálhat az általunk átadni kívánt tudás, készségek, képességek meghatározására, a kiberbiztonsági tantervek, tantárgyi adatlapok kidolgozására.

A NICE kapcsán szükséges megemlíteni az ENISA[10] Európai Kiberbiztonsági Képességek Keretrendszerét,[11] amely definiálására és kidolgozására külön munkacsoportot hoztak létre 2020-ban. A keretrendszer célja a NICE Keretrendszerhez hasonlóan a kiberbiztonsággal összefüggő munkakörök és azok teljesítéséhez szükséges készségek, képességek azonosítása, amely szorosan igazodik az Európai Unió tagállamainak sajátosságaihoz, igényeihez.

2.3. A NICE Framework szerepe a nemzetközi oktatásban

A NICE Keretrendszerről és a kiberbiztonsági oktatás fontosságáról számos nemzetközi tanulmány tartalmaz megállapításokat, következtetéseket.

[7] Illésy (2014): i. m.

[8] Nagyné Takács Veronika – Kovács László: Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono – Magyar Közigazgatás,* 3. (2015), 4. 85–99.

[9] William Newhouse et al.: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology, 2017.

[10] *European Union Agency for Cybersecurity* (ENISA) – Európai Uniós Kiberbiztonsági Ügynökség.

[11] *European Cybersecurity Skills Framework* (bővebb információ a következő linken elérhető: www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework).

Alsmadi tanulmánya rámutat a jelenlegi kiberbiztonsági munkaerőhiány jelenségére, valamint kiemeli a NICE és az ehhez hasonló keretrendszerek alkalmazásának szerepét, továbbá azonosítja azon tényezőket, amelyek bizonyítják ezek szükségességét.[12] Armstrong és szerzőtársai szintén hangsúlyozzák a növekvő kiberbiztonsági munkaerőhiányt, ezáltal pedig a kiberbiztonsági munkaerő iránti kereslet és versengés megjelenését.[13]

Dodge és szerzőtársai kifejtik, hogy a kiberbiztonsági munkaerő fejlesztése elengedhetetlen, az ezek során felmerülő problémák, kihívások nem csak bizonyos országokban jelentkeznek, így figyelembe kell venni a globális hatásokat, következményeket.[14]

Andrew McGettrick rámutat, hogy már 2013-ban is egyértelmű volt, hogy a kiberbiztonsági oktatás több területet érint, mint például az akadémia, közigazgatás, egészségügy és a magánszféra. Ezért a hallgatókat motiválni kell annak érdekében, hogy felkeltsék az érdeklődésüket a kiberbiztonság iránt.[15]

Estes és szerzőtársai tanulmányukban feltárják, hogy a NICE kiberbiztonsági munkaerőrendszere hogyan igazítja és hangolja össze a kiberbiztonági munkákat a potenciális jelöltekkel. A keretrendszer segítséget nyújt a szervezeti kiberbiztonsági igények, illetve a személyes karriercélok és ezek eléréséhez szükséges eszközök meghatározásához is.[16]

Scheponik és szerzőtársai arra keresik a választ, hogyan értelmezik a hallgatók a kiberbiztonság egyes fogalmait, illetve hogy a kiválasztott egyetemeken tanuló hallgatók milyen kiberbiztonsági ismeretekkel rendelkeznek. A tanulmány célja interjúk elkészítésével a hallgatók tudásának mérése, a hiányosságok feltárása, azok okainak azonosítása, valamint hosszú távon az oktatás fejlesztése.[17]

Bicak és szerzőtársai kifejtik, hogyan változott meg a kiberbiztonsági képzések tanterve. Ennek keretében rövid áttekintést adnak a NICE Keretrendszerről és egyéb, például információbiztonsággal kapcsolatos programokról, illetve ezek követelményeiről. Ezt követően bemutatják, milyen változások figyelhetők meg a kiberbiztonsági oktatásban a tantervek tekintetében.[18]

Összegezve megállapítható, hogy a NICE Keretrendszeren alapuló egyetemi oktatás megfelelő szaktudást biztosít a kiberbiztonság témakörében. Azonban az is

[12] Izzat Alsmadi: Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA Journal,* 4. (2018), 1–6.

[13] Miriam E. Armstrong – 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.

[14] Ronald C Dodge – Costis Toregas – Lance Hoffman: Cybersecurity Workforce Development Directions. *HAISA,* (2012), 1–13.

[15] Andrew McGettrick: Toward Effective Cybersecurity Education. *IEEE Security & Privacy,* 11. (2013), 6. 66–68.

[16] Adriane C. Estes – Dan J. Kim – T. Andrew Yang: Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates. In *Proceedings of the 2018 International Conference on Frontiers in Education: Computer Science & Computer Engineering.* Las Vegas, Nevada, CSREA Press 2018. 1–7.

[17] Travis Scheponik et al.: How Students Reason about Cybersecurity Concepts. In *IEEE Frontiers in Education Conference* (FIE). 2016. 1–5.

[18] Ali Bicak – Michelle (Xiang) Liu – Diane Murphy: Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal,* 13. (2015), 3. 99–110.

látható, hogy a keretrendszer hatékony integrálása az egyetemi oktatásba nagyban függ a hallgatók kezdeti tudásának mértékétől.

2.4. Certified Information Systems Security Professional (CISSP) vizsga

A CISSP egy nemzetközi tanúsítvány az információbiztonság területén. A tanúsítvánnyal rendelkező információbiztonsági szakemberek képesek megérteni és alkalmazni a kiberbiztonsági stratégiákat, illetve kellően részletes szaktudással és gyakorlati ismeretekkel rendelkeznek, hogy képesek legyenek megtervezni és vezetni egy szervezeti egység teljes biztonsági struktúráját. A képzés nyolc fő témából áll, amelyeket minden jelöltnek el kell sajátítania.[19] Ezek az alábbiak:

- biztonsági kockázatok és kockázatkezelés;
- vagyon- és eszközbiztonság;
- biztonsági architektúra és tervezés;
- kommunikáció és hálózati biztonság;
- identitás és hozzáférés-kezelés;
- biztonsági értékelés és tesztelés;
- biztonsági műveletek;
- szoftverfejlesztési biztonság.

A CISSP-képesítés megszerzéséhez számos követelmény teljesítése szükséges. A jelölteknek legalább ötéves szakmai tapasztalattal kell rendelkezniük a fentebb említett témakörökből minimum kettő vagy több témát érintően. Amennyiben a jelölt négyéves főiskolai végzettséggel vagy azzal egyenértékű regionális tanúsítvánnyal, illetve kiegészítő tanúsítvánnyal rendelkezik az ISC által jóváhagyott listáról, akkor azt egyéves munkatapasztalatként ismerik el. A vizsgával kapcsolatos főbb információk az alábbi táblázatban láthatók:

1. táblázat
CISSP-vizsga adatai
Forrás: (ISC)² (2018): i. m.

A vizsga időtartama	3 óra
Kérdések száma	10–150
Kérdések formátuma	Feleletválasztós és kifejtős
Minimum pontszám	700 (1000-ből)
Vizsga nyelve	Angol
Vizsgaközpont	ISC által engedélyezett vizsgaközpontok

[19] (ISC)²: Certification Exam Outline (2018. április).

2.5. Pedagógiai értékelések

Több hazai egyetemen is megtalálható az oktatók értékelési rendszere, ezáltal megvalósíthatóvá válik az oktatók minőségellenőrzése, többek között a Nemzeti Közszolgálati Egyetemen, a Budapesti Műszaki Egyetemen, valamint az Óbudai Egyetemen. Nemzetközi szinten is gyakran alkalmazzák ezen értékelési módszereket. Samian és Noor is bemutatnak cikkükben egy ilyen hallgatói benyomásokon alapuló értékelési rendszert. A visszacsatolást minden félévben elvégezik az egyetem összes kurzusán. A hallgatóknak a félév végén több hét áll rendelkezésükre, hogy az általuk elvégzett kurzusokat és azok előadóit értékeljék. Ezt követi a kiértékelés, valamint a felsővezetés és az oktatók általi megismerés.[20]

Kumaladewi és Sugiarti tanulmányukban bemutatott módszer segítségével a hallgatók visszajelzésén keresztül megkapott adatok alapján nemcsak egyszerű méréseket képesek végrehajtani, hanem stratégiai döntéseket és előrejelzéseket is.[21]

Falusi Iván és társai definiálják a tantervi vagy programértékelést mint kutatási módszert, aminek célja, hogy egy adott tanterv, taneszközegyüttes stb. hatékonyságát a saját maga elé tűzött célok elérése szempontjából értékelje.[22]

Összegezve kijelenthető, hogy a pedagógiai-statisztikai szakirodalom elsősorban statikus ellenőrzéseket használ a tantervek és programok fejlesztésére (például a követelmények teljesülnek-e), illetve az oktatók teljesítményértékelése határozza meg a tudásátadás minőségét a hallgatók szubjektív benyomásai, érzései alapján. Kijelenthető, hogy olyan módszertant a szakirodalom ezidáig nem definiált, amely a tudásátadás hatékonyságát objektív módon mérné és biztosítaná egy tantárgy fejlesztésének lehetőségét.

3. A NICE, a CISSP és az oktatási anyag kapcsolata

Az oktatási anyag kidolgozása során a NICE Framework keretrendszer kiberbiztonsági pozíciói közül az adatvédelmi tisztviselő munkakört választottuk ki, amely tartalmazza mindazon tudást, képességeket és készségeket, ami a leginkább illeszkedik a célcsoport előképzettségéhez, a tantárgy kimeneti követelményeihez, valamint az általuk megszerezhető szakképzettséghez. Ezt követően megvizsgáltuk a keretrendszer által előírt tudás, feladat, képesség és készség halmazát, és kiválasztottuk azokat, amelyek az általunk átadni kívánt tudás és a tantárgy kimeneti követelményei szempontjából relevánsak.

Ezek alapján az alábbi, 2. táblázat tartalmazza e feladatokat, tudást, képességeket és készségeket:

[20] Yahya Samian – Norah Md Noor Student's Perception on Good Lecturer based on Lecturer Performance Assessment. *Procedia-Social and Behavioral Sciences,* 56. (2012), 8. 783–790.

[21] Nia Kumaladewi – Yuni Sugiarti: Design Analysis of Data Warehouse for Lecturer Performance Evaluation (Case study: Faculty of science and technology UIN Jakarta). In 4*th* International Conference on Cyber and IT Service Management. 2016. 1–6.

[22] Falus Iván (szerk.): *Bevezetés a pedagógiai kutatás módszereibe.* Budapest, Keraban, 1996.

2. táblázat

Az átadni kívánt tudás és a vizsgált tantárgy kimeneti követelményei szempontjából releváns elvárások
Forrás: a szerző szerkesztése a NICE Keretrendszer alapján

Tudás
• számítógép-hálózatokhoz kapcsolódó alapfogalmak ismerete • kockázatkezelési folyamatok ismerete • kiberbiztonsági, adatvédelmi alapelvek ismerete • az alkalmazandó üzleti folyamatok működésének ismerete • kibertérből érkező fenyegetések ismerete • vezeték nélküli technológiák ismerete
Feladat
• tanácsadás a felsővezetésnek a kockázatértékelési folyamatról, kockázati szintekről, az információbiztonsági programokról, rendszerekről, irányelvekről, folyamatokról és eljárási szabályokról • üzletmenet-folytonossági tervek elkészítése, tesztek elvégzése • belső audit végrehajtása, auditjelentések elkészítése • közvetítés a műszaki és nem műszaki szakemberek között • adatbiztonsági követelmények megvalósulásának biztosítása • együttműködés az informatikai, információbiztonsági politikák és eljárások területén • közreműködés az információs infrastruktúra kialakításában, fejlesztésében • incidenskezelési folyamat kialakítása, incidensek kezelése • figyelemmel kíséri a szervezet folyamatait, az infokommunikációs rendszerek fejlesztését, működését a biztonsági és az adatvédelmi szabályok betartásának ellenőrzése céljából • adatvédelmi események, incidensek, jogsértések kezelése, dokumentálása, intézkedési terv készítése és megvalósítása
Képesség
• egyértelmű, világos, átlátható stratégia, iránymutatások, szabályok, eljárások, folyamatok és képzési anyagok, dokumentációk kidolgozásának képessége • szabványos működési eljárások, folyamatok kidolgozásának és folyamatos fejlesztésének képessége • a releváns adatvédelmi, kiberbiztonsági jogszabályok, technológiák változásának nyomon követésének képessége
Készség
• adatvédelmi szabályok, irányelvek készítésének készsége • adatvédelmi eljárások, folyamatok, gyakorlatok kialakításának készsége • különböző szintű kommunikációs készség a szervezet különböző területeinek megfelelően

A NICE Keretrendszerből kiválasztott tudás-, képesség-, készséghalmazt az általunk szükségesnek ítélt további elvárásokkal kiegészítve összeállítottuk azon elvárásokat, amelyek jelen tanulmányban vizsgált tantárgy szempontjától relevánsak, és ez alapján készítettük el a vizsgált félév tananyagát. Mindezt annak fényében, hogy a félév végi vizsgán a hallgatók meg tudnak-e olyan tipikus vizsgakérdéseket oldani, amelyek a CISSP-képesítés mintafeladatai között szerepelnek.

A CISSP-képesítésre több okból esett a választás. Először is, nevesítve szerepel a magyarországi információbiztonsági jogszabály oktatással kapcsolatos végrehajtási rendeletében. A 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének

és továbbképzésének tartalmáról 7. § (2) szerint: „Az Ibtv. 13. § (10) bekezdése alapján nem kell a 4. § (1) bekezdése szerinti végzettséget megszereznie annak a személynek, aki rendelkezik: […] *b)* az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP) érvényes oklevéllel." Másrészt az irodalomkutatás alapján a CISSP-vizsga tudásanyaga jól illeszkedik a NICE Keretrendszer elvárásaihoz.

Összegezve, a releváns szakirodalom és a kapcsolódó munkák mélyebb vizsgálata elengedhetetlen az átadni kívánt tudás meghatározásához, ennek következtében pedig a tudástranszfer méréséhez egyaránt, hiszen a hazai és nemzetközi oktatásban megjelenő kiberbiztonsággal kapcsolatos képzések, képességfejlesztést célzó tréningek elemzésével feltárhatók azok tapasztalatai, valamint azon „jó gyakorlatok", amelyek a hazai kiberbiztonsági oktatásba történő átültetésével jelentősen növelhető azok hatékonysága és eredményessége.

4. Mérési körülmények, módszertan

Jelen fejezetben szeretnénk prezentálni a mérésekhez kapcsolódó körülményeket, a mérés lefolytatásának jellemzőit, illetve módszertanát. A fejezet végén bemutatjuk a mérési eredményeket befolyásoló tényezőket is.

4.1. A tárgy jellegzetességei

A tantárgy során az adatvédelem és az adatbiztonság által meghatározott követelmények informatikai leképeződését kell elsajátítania a hallgatóknak. Itt kifejtik a következőket:

- számítógépes, hálózati és internetes biztonság;
- a védelem szintjei – fizikai védelem;
- a védelem szintjei – informatikai védelem;
- a biztonsági protokoll, a tűzfal és a biztonsági támadások;
- rendszergazdai irányelvek.

Ezenkívül a tantárgy segít megismertetni a hallgatókkal a kibertérből érkező fenyegetéseket és az információs társadalom új típusú kihívásait, valamint bemutatja az adatbiztonság összetevőit, a védelem lehetséges eszközeit, módszereit.

Jelen tantárgyat az Eötvös Lóránd Tudományegyetem Állam- és Jogtudományi Kar által szervezett Adatbiztonság és adatvédelmi szakjogász képzés második félévében tartották meg 6 kredit értékben,[23] kizárólag előadások formájában, gyakorlati oktatásra nem került sor. A tárgy teljesítése kollokvium keretében, tesztfeladatok megoldásával történik a félév végén. A mérést a 2018/19-es tanév tavaszi szemeszterében végeztük.

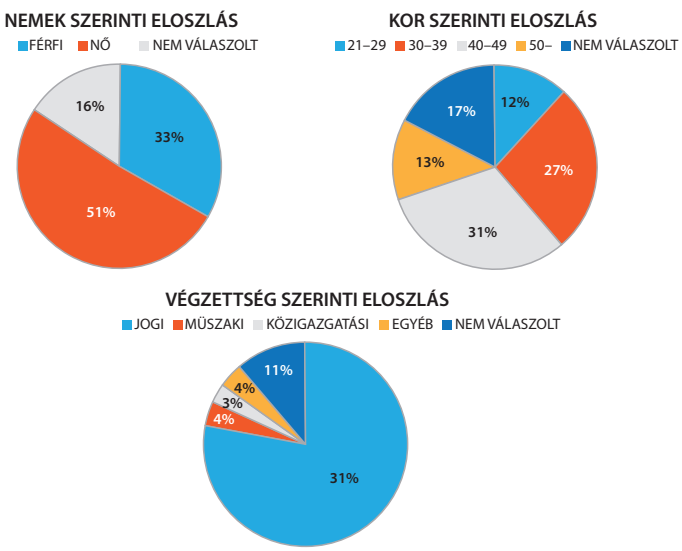
[23] A jelenlegi felsőoktatási rendszerben a kredit a tanulmányok elvégzése során alkalmazott mérőeszköz, amely a tantárgy súlyozására és típusának meghatározására szolgál.

4.2. A mérés körülményei

Az első előadás során egy átlagos információbiztonság-tudatosság mérésére szolgáló tesztet töltettünk ki a hallgatókkal. Ennek célja, hogy felmérjük a hallgatók általános biztonságtudatosságának szintjét, valamint a statisztikai kérdéseknek köszönhetően számos további következtetést határozzunk meg az egyes témakörök esetében. Ezt követően minden témakör oktatása előtt és után egy, a témára vonatkozó tesztet töltöttek ki. Témakörönként különböző kérdések, de a témakörök előtt és után azonos kérdéseket válaszoltak meg a hallgatók. A témakörökhöz kapcsolódó kérdések minden esetben szorosan illeszkedtek az előadáson elhangzott tananyaghoz. Tesztenként öt feleletválasztós kérdésre kellett válaszolniuk a hallgatóknak négy lehetséges opcióból a Kahoot alkalmazáson[24] keresztül. Ezek a kérdések a félév végén bekerültek a vizsgakérdések közé is, amelyet az egyetem Moodle rendszerén keresztül töltöttek ki.

4.3. A hallgatóság összetétele

A hallgatóság összetételét az első, általános információbiztonság-tudatosság mérésére szolgáló teszt alapján vizsgáltuk nem, kor és végzettség szerint, amelyek eloszlását az 1. ábra szemlélteti. A teszt kitöltése előtt a hallgatók beleegyezését kértük azzal kapcsolatban, hogy a félév során összegyűjtött adatokat anonim módon a kutatásban felhasználhassuk, ezzel teljesítve az adatvédelmi követelményeket.



1. ábra

A hallgatóság összetétele nem, kor, végzettség szerint

Forrás: a szerző szerkesztése

[24] A Kahoot kvízalapú oktatási platform, amely lehetővé teszi a hallgatók ismereteinek áttekintését, értékelését feleletválasztós kvíztesztek segítségével. Bővebb információ elérhető a következő weboldalon: https://kahoot.com/

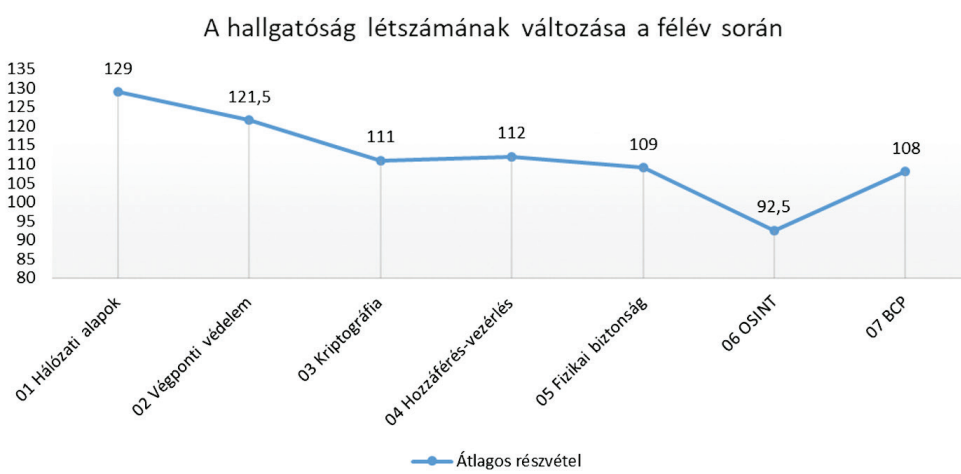
Összesen 130 hallgató töltötte ki a tesztet, 51%-uk nő (66 fő) és 33%-uk férfi (43 fő), a maradék 16% (21 fő) erre a kérdésre nem válaszolt. A nemek szerinti eloszlás alapján megállapítható, hogy a hallgatók többsége nő.

A kor szerinti eloszlás vizsgálatára négy életkori kategóriát állapítottunk meg. A hallgatók 12%-a (16 fő) 21–29 év közötti, 27%-a (35 fő) 30–39 év közötti, 31%-a (40 fő) 40–49 év közötti, 13%-a (17 fő) 50 éves vagy annál idősebb. Az életkorra vonatkozó kérdésre a hallgatók 17%-a, összesen 22 fő nem válaszolt. A kor szerinti eloszlás alapján a kérdésre válaszoló hallgatók többsége a 40–49 év közötti kategóriába tartozik.

A hallgatók végzettségének megállapítására szintén négy kategóriát határoztunk meg. A hallgatók 72%-a (102 fő) jogi, 4%-a (5 fő) műszaki, 3%-a (4 fő) közigazgatási és 4%-a (5 fő) valamilyen egyéb területen szerzett végzettséget. Erre a kérdésre a hallgatók 11%-a (14 fő) nem válaszolt. Ezek alapján megállapítható, hogy a hallgatók túlnyomó többsége jogi végzettséggel rendelkezik, de más előképzettséggel rendelkező hallgatók is részt vettek a képzésen.

4.4. A hallgatóság létszámának változása

A mérés eredményeinek érvényességét befolyásolta a tesztet kitöltő hallgatók létszáma az adott témakör előadásán. A 2. ábra a hallgatók létszámváltozását szemlélteti a félév során. Ezek alapján megállapítható, hogy kis mértékben, de folyamatosan csökkent a létszám. A hallgatói létszámcsökkenés számos okkal magyarázható, köszönhető többek között a féléves terhelésnek, a házi feladatok és zárthelyi dolgozatok gyakoriságának.



2. ábra

A hallgatóság létszámának változása a félév során

Forrás: a szerző szerkesztése

4.5. A kutatást befolyásoló tényezők

Jelen pontban szükséges megemlíteni a kutatás eredményét befolyásoló egyéb tényezőket. A kutatás során számos olyan tényező befolyásolta a kutatás lefolytatását és annak eredményét, amelyet mindenképp szükséges figyelembe venni a kutatás értékelésekor, a hipotézisek megválaszolásakor, illetve a következtetések megfogalmazásakor. Ezek alapján felmerülhet a kérdés, hogy milyen tényezők befolyásolhatták az eredményeket?

Az első ilyen tényező, hogy jelen kutatásban kizárólag egy évfolyamot vizsgáltunk, mivel korábbi évek statisztikái nem állnak rendelkezésre. Így csak ezen évfolyam tekintetében tudunk következtetéseket megfogalmazni. Jelen kutatásban ellenpéldát egyelőre még nem elemeztünk. Ennek következtében további megválaszolandó kérdések merülnek fel, például milyen eredmények születnének abban az esetben, ha nagyobb mennyiségű, illetve részletesebb ismeretanyagot adnának át a hallgatók számára.

Ezenkívül az eredmények kiértékelését nehezítette, valamint az elemezhető hallgatói eredmények számát csökkentette az a tény, hogy voltak olyan hallgatók, akik vagy az óra elején nem voltak még jelen, vagy pedig korábban távoztak az előadásról.

Továbbá meg kell még említeni mint befolyásoló, illetve nehezítő körülményt, hogy a negyedik hipotézisben említett kiberbiztonsági képzés esetén csak feltételezéssel élünk a hallgatók előképzettségének aránya tekintetében, illetve nem tudhatjuk, hogy az adott ismeretanyagot milyen mértékben képesek elsajátítani az egyes területekről érkező személyek, még hogyha a tudásuk azonos szinten is van az adott témában.

Ezek mellett érdemes megvizsgálni a továbblépési lehetőségeket is, a tananyag hosszú távú beépülésével kapcsolatban. Ezt a félévi vizsga útján lehet megtenni. A vizsgált szemeszterben a vizsgáztatás során lehetővé tettük, hogy a hallgatók egy 24 órás időintervallumban megnyithassanak egy Moodle-alapú tesztfelületet és ott egy előre megkonstruált kérdéssort tölthessenek ki. Ez 20 kérdésből állt, és összesen 30 perc állt rendelkezésre a kitöltéshez. A számonkérés megkönnyítése érdekében a teszt mindenkinek ugyanaz volt, de a feleletválasztós tesztek és ezeken belül a lehetséges megoldások véletlenszerűen keverve jelentek meg. A kérdések a CISSP-vizsga mintakérdései közül kerültek ki. Összesen 218 kitöltés született, átlagosan a 93,58%-os végső eredménnyel. A magas sikerrátában szerepe van annak, hogy a jó megoldásokat az évfolyamon belül a hallgatók megosztották egymással, de mivel módszertanilag jelen tanulmányban nem volt célunk objektív mérést végezni ezen a területen, pusztán a mérési módszertan lehetőségeit kívántuk kipróbálni, az eredmény nem befolyásolja megállapításainkat. További kutatásaink során azonban ezt a faktort is alaposabban tervezzük megvizsgálni.

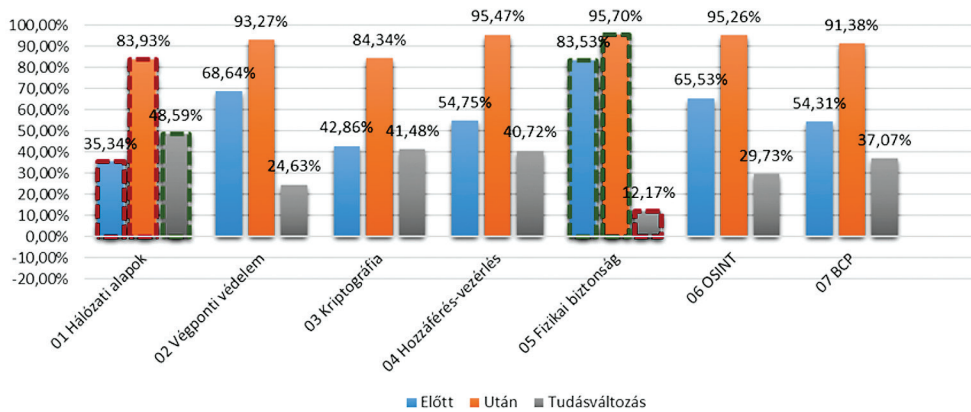
Összességében megállapítható, hogy a korábban említett befolyásoló tényezők ellenére is jelen kutatás megfelelő kiindulóalapot jelent a kiberbiztonsági képzés tantárgyi programjainak kidolgozásához.

5. Adatelemzés és a témakörök osztályozása

Jelen fejezetben bemutatjuk a hallgatók által kitöltött tesztek eredményeit, az azok alapján levonható következtetéseket, valamint az egyes témakörök előadásai során átadott tudás hallgatók általi elsajátítása alapján történő osztályozást.

5.1. Adatelemzés

Az egyes témakörök előtt és után kitöltött tesztek százalékos arányát, valamint az egyes témakörök tudástranszferjének hatékonyságát vizsgáltuk, aminek eredményeit a 3. ábra mutatja be.



3. ábra

Az egyes témakörök előtt és után mért összesített eredmények

Forrás: a szerző szerkesztése

A 3. ábra eredményeibe minden olyan hallgató válasza beleszámít, akik részt vettek a teszt kitöltésében, függetlenül attól, hogy kitöltötték-e az első órán megtartott általános kérdőívet.

1. témakör – Hálózati alapok

Az első témakör a *Hálózati alapok* címet viseli, amely összefoglalja és részletezi a számítógép-hálózatokhoz kapcsolódó alapfogalmakat, alapismereteket. A téma oktatása előtt egy öt kérdésből álló tesztet töltöttek ki, amelyre a hallgatók 35,34%-ban válaszoltak helyesen. Az óra végén ugyanazt a kérdéssort kapták a hallgatók, amely esetén már 83,93%-ban választották ki a megfelelő megoldásokat. Ezen téma esetében 48,59%-os tudásváltozás állt be, amely azt mutatja, hogy az órán elhangzottak

alkalmasak voltak tudásuk bővítésére. Jelen témakör esetében megállapítható, hogy az összes téma közül itt teljesítettek a legrosszabbul az oktatás előtti teszten a hallgatók (35,34%), és a tanítás utáni kérdéssorok esetében is (83,93%). Az összes témakörhöz viszonyítva ennek ellenére jelen témakörnél valósult meg a leghatékonyabb tudástranszfer, ugyanis a korábban említett 48,59%-os tudásváltozás a legmagasabb az összes témakör között.

2. témakör – Végponti védelem

A második, *Végponti védelem* című témakör a különféle kártékony programokat és az ezek elhárítására, megelőzésére szolgáló lehetséges alternatívákat, védelmi mechanizmusokat ismerteti. Ez esetben a tanítás előtti kérdéssorra 68,64%-os arányban érkeztek helyes válaszok, míg az előadás végén 93,27%-os arányban. A hallgatók tudásának változása az előadás előtthöz viszonyítva 24,63%-os volt.

3. témakör – Kriptográfia

A harmadik téma a *Kriptográfia* kérdéskörét öleli fel, amelyben kifejtették többek között a főbb alapfogalmakat, a kriptográfia történetét és módszereit, valamint az elektronikus aláírást is. Az oktatás előtti tesztre a hallgatók 42,86%-os arányban válaszoltak helyesen, az előadás végén pedig 84,34%-os arányban érkeztek helyes válaszok. A *Kriptográfia* téma esetében a tudásváltozás az összes téma tekintetében a második legmagasabb, 41,48%-os volt.

4. témakör – Hozzáférés-vezérlés

A negyedik témakör a *Hozzáférés-vezérlés* címet viseli, amely részletezi a kapcsolódó fogalmakat, elveket, a hozzáférés-ellenőrzés típusait, az esetleges védelmi intézkedéseket és a mobilbiztonság alapvető elemeit, lehetőségeit. Az előadás előtti kérdéssorra 54,75%-ban érkeztek helyes válaszok, míg a végén 95,47%-ban, amely a második legjobbnak értékelhető az összes témakör között. A hallgatók tudásváltozása 40,72%-os volt a két teszt között.

5. témakör – Fizikai biztonság

Az ötödik, *Fizikai biztonság* nevű témakör összefoglalja a fizikai biztonság alapjait, szükségességét, módszereit, a különféle információbiztonsági követelmények tartalmát, valamint a biztonsági technológiák és eszközök fontosságát és lehetőségeit. Az oktatás előtti tesztre 83,53%-ban, míg az oktatást követően 95,70%-os arányban érkeztek helyes válaszok. Az összes témakör közül a Fizikai biztonság esetén érkezett a legtöbb jó válasz a témáról tartott előadás előtt és után is, kifejezetten magas

értéket mutatott az előadás előtti teszt is, amelyből következik, hogy a tudásváltozás, a magas bemeneti értéknek köszönhetően jelen témánál volt a legalacsonyabb, mindössze 12,17%.

6. témakör – Nyílt forrású információszerzés (OSINT)

A hatodik téma az OSINT (*Open Source Intelligence* vagy más néven nyílt forrású információszerzés) kérdéskörét felölelő előadás, amely tartalmazza többek között az ehhez kapcsolódó alapismeretek, a lehetséges eszközök és módszerek, valamint a védelem alternatíváit is. Az előadás előtti teszten a hallgatók 65,53%-os arányban, míg az előadást követően 95,26%-os arányban válaszoltak helyesen. Ezek alapján megállapítható a hallgatók tudásváltozása, amely 29,73%-os arányú volt.

7. témakör –Üzletmenet-folytonossági terv (BCP)

A hetedik, vagyis az utolsó téma a BCP (*Business Continuity Plan*, más néven üzletmenet-folytonossági terv, amely magában foglalja az üzletmenet-folytonosság alapjait, az ehhez szükséges dokumentációkat és azok tartalmát. A témából tartott előadás megtartása előtt a hallgatók 54,31%-os arányban teljesítették jól a tesztet, míg az oktatást követően 91,38%-os arányban, ezek alapján a tudásuk változása 37,07%-os volt.

Összességében megállapítható, hogy minden témakör esetén megvalósult valamilyen szintű tudásátadás, átlagosan 33,48%-os tudásváltozás volt jellemző az oktatást követően, az oktatást megelőző tudásszinthez viszonyítva. Az ötödik, fizikai biztonság nevű téma esetében rendkívül alacsony (12,17%-os) volt a tudástranszfer, amelyből további következtetések vonhatók le. Általában, amennyiben a tudásváltozás alacsony, úgy mélyebb, részletesebb tudásátadásra van szükség, tehát ilyen esetekben az adott témakör ismereteinek mélyítése indokolt. A konkrét esetben azonban magas bázisról indult a teszt, azaz a hallgatók jól ismerték a fizikai biztonsággal kapcsolatos alaptéziseket, köszönhetően annak, hogy míg a kibertéri veszélyek a felmért csoport számára meglehetősen absztraktak, a fizikai tér kihívásait jól ismerik.

5.2. A témakörök osztályozása

A cél a korábban ismertetett NICE Keretrendszer általunk kiválasztott kiberbiztonsági munkakör esetén meghatározott követelmények hatékony átadása. Szükséges megvizsgálni minden témakör esetén, hogy a hallgatók e tudást maradéktalanul elsajátították-e. A témakörök előadásai után kitöltött teszek eredményei alapján a témakörök osztályozhatók aszerint, hogy a NICE Keretrendszerben rögzített ismereteket milyen mértékben sajátították el a hallgatók. Ehhez egy speciális szempontrendszert dolgoztunk ki. Ez azért elengedhetetlen, mert ennek segítségével megállapítható

minden egyes témakör tekintetében, hogy a továbbiakban szükséges-e mélyebb tudásátadás az előadásokon, kellően részletes-e az adott témakör, illetve indokolt-e a téma egyszerűsítése.

A témakörök csoportosításához az átadott tudás szintjét használjuk fel. Ezek alapján a következő csoportosítás alkalmazható:

- 90% felett: Kiváló
- 80%–90%: Jó
- 70%–80%: Közepes
- 60%–70%: Elégséges
- 60% alatt: Nem megfelelő

A bemutatott témaköröket ez alapján az alábbi csoportokba lehet helyezni:

- 1. témakör – Hálózati alapok: Jó
- 2. témakör – Végponti védelem: Kiváló
- 3. témakör – Kriptográfia: Jó
- 4. témakör – Hozzáférés-vezérlés: Kiváló
- 5. témakör – Fizikai biztonság: Kiváló
- 6. témakör – OSINT: Kiváló
- 7. témakör – BCP: Kiváló

E szempontrendszer és csoportosítás alapján megállapítható, hogy a célul kitűzött tudásmennyiséget szinte kiválóan sikerült átadni a hallgatók számára a tárgy keretében, hiszen a hét témakörből öt esetén 90% feletti eredményt értek el, és a maradék két témakör is jó „osztályzatot" ért el.

5.3. Következtetések

Ahhoz, hogy a tárgy keretében minden témakör kiváló minősítést kapjon, érdemes lenne a két „Jó" minősítéssel rendelkező témakört részletesebben oktatni, ami egyben azt is jelenti, hogy ezen előadások tekintetében az előadás hosszát, idejét növelni kell. Ennek következménye, hogy más témaköröknek az előadási idejét rövidíteni kell, célszerű azon témakörök előadásának hosszát csökkenteni, amelyek esetében a bemeneti tudás 80% feletti (például a fizikai biztonság témaköre, ahol a témakör előtti teszteredmények 83,53%-osak voltak).

A rosszabb eredményt elért témakörök esetén előfordulhat, hogy túl bonyolult volt a tananyag, ezért annak egyszerűsítése válik szükségessé.

További következtetések fogalmazhatók meg a „Kiváló" minősítéssel rendelkező témakörök esetében is. Ezen témakörök ismeretanyaga kellően részletes és megfelelően fedi a szükséges alapismereteket, így ezen előadások tartalmát tekintve további változtatási, módosítási teendő nincs. Kivételt képez ez alól a fentebb említett magas bemeneti értékű témakör, amely esetén a hallgatók alaptudása magas volt, így e témáknál lehetőség nyílik az előadások időtartamának rövidítésére a többi témakör javára.

6. Összefoglalás és következtetések

Tanulmányunkban definiáltuk a kibervédelmi képesség kialakításához szükséges készségek, képességek elsajátításához szükséges informatikai alapismeretek halmazát, amely nélkülözhetetlen a hatékony közszolgálati kiberbiztonság elérése érdekében. Az informatikai alapismeretek meghatározása egy, már folyamatban lévő rokon területen megvalósított képzés keretében oktatott tantárgy hatékonyságának elemzésével történt. A cél annak feltárása, hogy a vizsgált tantárgy tematikája esetlegesen felhasználható-e a közszolgálati kiberbiztonsági képzéshez.

Ennek megállapításához hipotéziseket fogalmaztunk meg, amelyek bizonyítására méréseket végeztünk a hallgatók már meglévő és az előadások segítségével elsajátított tudása tekintetében.

Ezenkívül felállítottunk egy szempontrendszert, amely segítségével osztályoztuk a témaköröket. A csoportosítás alapján javaslatokat fogalmaztunk meg az oktatás hatékonyságának fejlesztése, és a hallgatók által elsajátítható tudás növelésének elérése érdekében.

Az első hipotézisünkben azt vizsgáltuk, hogy a korábbiakban bemutatott tantárgy keretein belül hatékony volt-e a tudástranszfer. A hatékonyság fogalmát az első pontban, az 1. egyenlet segítségével definiáltuk. Ezek alapján a 4. pontban megvizsgáltuk az egyes tárgyak hatékonyságát (lásd 3. ábra), amely megmutatja, hogy minden témakör esetében hatékony volt a tudástranszfer. Ez alapján az első hipotézis igaznak bizonyult.

A második hipotézis esetében arra a kérdésre kerestük a választ, hogy a tantárgy tematikája alkalmas-e a szükséges informatikai alapismeretek elsajátítására, átadására. Az állítottuk, hogy a korábbiakban meghatározott ismeretanyag megfelelően fedi a szükséges informatikai alapismeretek halmazát, amely magában foglalja az általunk kiválasztott és 2. pontban ismertetett NICE Keretrendszerben rögzített adatvédelmi tisztviselő munkakör betöltéséhez elsajátítandó informatikai alapismereteket. Ezért jelen tantárgy a hipotézisben szereplő szükséges informatikai alapismeretek átadását maradéktalanul teljesíti. Továbbá extra témákat is érint (például OSINT), amely a kezdeti célokat túl is teljesíti.

A harmadik hipotézis esetében azt feltételeztük, hogy definiálható egy szempontrendszer, amely alapján osztályozható, hogy a témakörök során átadott tudás kellően részletes-e. A hipotézis bizonyításához a szempontrendszert az 5. pontban definiáltuk és fejtettük ki, amely alapján a témák megfelelően kategorizálhatók és osztályozhatók voltak. Ez alapján a harmadik hipotézis szintén igaznak bizonyul, hiszen a szempontrendszer segítségével megállapítható, hogy melyik témakört szükséges részletesebben oktatni, illetve melyhez szükségesek további előadások.

A negyedik hipotézis esetén azt vizsgáltuk, hogy az oktatott tantárgy felhasználható-e a kiberbiztonsági képzés során. E hipotézis igazolására az előző három hipotézis eredményét vesszük alapul. Az első hipotézis igaznak bizonyult, amely azt jelenti, hogy a tárgy keretén belül hatékony volt a tudástranszfer. Ezek alapján megállapítható, hogy az általunk elérni kívánt cél teljesült, a kiválasztott ismerethalmazt a hallgatók eredményesen sajátították el. A második hipotézisben bebizonyítottuk, hogy a tantárgy

tematikája és tananyaga megfelelően fedi a szükséges informatikai alapismereteket a NICE Keretrendszerben meghatározott és az általunk definiált elvárások szerint.

Ezt továbbá a leadott tananyag hatékonysága és a hallgatók által teljesített tanórai tesztek, valamint a félév végi vizsga is bizonyítja. A harmadik hipotézis alapján definiált szempontrendszer és az ezek segítségével megvalósuló osztályozás, vagyis az egyes témakörök csoportosításával megállapítottuk, hogy az átadott ismeretanyag kellően részletes volt-e, szükséges-e módosítani a hallgatók számára leadott tananyagot. Ezenkívül arra is választ kaptunk, hogy milyen módosításra, kiegészítésre szorul az adott témakör.

A három hipotézis teljesülése esetén megállapítható, hogy a negyedik hipotézis is igaznak bizonyul, amennyiben a harmadik hipotézisben foglalt változtatásokat végrehajtjuk, a vizsgált tantárgy felhasználható a kiberbiztonsági képzés során.

Meggyőződésünk szerint jelen kutatás eredményei megfelelő és hasznos kiinduló alapot jelentenek további kutatások számára, a jelen a tanulmányban említett kiberbiztonsági képzés szempontjából releváns további tantárgyak elemzése, illetve más képzések esetében egyaránt. Ezenkívül a kutatás folytatásaként a korábbiakban említett változtatások végrehajtását követően a vizsgált tantárgy újabb kiértékelése indokolt. Amennyiben az általunk definiált szempontrendszer alapján javasolt módosításoknak köszönhetően a tudástranszfer hatékonysága nő, úgy a szempontrendszer más tantárgyi struktúrák esetére is kiterjeszthető.

Felhasznált irodalom

Alsmadi, Izzat: Cybersecurity Education Based on the NICE Framework: Issues and Challenges, *ISACA Journal, 4.* (2018), 1–6. Online: www.isaca.org/Journal/archives/2018/Volume-4/Pages/cybersecurity-education-based-on-the-nice-framework.aspx

Armstrong, Miriam E. – Keith S. Jones – Akbar Siami Namin: Framework for Developing a Brief Interview to Understand Cyber Defense Work: An Experience Report. In *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting,* 61. (2017), 1. 1318–1322. Online: https://doi.org/10.1177/1541931213601812

Bicak, Ali – Michelle (Xiang)Liu – Diane Murphy: Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal,* 13. (2015), 3. 99–110. Online: http://isedj.org/2015-13/n3/ISEDJv13n3p99.pdf

Dodge, Ronald C – Costis Toregas – Lance Hoffman: Cybersecurity Workforce Development Directions. *HAISA,* (2012), 1–13. Online: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/costis_-_cybersecurity_workforce_development_directions_0.pdf

Estes, Adriane C. – Dan J. Kim – T. Andrew Yang: Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates. In *Proceedings of the 2018 International Conference on Frontiers in Education: Computer Science & Computer Engineering.* CSREA Press, Las Vegas, Nevada, 2018. 1–7. Online: https://par.nsf.gov/servlets/purl/10094856

Falus Iván (szerk.): *Bevezetés a pedagógiai kutatás módszereibe.* Budapest, Keraban, 1996.

Illésy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. *Információs Társadalom,* (2014), 1. 52–73. Online: http://epa.oszk.hu/01900/01963/00043/pdf/EPA01963_informacios_tarsadalom_2014_1_052-073.pdf

(ISC)²: *Certification Exam Outline* (2018. április). Online: www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CISSP-Exam-Outline-2018-v718.ashx

Kumaladewi, Nia – Yuni Sugiarti: *Design Analysis of Data Warehouse for Lecturer Performance Evaluation (Case study: Faculty of science and technology UIN Jakarta).* 4th International Conference on Cyber and IT Service Management. 2016. 1–6. Online: https://doi.org/10.1109/CITSM.2016.7577531

McGettrick, Andrew: Toward Effective Cybersecurity Education, *IEEE Security & Privacy,* 11. (2013), 6. 66–68. Online: https://doi.org/10.1109/MSP.2013.155

Nagyné Takács Veronika – Kovács László: Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono – Magyar Közigazgatás,* 3. (2015), 4. 85–99. Online: https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2653/1918

Newhouse, William – Stephanie Keith – Benjamin Scribner – Greg Witte: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* National Institute of Standards and Technology, 2017. Online: https://doi.org/10.6028/NIST.SP.800-181

Samian, Yahya – Norah Md Noor: Student's Perception on Good Lecturer based on Lecturer Performance Assessment. *Procedia-Social and Behavioral Sciences,* 56. (2012), 783–790. Online: https://doi.org/10.1016/j.sbspro.2012.09.716

Scheponik, Travis – Alan T. Sherman – David DeLatte – Dhananjay Phatak – Linda Oliva – Julia Thompson – Geoffrey L. Herman: How Students Reason about Cybersecurity Concepts. In *IEEE Frontiers in Education Conference (FIE)*. 2016. 1–5. https://doi.org/10.1109/FIE.2016.7757363

Jogi forrás

26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszerbiztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

HADMÉRNÖK
VÉDELEMINFORMATIKA
16. évfolyam (2021) 4. szám 133–143.
DOI: 10.32567/hm.2021.4.10

Attila Horváth[1]

Nanosatellite Constellation Operational Network Ground Segment Analysis

With the ever-increasing capabilities of the smallest remote sensing satellites, a serious bottleneck is encountered at the space-ground interface. While the satellites are capable of collecting data, downlinking said data is not always straightforward. Analysis of the satellite orbits show that the most beneficial downlink station locations can be found in the polar region. This article introduces the reader to the typical Earth observation orbits, their effects on the data communication periods and describes a possible nanosatellite operational radiocommunication network.

Keywords: **nanosatellite, Sun-synchronous orbit, Earth observation, satellite operations, Systems ToolKit**

We have seen a nanosatellite[2] revolution in the last decade. The milk-carton, shoe box, microwave oven sized spacecraft originally intended to provide the first on-hand experience for university students broke out of that use case and became a viable branch of the space industry. We now see businesses based on nanosatellites in the upstream and also the downstream section of the space value chain.

But while the nanosatellites can provide valuable service, the strict size, weight, power constraints force the designers, operators to invest in the ground segment to overcome the limitations of the satellite. Good examples are the SMOG-P and SMOG-1 satellites, where the satellite is 5*5*5 cm, so it occupies 25 square centimetre when placed onto a surface. At the same time, the surface of the ground station antenna is roughly 160,000 square centimetre (4.5 meter paraboloid reflector[3]), so we could fit more than 6,000 SMOG satellites into the antenna dish.

[1] HDF Modernization Institute, Head of Department, e-mail: attila@horvath.space

[2] Typically the satellites weighing from 1 to 10 kg are called nanosatellites, and 10–100 kg spacecraft are called microsatellites. However, for the purpose of this article, I call all satellites based on the CubeSat standard scaled up to 16 units (approximately 20*20*40 cm) nanosatellites weighing up to about 30 kg. The reason behind this is that these satellites are built from similar components, based on a similar methodology. Above this, different design and manufacturing practices are used.

[3] BME–GND, s. a.

This article analyses another limitation of the nanosatellites, namely, the downlinking of the data collected. Bigger remote sensing satellites regularly use geostationary communication satellites to relay data to the ground stations, but realising this on a satellite literally the size of a shoe box is, while not impossible, certainly impractical. However, a solution is clearly available.

1. Introduction to Sun-synchronous polar orbits

A typical application of nanosatellites is Earth observation remote sensing. With advanced (but readily available off-the-shelf) camera technology, it is possible to provide 4–5 metre Ground Sampling Distance electro optical (visual or infrared) imagery from a 500 km circular orbit with a 6 unit cubesat (approximately 10*20*30 cm structure) with a camera based on optics with 90–95 mm front lens diameter.[4] In a 12 or 16 unit body (20*20*30 cm or 20*20*40 cm) one can fit a front lens almost 200 mm in diameter, or if the front lens is square (cut from a circular lens, just like eyeglasses are cut), the effective diameter is around 250 mm. With such a camera, Ground Sampling Distance around 1.5–2 metres is possible from 500 km.[5] However, this data is only valuable, if it can be readily and effectively downloaded.

Remote sensing satellites typically operate on a Sun-synchronous orbit, which is often (but not always) circular.[6] The orbit lies usually 500–800 km above the Earth. With an appropriately selected inclination, the gravitational perturbations caused by Earth force the plane of the orbit to rotate around the centre of the Earth, somewhat less than 1 degree every day. This way the orientation of the orbit relative to the Sun is constant, that is why these orbits are called Sun-synchronous. Sun-synchronicity is very useful for radar satellites. When such a satellite is placed on an orbit perpendicular to the direction of the Sun (the orbit is riding the terminator), the satellite is in constant daylight, and the solar cells can supply energy for the radar without interruption. For optical remote sensing payloads the Sun-synchronicity means that the light conditions on the ground are constant.

However, a satellite moving on such an orbit has relative movement, when viewed from the surface. This is good for remote sensing – we can see almost the complete surface of the Earth, sooner or later, with the exception of the extreme polar regions. But this also means that the data downlink and control stations can only contact the satellites for a few minutes during an overhead pass. Moreover, the closer the data communications station is to the Equator, the fewer the contact times during a day. This limits the amount of data to that can be downloaded, consequently, the amount of data that can be collected, since the onboard storage is limited. Another operational consequence is that whenever the data is collected by the sensor, it will only be available for analysis after it is downlinked, hours or even half a day later. And this is true for the "housekeeping" data also, that is, the telemetry data used by the

[4] Simera Sense MultiScape100 CIS datasheet Rev 3 2020-06-03.
[5] Simera Sense MultiScape200 CIS datasheet Rev 4 2020-06-03.
[6] ESA: Polar and Sun-Synchronous Orbit, 2020.

spacecraft operators to monitor the status of the spacecraft itself; and the command uplink channel is also open only during the overpasses.

But the farther we are from the Equator, that is, closer to the poles, the number of communication windows increases dramatically. This is hardly surprising – the satellite is on a polar trajectory, so it overflies the polar regions on every orbit. So, the closer to the poles, the better – up to a limit.

It is not enough to downlink the data, it must be provided for the analysts to create the usable, marketable products. High-capacity, reliable telecommunication connection is necessary between the satellite downlink (or combined downlink and control) station and the data processing facility. That is hard to come by in the polar region. The Arctic is a more or less ice-covered ocean, the Antarctic continent is far from populated landmasses and no fibre connection is available. Geostationary satellites cannot see the extreme polar region, so satellite communications is also limited. We need to find a compromise: we have to find a suitable real estate for the downlink facility sites as close to the poles as possible, but still within the coverage of a geostationary satellite.

The scenario forming the basis of this article is centred on Hungary – our stated space ambitions and objective limitations are related to our place on the Earth geography. Therefore, the geostationary satellite used in this scenario is placed at the 4 degrees West position over the Equator, the orbital slot assigned to Hungary by the International Telecommunications Union (currently leased by an Israeli commercial satellite operator). The coverage area of such a satellite is easily mapped onto the Earth surface, so we have to find suitable polar landmasses within this area.

On the Northern hemisphere, the Svalbard Islands are optimal. Because Hungary is a state party to the Spitsbergen Treaty, we can exercise our rights to undertake trade activity on the islands, and a non-military satellite downlink station falls within these rights (military bases for wartime use are prohibited by the Treaty).[7] Building an independent, all-year operational facility on our own would be, however, an unnecessary and extremely hard endeavour, therefore, a suitable host facility should be found. Hungary is an active member of the Visegrád 4 group and Poland operates an all-year research base on Svalbard, specifically, at Hornsund: the Polish Polar Station.[8] This site is selected for hosting the Northern hemisphere polar downlink facility. The Polish Polar Station is located at 77 degrees North, 15 degrees 33 minutes East.

The Southern hemisphere is more problematic. Within the coverage area of the geostationary communications satellite, we find South Africa, but it is not farther from (actually, closer to) the Equator than Hungary, so it would not provide any operational benefits. The Southern end of Tierra del Fuego or the Falkland Islands is only 5–8 degrees farther from the Equator, so the number of overpasses would be comparably the same, just at different times. While even this can be seen as an operational benefit, for real performance increase, one needs to go the Antarctic continent.

Several research bases can be found within the area of coverage at or near the shoreline. Again, Northern (closer to the Equator) sites are better for reachback communication, but worse for the polar-orbiting satellite visibility. A good compromise, and a fitting solution

[7] Treaty of 9 February 1920 relating to Spitsbergen (Svalbard).
[8] The Station's history. Hornsund Polska Stacja Polarna, s. a.

(together with the Northern site) is the Henryk Arctowski Polish Antarctic Station on King George Island, which is also an all-year operational facility. The Henryk Arctowski Station is located at 62 degrees 10 minutes South, 58 degrees 28 minutes West.[9]

2. The reference constellation used for modelling

To analyse the communication windows, a digital twin of an imaginary nanosatellite Earth observation constellation was built with the Analytical Graphics Systems ToolKit software. This software is an industry standard tool used for modelling and analysing complex, multi-domain mission systems, including (but certainly not limited to) satellites.

The orbits of the satellites is based on the KH-11 Crystal constellation, the most advanced defence Earth observation remote sensing satellite system operated by the National Reconnaissance Office of the United States. Two satellites are used, on two polar Sun-synchronous orbital planes, one plane set before local noon, the other plane after.[10]

Both satellites operate on a 450 km altitude circular orbit, Local Time of Descending Node is set at 1000 and 1400, respectively.[11] It is assumed that the satellites carry thrusters for orbit maintenance, so the orbit remains unchanged during the operational lifetime.

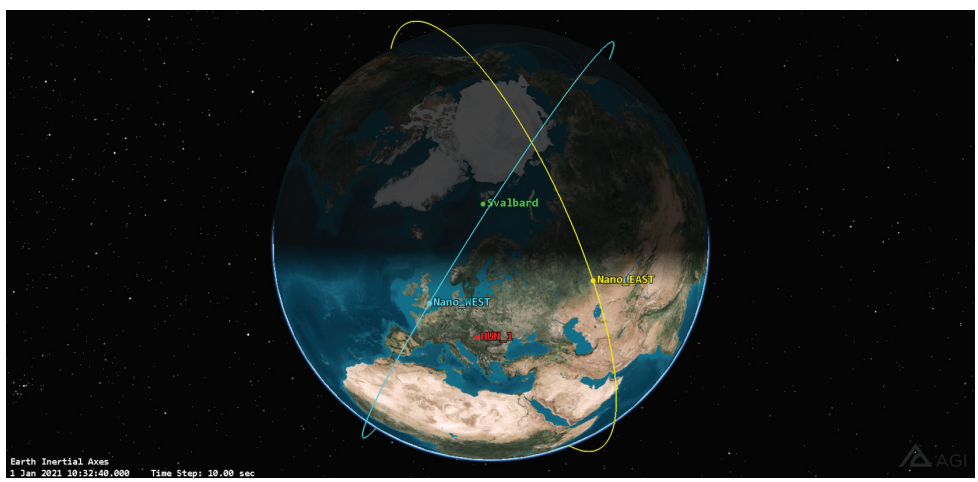


Figure 1

The orbital planes with the two satellites, the Polish Polar Station at Svalbard, and one of the Hungarian stations

Source: Simulated in STK by the author.

[9] History of the founding of the Station, s. a.

[10] KH-11 Status, s. a.

[11] The KH-11 Crystal satellites are launched into elliptical orbits to provide higher resolution imagery of the Northern hemisphere, where most of the targets are located. But this orbit requires frequent and fuel-consuming orbit-maintenance thruster firings, so after a few years, the orbit is circularised by raising the periapsis and lowering the apoapsis. In the scenario used in this article, the orbit is circular from the beginning. The Local Time of the Descending Node values are representative of the KH-11 orbits, but they are rounded to whole hours. This has no practical effect regarding the simulation.

The satellites are equipped with a UHF bidirectional telemetry + control radio and an X-band data downlink radio. The UHF antenna onboard is omnidirectional, the X-band antenna is directional, mounted firmly on the satellite structure; so to communicate with the ground station, the whole satellite body is rotated towards the station by the attitude control system (this makes the remote sensing payload unusable during the communications session).

The 4 ground stations (described in the next section of the article) are also modelled in the Systems ToolKit. The 2 Hungarian stations are placed at arbitrary coordinates (47 degrees North, 19 degrees and 20 degrees East). The polar stations are at their correct coordinates. A 7 degree elevation mask is added to the ground stations to symbolise the possible ground obstacles. Communication is only possible when the satellite is above the mask. The onboard antennas are assumed omnidirectional (even if they are not in reality, this just makes the running of the simulation easier, and during a real operation the attitude control system would keep the antenna pointed for the necessary communication time towards the ground station).

The simulation gives us the time of the rising and setting of the satellite, and the length of the communications window during the transit. The simulation shows the communication opportunities during an arbitrarily selected week, that is, from the 23rd of April 2021 00:00 to the 29th of April 2021 23:59. Only one Hungarian site is included in the simulation of one satellite (HUN_1 site for Nano-EAST satellite and HUN_2 site for Nano-WEST). The second site would theoretically double the communication time, but without a second communication system onboard, the received data would be the same. All times are in Universal Time Coordinated.

3. Simulated communication windows

During the one week long period, for the Nano-EAST satellite, we get the following data from the simulation:

- Access from Arctowski Station: 45 times, 16,330.435 seconds (roughly 4.5 hours, 27.8%) total downlink time
- Access from HUN_1 station: 28 times, 10,324.225 seconds (little less than 3 hours, 17.6%) total downlink time
- Access from Polish Polar Station: 78 times, 32,090.797 seconds (little less than 9 hours, 54.6%) total downlink time
- Altogether, 58,745.457 seconds (roughly 16.5 hours) downlink time

For the Nano-WEST satellite, the number of the communication windows is the same, and the total downlink times are also practically the same, the difference is a few minutes over the whole week.

There are several colliding communication windows at Svalbard, and a few at Arctowski Station ("collision" in this case means that the two satellites arrive to the coverage of the station together, and their respective communication windows overlap at least partially).

This data is extracted from the simulation, via the access analysis function of the Systems ToolKit. By calculating the accesses (that is, communication windows) for the respective stations, it is possible to compile a timetable, listing all the communication opportunities for operations planning. The Systems ToolKit access analysis provides antenna training data (azimuth of the rise above the horizon, azimuth and elevation of the highest point and azimuth of the set).

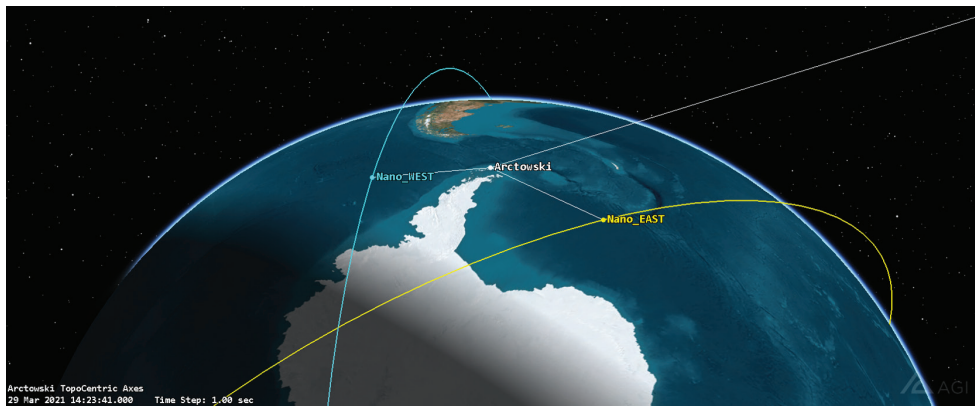


Figure 2

Both satellites are within the communications coverage area of Arctowski Station. The white line going off-screen towards the upper right is the link to the geostationary communications satellite

Source: Simulated in STK by the author.

4. The architecture of the Nanosatellite Operational Network

This section of the article introduces the radio communication systems of a possible multisite nanosatellite downlink and control system. It is designed to provide an optimal number of communication windows with reasonable investments. Even more communication time could be provided with more stations, possibly outside the 4 degree West geostationary position coverage area (that is, visible from another satellite). As of now, I consider this unnecessary. In addition to the investment involved, we need to keep in mind that both the camera and the downlink antenna is installed in a fixed position. So unless the purpose of the satellite is to image the downlink station (an operational scenario hardly justifiable), we have to select whether we download or collect data. The more time we spend for communication, the less remains for imaging.

In the same way, I consider satellite-to-satellite relaying impractical for nanosatellites. Bigger satellites operating in low Earth orbit and spacecraft used for human spaceflight routinely transmit data from the low-orbiting satellite upwards to a geostationary communications satellite to transfer to a suitable ground station. Typical examples are the Tracking and Data Relay Satellite (TDRS) system of the United States,[12] and

[12] Tracking and Data Relay Satellite (TDRS), s. a.

the European Data Relay System and SpaceDataHighway, cooperations of the European Space Agency and Airbus Defence and Space.[13] While intersatellite linking could provide several hours of communication time every day, there are no readily available tracking and narrow beamwidth antennas for nanosatellites today. Widebeam antennas would cause severe adjacent-satellite interference, making frequency coordination and spectrum management difficult. Moreover, without tracking, the whole nanosatellite would need to be trained on the communications satellite, effectively prohibiting the remote sensing payload from operation during the communication time. While the same is true for the ground station communications also, there orbital mechanics limit the communication window. Outside the window the payload can freely operate. In the case of an intersatellite link based operation, we either enjoy the long communication windows (but why, since we cannot collect data), or limit the communication time, just like it is already limited in the ground based case. Laser intersatellite links would be a viable solution (very high datarate, so just a short interruption of the data collection), but fitting a suitable laser terminal into a nanosatellite body (in addition to the payload, power system, thruster and attitude control system, computer and radios) would be very challenging – this only works for bigger satellite bodies as of now.[14]

Therefore, our nanosatellite operational network is based on 4 ground stations: 2 in Hungary for redundancy, one on the Northern and one on the Southern hemisphere polar regions. The polar sites are connected to the satellite operations centre (located in Hungary) via satellite communications links. The Hungarian sites are conveniently colocated with the operations centre(s), or connected via fibre optic and/or microwave links.

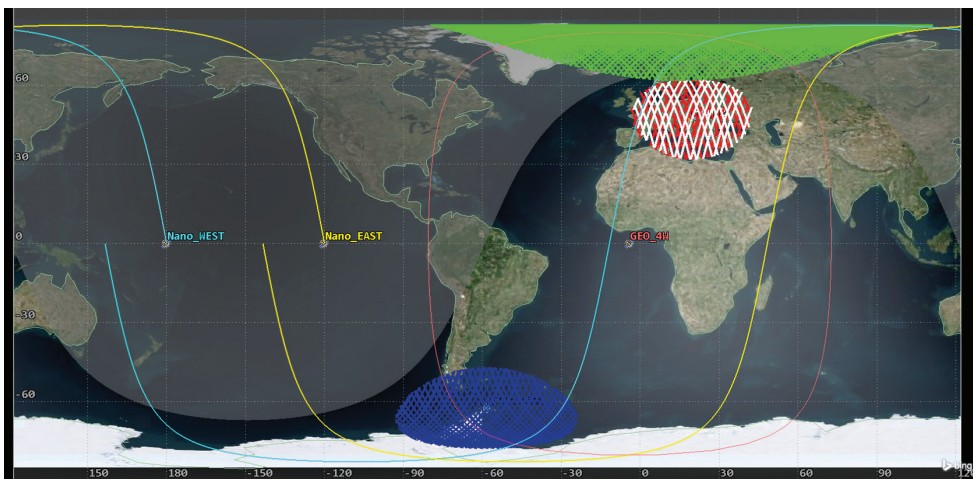


Figure 3

Map of the possible communication windows

Note: When a satellite is the coloured section of the orbit, it is visible to the respective downlink station.

Source: Simulated in STK by the author.

[13] SpaceDataHighway, s. a.

[14] TESAT SMART-LCT datasheet, s. a.

All stations have different advantages and disadvantages. The Hungarian sites can be built the most robust and can have the most reliable connection to the operations centre. They form the backbone of the nanosatellite operations network – although they provide the smallest percentage of the overall communications time. They also have a legal advantage: a remote sensing satellite is a prime asset for defence and security applications, including the space support of military operations. The international treaties governing the utilisation of Svalbard Islands and Antarctica were written without focusing on space activities (obviously). It is not clear if and how infrastructure built there could be used for military purposes, when the supported military activity is happening far from the facilities. Several times the use of imagery downloaded via the Svalbard Satellite Station (a commercial operation of Kongsberg Satellite Services) by military forces resulted in controversial legal publications[15] and political reactions.[16] By declaring that the polar facilities of the nanosatellite operational network are used only for non-warlike purposes, and any directly war-related activity is conducted via the Hungarian sites (if at all), we can avoid such situations.

Serious consideration is necessary to decide whether command uplink should be added to the remote sites or not. The numerous communication time windows provided by these stations increase the operativity and responsiveness of the satellites. But very strong cyber defence safeguards are necessary to prevent the unauthorised access to the satellites via those remote, potentially unmanned sites. Therefore, the safest way is to provide telemetry and data downlink there, this way cybersecurity can be rock-solid.

At the same time, the polar stations provide most of the data throughput and fast access times. Since the nanosatellite is not stationary relative to the observer (the downlink station), the satellite rises above the horizon, transits the sky and then sets. Therefore motorised tracking antennas have to be installed. These tracking antenna mounts must be certified for the environmental conditions expected at the polar locations. The mounts can (and have to be) serviced in-person during the local summer, and they are expected to operate during the local winter remote-controlled. To protect them from the elements (wind load, icing), they must be placed inside a radome. It must be pointed out that the operation of the polar sites is not essential for the safety and usability of the nanosatellites, they just provide extra communication time. Therefore, while losing one or both sites because of a technical problem would severely hurt the performance of the system, it would not cause any danger to the operations.

At the polar stations satellite communications antennas have to be installed. On Svalbard, the elevation angle towards the communications satellite at 4 degrees West is only 3.8 degrees. This is very low, and while it does not prohibit the successful installation of the link, it causes serious challenges. Careful consideration is necessary when selecting the antenna site. The elevation angle at the Henryk Arctowski Station is 7.3 degrees, a much more moderate value. Since the telecommunication satellite is stationary relative to the observer, these antennas do not need to be motorised.

[15] Erik Lieungh, 'Hevder satellittstasjonen på Svalbard blir brukt til krigføring', 09 November 2011.
[16] Erik Lieungh, 'Ingen kontrollerer datastrømmen fra satellittene', 09 November 2011.

The number of antennas at the polar sites depends on the operational tempo. We can safely assume that for telemetry downlink and command uplink one set of antenna is enough, since these operations are comparably fast. To determine the number of sensor data downlink antennas, we have to calculate how much data needs to be downloaded and the time necessary for it.

Based on the MultiScape cameras by Simera, we can assume at most 128 Gigabytes of data to be downloaded, which is 131,072 Megabytes (this is the data of a 2,000 km long strip of imagery for the 200 type camera, or 4,500 km strip for the 100 type). We can also assume, based on various commercially available X-band datalink radios, that the average downlink datarate is around 50 Megabits/second, that is, 6.25 Megabytes/second. The time to download the complete storage is around 21,000 seconds, roughly 6 hours. Careful management of the data collection is necessary, to avoid the generation of imagery which must be discarded after download, because this is roughly two and a half days' worth of communication time!

Because the polar stations cover a significant part of the orbit, "collisions", that is, overlapping satellite arrivals are present, especially at Svalbard. This is not necessarily a problem for the telemetry and control communications, but it would cause significant data loss, unless two downlink antennas are installed. It is absolutely important for Svalbard, and nice to have at the Arctowski Station.

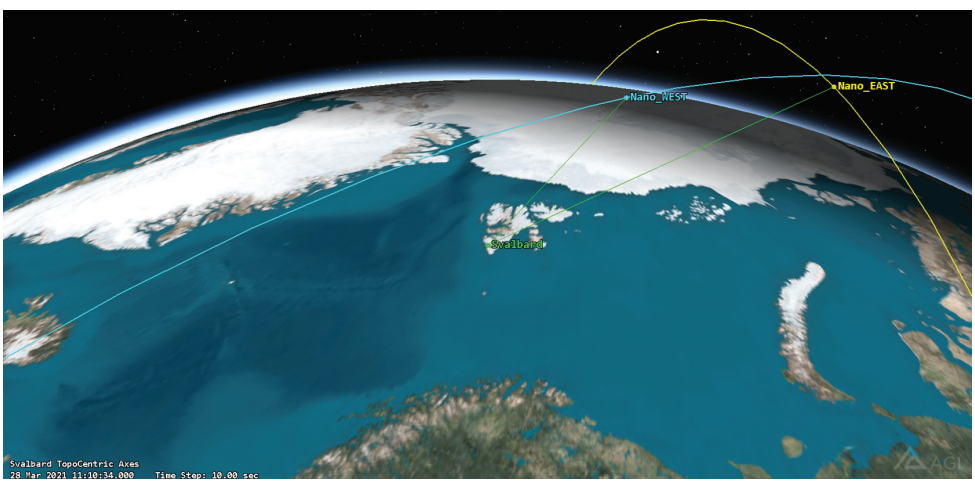


Figure 4

Both satellites are within the communication coverage of Svalbard

Source: Simulated in STK by the author.

Sufficient storage capacity needs to be installed at the remote sites. The reason behind this is that the throughput of the reachback satellite link most likely has significantly lower capacity. So the operational pattern of the remote site is store-and-forward. The exact throughput will have to be determined knowing the actual satellite (frequency, EIRP) and ground station (antenna, amplifier) parameters for the

link budget calculation. But again we can see the advantages of the remote sites, that is, the data can be downloaded in shorter segments, within manageable timeframes, and while the satellite completes the next orbit, the data can be brought home via the slower VSAT link.

5. Summary

With the recent advancement of nanosatellite technology, we can now observe a bottleneck at the space-ground interface, specifically, the ability to download the enormous amount of data collected by a satellite. While it is possible to increase the datarate of the downlink up to a certain limit, this does not solve the problem of timeliness – however fast one can download, the download can only start when the satellite is within line-of-sight to the ground station.

Since a typical Earth observation remote sensing satellite travels on a polar orbit, it is logical to locate the ground stations in the polar regions. But the way the data must travel does not end at the ground station, so we also have to take the means to transport it to the place of the procession into account. Practically, this means satellite communications, which limits how close to the poles the ground stations can be placed.

In this article I described, based on a hypothetical two-satellite remote sensing constellation simulated in Systems ToolKit, a nanosatellite operations network consisting of 3 ground station locations (since the two stations in Hungary can be considered one), one at the North pole, one at the South pole, and one active and one alternate station in Hungary. The polar stations are located at Polish research bases, and they are connected to Hungary via VSAT links provided by a satellite at the orbital slot assigned to Hungary, 4 degrees West over the Equator.

The results of the analysis show that such a network architecture is immensely beneficial, as it is able to increase the communication time roughly by a factor of 6.

It is recommended therefore, to plan with polar ground station infrastructure, if and when a nanosatellite constellation is being built to support defence and security operations.

This article was written with the support of the ÚNKP New National Excellence Program in cooperation with the National Research, Development and Innovation Office and the Ministry of Innovation and Technology (ÚNKP ID: ÚNKP-20-3-II-NKE-62).

References

BME–GND, s. a. Online: https://gnd.bme.hu/articles/20150831_gnd_fejlesztes.php
ESA: Polar and Sun-Synchronous Orbit, 2020. Online: www.esa.int/ESA_Multimedia/Images/2020/03/Polar_and_Sun-synchronous_orbit
History of the founding of the Station, s. a. Online: http://arctowski.aq/en/station-history/
KH-11 Status, s. a. Online: www.zarya.info/Diaries/US/KH11.php
Lieungh, Erik, 'Hevder satellittstasjonen på Svalbard blir brukt til krigføring', 09 November 2011. Online: www.nrk.no/tromsogfinnmark/hevder-svalsat-brukes-i-krigforing-1.7860894
Lieungh, Erik, 'Ingen kontrollerer datastrømmen fra satellittene', 09 November 2011. Online: www.nrk.no/tromsogfinnmark/ingen-kontrollerer-satelittdataen-1.7865712
Simera Sense MultiScape100 CIS datasheet Rev 3 2020-06-03. Online: https://simera-sense.com/products/multiscape100-cis/
Simera Sense MultiScape200 CIS datasheet Rev 4 2020-06-03. Online: https://simera-sense.com/products/xscape200/multiscape200-cis/
SpaceDataHighway, s. a. Online: www.airbus.com/space/telecommunications-satellites/space-data-highway.html
TESAT SMART-LCT datasheet, s. a. Online: www.tesat.de/products
The Station's history. Hornsund Polska Stacja Polarna, s. a. Online: https://hornsund.igf.edu.pl/about-the-station/the-stations-history/
Tracking and Data Relay Satellite (TDRS), s. a. Online: www.nasa.gov/directorates/heo/scan/services/networks/tdrs_main
Treaty of 9 February 1920 relating to Spitsbergen (Svalbard). Online: http://library.arcticportal.org/1909/1/The_Svalbard_Treaty_9ssFy.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 145–156.
DOI: 10.32567/hm.2021.4.11

Kerti András,[1] Koller Marco[2]

Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása[3]

Possible User-level Reduction of Misuse of Metadata Collected by Smart Device Applications at Risk Level

Az okoseszközök hétköznapivá válásával és a különböző funkciókat betöltő alkalmazások elterjedésével olyan információbiztonsági kockázatokkal néz szembe az átlagos felhasználó, amelynek talán nincs is tudatában. A különböző személyek és csoportok által fejlesztett applikációk, olyan (meta)adatokat is gyűjthetnek, amelyekkel adott felhasználó szokásai és kapcsolati hálózata könnyen beazonosíthatóvá, illetőleg felhasználhatóvá válhat az alkalmazás mögött rejlő személyek, csoportok számára. A nem kívánt adatgyűjtés elkerülése érdekében sokat segíthet a tudatos felhasználói magatartás. Ezen magatartás kialakításához hozzájárulhat, ha az applikációk alkalmazása előtt a vállalatok által is használt kockázatmenedzsment szemléletén keresztül közelítjük meg a különböző szoftvereket. Jelen kutatás célja a fentiek során kifejtett szemléletmód általi kockázatcsökkentés.

Kulcsszavak: **információbiztonság, kockázatmenedzsment, okoseszközök, metaadat, biztonságtudatosság**

As smart devices and applications with different functions become ubiquitous, the average user faces information security risks that he or she may not be aware

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi docens, e-mail: kerti.andras@uni-nke.hu
[2] Hadtudományi Doktori Iskola, doktori hallgató, e-mail: marcoakoller@gmail.com
[3] A tanulmány az Innovációs és Technológiai Minisztérium ÚNKP-20-3-I-NKE-94 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

of. Applications developed by different people and groups can also collect (meta) data with which a person's habits and network of contacts can be easily identified or used by the people and groups behind the application. Conscious user retention can help a lot to avoid unwanted data collection. Contributing to the development of this attitude can be achieved by approaching different software through the risk management approach used by companies before applying applications. The aim of the present research is to reduce the risk by the approach outlined above.

Keywords: **information security, risk management, smart devices, metadata, awareness**

1. Bevezetés

Az információs társadalom egyik ismérve a keletkezett adatok, információk mennyiségének és áramlásának nagymértékű növekedése. Ezen társadalom alkotórészévé vált a technológia, illetve a technológiai fejlődés, amely számos lehetőséget és kihívást rejt magában. Az ember és a gép kapcsolatát megvalósító eszközök a felhasználó és a berendezés kommunikációját teszik lehetővé, ez az ember-gép interfész technológia. E technológia legjellemzőbb példái a különböző okoseszközök.

Az okoseszközök térnyerésével, azok mindennapjaink szerves részévé válásával a különböző állami és nem állami szereplők olyan értékes információkhoz juthatnak az emberek mindennapi szokásairól, amelyekkel következtetni lehet adott személy kapcsolati hálózatára, baráti körére, tartózkodási helyeire, fogyasztási szokásaira, vagy akár káros szenvedélyeire is.[4] Kiemelt figyelmet érdemelnek az okoseszközök által betöltött különböző funkciók, azok evolúciója, mint például az okostelefonokon működő mobil banking applikációk, amelyekkel mindennapi banki ügyeinket már telefonon keresztül is végre tudjuk hajtani.[5] A fentiek alapján kijelenthető, hogy az okoseszközök és a hozzájuk köthető applikációk kockázatot hordoznak magukban.

1.1. A kutatás célja

A publikáció célja kockázati szemléletmód-alapú, a kockázatmenedzsment folyamatán keresztül tudományos igényességgel bemutatott, tudatos felhasználói magatartás megfogalmazása, amely alkalmas arra, hogy a felhasználó visszaszorítsa a nemkívánatos, személyével kapcsolatos (meta)adatgyűjtést. Ezzel járulva hozzá a személyes és társadalmi információbiztonsághoz egy humán aspektusú megközelítésen keresztül. Azért tartom fontosnak a humán aspektusú megközelítést, mert bár már közhelyes, azonban igaz, bármilyen erős fizikai és/vagy logikai védelemmel van ellátva adott technológia, maga a felhasználó (humán tényező) gyenge pont lehet, amelyen keresztül információt, adatot lehet kinyerni.[6]

[4] Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom,* 17. (2017), 1. 55–71.
[5] Vizi Pál: Okostelefonok biztonsági kihívásai. *Hadmérnök,* 6. (2011), 3. 131–141.
[6] Bányász Péter: Social Engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018b), 1. 4.

1.2. Kutatási módszertan

Jelen tanulmány elkészítése során a hazai és a nemzetközi szakirodalmat, illetve szabályozókat tekintettük át, illetve elemeztük a kockázatmenedzsment, a biztonságtudatosság, a metaadat, illetve az okoseszközök területén.

2. Alapfogalmak definiálása

A mobil applikációk által gyűjtött metadatokkal való visszaélések és abban rejlő kockázatok megértéséhez szükséges megteremteni az értelmezési keretet és a kellő kontextust, így fontos bemutatni a téma alapfogalmait. Az alábbiakban a kockázat és a metaadat fogalmi kereteit tisztázzuk.

2.1. A kockázat fogalmának bemutatása

A kockázat fogalmának több megközelítése is van. Resperger szerint a kockázat fogalma „az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek”.[7] A fenti besorolás a kockázatot mint biztonságpolitikai, hadtudományi, illetve nemzetbiztonsági fogalmat közelíti meg egy hármas rendszerezésben, ahol a kockázat középen, a kihívás legalul helyezkedik el, és a legnagyobb veszéllyel, úgymond hatással rendelkező lehetséges eseménynek a fenyegetést nevezi meg és helyezi legfölülre. Megállapítható, hogy ez a fogalmi keret hatásalapú megközelítést mutat be, azonban álláspontom szerint a hatás nagysága mellett a bekövetkezési valószínűség és a kettő elhárításának nehézsége is a fogalom részét kell képezze. „A kockázattal kapcsolatos fogalmakat a szakirodalom a szóban forgó tudományterülettől, a vizsgálati céloktól”[8] függően többféle szempont szerint tárgyalja.

Egy másik megközelítés szerint a kockázat: „A kockázati esemény esetleges bekövetkezésekor annak a szervezetre gyakorolt jelentősége, fontossága.”[9] A kockázati esemény pedig: „A szervezetre (a vezetők által meghatározott célok elérésre vagy a követelmények teljesítésére) várhatóan jelentős hatást gyakorló, de még be nem következett esemény. Egy eseményre vonatkozóan bejelentett gyanút nem lehet kockázati eseményként kezelni, mert ez utóbbi esetben egy, a feltételezés szerint már bekövetkezett eseménnyel kapcsolatban vagyunk bizonytalanok.”[10] A kockázatot – az ISO 31000 szabvány alapján – mint a bizonytalanság szervezeti célokra való hatását értelmezzük. A fentiek alapján megállapítható, hogy a kockázat valamilyen

[7] Resperger István: Biztonsági kihívások, kockázatok és fenyegetések 2030-ig. In Kobolka István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest, Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 31–33.
[8] Székely Csaba: Stratégiai kockázatmenedzsment. *Taylor,* 7. (2015), 1–2. 105.
[9] Horváth Péter – Németh Edit: *Integrált kockázatkezelési rendszer alapjai*. Budapest, Dialóg Campus, 2018. 9.
[10] Horváth–Németh (2018): i. m. 9.

bizonytalansági faktort jelöl, amelynek bekövetkezése esetén negatív hatása van valamilyen védendő értékre.

A kockázat fogalmából, amelyet a fentiek alapján értelmezünk, következik, hogy mi az a bizonytalanság, amely hatással lehet az adott célokra, a biztonság összetevőire. Információbiztonsági szempontból bizonytalanság annak a hiánya, hogy képesek vagyunk előre jelezni az aktuálisan végbe menő cselekmények jövőre történő hatását. „Kockázat esetén nem lehet pontosan előre jelezni az egyes kimenetelek bekövetkezését, illetőleg annak valószínűségeit."[11]

Amennyiben a bizonytalanság és a kockázat fenti definícióiból indulunk ki, arra a következtetésre juthatunk, hogy a kockázat negatív hatása bekövetkezésének megelőzése érdekében (proaktív gondolkodást elősegítve a reaktív ellenében) a bizonytalanságot kell csökkenteni, úgy, hogy a lehetséges hatás felmérése érdekében növeljük az informáltságunkat.[12]

A kockázat fogalma során felmerült összetevők közül a bizonytalanság tényezőjét tisztáztuk, az alábbiakban a hatás fogalmi kereteit kívánom körülírni. Tekintettel arra, hogy a kockázat minden egyes szervezet vagy személy számára mást-mást jelenthet, a különböző hatásokból is többféle létezik. Elmondható továbbá, hogy a hatások heterogenitásán túl annak nagysága alapján is érdemes differenciálni, ahogy ezt a különböző biztosítási társaságok teszik. Az átlag okostelefont használó személy esetében álláspontom szerint az is előrelépés, ha tisztában van, hogy egy applikáció telepítése, használata előtt szükséges felmérnie, hogy azzal kapcsolatban milyen mennyiségű és minőségű információkkal rendelkezik, így nehezebben érheti kellemetlen meglepetés.[13]

2.2. A metaadat fogalmának meghatározása

Minden informatikai eszköz vagy program használata során – így a különböző mobilapplikációk esetében is – keletkeznek metaadatok, mivel fontos szerepük van az automatizált adatfeldolgozás hátterének biztosításában, az adattárolási rendszerekben.[14]

A metaadat legegyszerűbb megfogalmazása álláspontom szerint: adat az adatról. Valójában a dokumentumok azonosítására szolgál, azáltal, hogy a leíró adatok struktúrája egységes szerkezetnek megfelelő struktúrában készül.[15] Azaz valamilyen adatról, információról nem tartalmi adat, hanem azzal kapcsolatos, kvázi külsőleges adat. Például egy levélnek a tartalma a fő információ, azonban az, hogy milyen szolgáltatón keresztül, kitől érkezett a levél és kinek, illetve mikor, az a levélről szóló adat, azaz a metaadat. Az ilyen jellegű információk birtokában az állami és nem állami szereplők különböző személyek szokásait, illetve kapcsolati hálóját képesek felderíteni.

[11] Székely (2015): i. m. 105.
[12] Székely (2015): i. m. 113–118.
[13] Székely (2015): i. m. 113–118.
[14] Kovács László – Bednarik László: Digitális dokumentumok formátumai és az XSLT-FO. In Berke József (szerk.): *Multimédia az oktatásban konferencia.* Nyíregyháza, MTESZ Neumann János Számítógép-tudományi Társaság, CD kiadvány, 2010.
[15] Lásd: https://openscience.hu/metaadat/

A metaadat fogalmát behelyezhetjük a személyes adatok halmazába, tekintettel arra, hogy a GDPR[16] szerint személyes adatnak minősül minden olyan adat, amely a természetes személy azonosítására akár részben is alkalmas. Ilyen lehet például a helymeghatározó adat, vagy az online azonosító. A fentiek alapján, amikor egy mobilapplikáció a különböző online azonosítónkat vagy a GPS-koordinátánkat kéri el, akkor a személyes adatainkat kezeli, így az alkalmazásért felelős cég adatkezelőként van jelen. A GDPR egyik nagy előnye, hogy tiltja azt a korábban bevett gyakorlatot, amely lehetővé tette a hallgatólagos beleegyezéssel történő adatgyűjtést, továbbá szankciókat is kilátásba helyez, amennyiben egy adatkezelő nem felel meg az előírtaknak.[17] A személyes adattal való visszaélés nem csupán a GDPR-ban megjelenő fogalom, a magyar büntetőjog is bünteti.[18]

A metaadatok, mint ahogy a fentiekben kifejtettem, adatok az adatról, általában egy dokumentum valamilyen strukturális, használati, formai, esetleg tartalmi kapcsolataira vonatkozó adat. Csoportosítása többféleképpen történhet, jelen tanulmányban két csoportra bontom a fogalmat, egyrészről leíró, másrészről forgalmi metaadatra.

- „A leíró metaadat a dokumentumok formai, tartalmi és strukturális jellemzőit biztosító, tipizált, másodrendű információ.
- A forgalmi metaadat a dokumentumok és a felhasználók közti használati, forgalmi kapcsolatokat (megtekintést, letöltést, meghallgatást, lájkolást, megvásárlást, kommentelést stb.) mint eseményeket leíró, másodrendű információ."[19]

A forgalmi metaadatok gyűjtése és elemzése által lehet felhasználói „profilokat", mintázatokat készíteni, amelyekkel vásárlási szokásokra, különböző kapcsolati hálókra lehet következtetni.

3. A kockázatmenedzsment folyamata

A kockázatmenedzsmentnek számos definíciója létezik, álláspontom alapján az alábbi az egyik legegyszerűbb és legérthetőbb. A kockázatmenedzsment „egy olyan vállalatvezetési alrendszer, ami a döntés szempontjából releváns kockázatokat rögzíti, méri és irányítja, valamint a vállalat összes kockázatát felügyeli és elemzi a kapcsolódó potenciális veszteségeket".[20] A kockázatmenedzsment mint folyamat magában foglalja a kockázatelemzést, kockázatkiértékelést, továbbá a kockázatszabályozással kapcsolatos irányítási elveket és gyakorlatokat. A folyamatos kockázatmenedzsment olyan széles

[16] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.

[17] Erdős Gabriella: *Néhány gondolat az adatbiztonságról és az adatkezelésről az okos alkalmazások területén.* Budapest, Corvinus Egyetem, 2020.

[18] 2012. évi C. törvény a Büntetőtörvénykönyvről (Btk). 219. § – Személyes adattal visszaélés.

[19] Metainformáció, metaadat: www.fogalomtar.hte.hu/wiki/-/wiki/HTE+Infokommunikacios+Fogalomtar/Metainform%C3%A1ci%C3%B3+-+metaadat

[20] Halczmann Attila: Kockázatmenedzsment követelménye irányítási rendszerekben. *International Journal of Engineering and Management Sciences,* 3. (2018), 3. 315.

körben használt módszer, amely alkalmas a különböző kockázati elemeket is magában foglaló munka menedzsmentjére.[21] „A kockázatmenedzsment iteratív és adaptív folyamat, mely minden tevékenysége az előzőre épül, felhasználva a korábbi lépések során feltárt információkat, folyamatosan csökkentve a kockázatot."[22] A fogalmi meghatározásból jól látszik, hogy nem egyszeri cselekmény, hanem folyamat, amely több alkotóelemből áll, fontos az állandó visszacsatolás.

A kockázatmenedzsment folyamata alkotóelemeire bontva az alábbiak szerint néz ki:

1. környezetkialakítás;
2. kockázatfelmérés (kockázatazonosítás, kockázatelemzés, kockázatértékelés);
3. kockázatkezelés;
4. kockázatelfogadás;
5. kockázatok kommunikációja, konzultációja;
6. kockázat figyelemmel kísérése és átvizsgálása.[23]

Az elemekre bontott folyamat alapján kitűnik, hogy bizonyos kockázatokat el kell fogadni, azaz vannak olyan bizonytalansági tényezők, amelyek nem iktathatók ki teljesen, ezeket a minimumra kell redukálni. A későbbiekben jól láthatjuk, hogy egy adott személyre lebontva a folyamatot, mint szemléletmód is számolni kell maradványkockázatokkal, azonban a tudatos felhasználói viselkedés, akár a kockázatmenedzsment a vállalatoknál, a fennálló bizonytalanságot és annak hatását próbálja a minimálisra csökkenteni.

4. Mobilapplikációk által gyűjtött adatok és kockázatok

Bányász Péter az okosmobileszközök biztonságával kapcsolatban készített elemzésében is megállapította, hogy a legnagyobb számban előforduló fenyegetést ezek az alkalmazások, azaz az applikációk jelentik. Tekintettel arra, hogy az eszközeinkre telepített alkalmazások sokfélék, számos kockázatot rejtenek magukban. Bányász Péter is arra a következtetésre jutott, hogy a biztonságtudatos alkalmazás vagy használat csökkenti a nemkívánatos adatgyűjtés kockázatát, de az sem nyújt természetesen 100%-os védelmet, azaz mindig számolni kell maradványkockázattal. A különböző applikációkban rejlő kockázatokat többféle módon lehet kategorizálni. Megítélésem szerint két fő kategóriára osztható: egyrészről a kockázat fellépésnek időpontja, másrészről a felhasználó számára jelentkező negatív hatás alapján. A fellépés időpontja alapján jelentkezhet a kockázat az adott applikáció letöltése, telepítése vagy konkrétan annak futtatása során. Álláspontom szerint az első két fázisban lehet tudatosság által csökkenteni az esetlegesen fellépő negatív következményeket, illetve elhárítani azokat. A felmerülő negatív következmény alapján a nem kívánt adatgyűjtés eredményének felhasználóra való hatása alapján lehet kategorizálni, például telefon bothálózat

[21] Hanane Bahtit – Boubker Regragui: Risk Management for ISO 27005 Decision support. *International Journal of Innovative Research in Science,* Engineering and Technology, 2. (2013), 3. 530–538.
[22] Abonyi János – Fülep Tímea: *Biztonságkritikus rendszerek*. Pannon Egyetem, 2014.
[23] Székely (2015): i. m. 113–118.

tagjává tétel, banki adatok ellopása, identitás ellopása, vagy egyszerűen nem kívánt marketingcélú felhasználás.[24]

Véleményem szerint a legnagyobb kockázatot magukban hordozó applikációtípusok közé tartoznak a banki alkalmazások, amelyek egyre elterjedtebbek hazánkban is, tekintettel arra, hogy kényelmi funkciójuk megkérdőjelezhetetlen. Egy ilyen applikáció azonban olyan adatok birtokában van, amelyeket az átlagember a legjobban félt, azaz a pénzügyével, számlájával kapcsolatos információk, az azon található összeg feletti rendelkezés lehetősége. Az ImmuniWeb1 2019 közepén saját fejlesztésű mesterséges-intelligencia-alapú platformja által tesztelte a világ 100 legnagyobb bankjának alkalmazásait adatbiztonsági kritériumok alapján. Arra a megdöbbentő megállapításra jutottak, hogy csak három bank volt rendben adatbiztonsági szempontból. A kutatás a megvizsgált összes applikációban legalább alacsony kockázatú sebezhetőségeket talált, továbbá megállapította, hogy minden ötödik banki alkalmazás súlyos hibákkal működik. A kutatás alapján az alkalmazások 55%-a fér hozzá különösen érzékeny adatokhoz.[25]

A különböző mobilalkalmazásokban rejlő kockázatot legjobban szemlélteti a külföldön elterjedt Uber applikációval kapcsolatban megjelent 2017-es hír. Az Apple operációs rendszerét (iOS) használó telefonoknál detektálták, hogy az Uber applikáció képes volt arra, hogy megfigyelje a készülék kijelzőjén történteket, mindezt a felhasználó előtt rejtve. Ezzel olyan biztonsági rést generált az alkalmazás, amellyel személyek jelszavait, személyes adatait is rögzíthették volna, azonban a visszaélés megtörténtére nem keletkezett bejelentés. Az Uber az applikáció következő verziójában ezt a sérülékenységet kijavította.[26]

5. A metaadattal történő visszaélésben rejlő kockázatok

A fentiekben már említett okoseszközök térnyerésével, kiváltképp az okostelefonok elterjedésével a letölthető különböző kényelmi vagy szórakoztatási funkciót betöltő applikációk száma is nőtt. Számos applikáció kér hozzáférést bizonyos jellegű, a telefonon tárolt információkhoz (például telefonkönyv, helyadatok, képernyőidő stb.), amely által a szoftver fejlesztője fel tudja használni ezen információkat saját vállalkozása és terméke fejlesztése érdekében, vagy harmadik félnek is esetlegesen átadhatja bevételszerzés céljából. Az előbbiek megvalósulhatnak a felhasználó tudatos beleegyezésével (felhasználói nyilatkozat), illetve anélkül is. A második kategóriába már több esetben beletartoznak a különböző káros szoftverek (adathalász programok), amelyek nem csupán saját, hanem akár munkahelyünk adatbiztonságát is veszélyeztethetik rajtunk keresztül.[27]

[24] Bányász Péter: Az okos mobil eszközök biztonsága. *Hadmérnök,* 13. (2018a), 2. 360–377.
[25] Erdős (2020): i. m.
[26] Fehér-Polgár Pál – Michelberger Pál: A sajáttulajdonú mobil eszközök információbiztonsági kockázatai. *International Journal of Engineering and Management Sciences,* 3. (2018), 4. 176–185.
[27] Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatása. In Kállai Attila et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése (Tanulmánygyűjtemény I., e-book).* Nemzeti Közszolgálati Egyetem, 2016. 666.

Azonban az első kategória esetén a felhasználói attitűd és „érzékenység" kiváltképp meghatározó a nemkívánatos adatgyűjtés elkerülésének szempontjából, ugyanis, ha a felhasználó nem, vagy nem kellő alapossággal olvassa el a felhasználói nyilatkozatot vagy szerződést, akkor tevékenységéről, személyéről olyan adatok kerülnek egy adott céghez, amelyhez az adott szerződés teljes tudatában lehetséges, hogy nem járult volna hozzá.

A CRAMM[28] támadási modell alapján kifejezetten leegyszerűsítve így foglalható össze a metaadatokkal való visszaélésekben rejlő kockázat: a fenyegetés a felhasználó (meta)adataival történő nemkívánatos felhasználás, illetve visszaélés. A sebezhetőség, amelyen keresztül a fenyegetés kifejti a hatását, az adott applikáció, illetve a telepítéséhez szükséges szerződés elfogadása, illetve a nem kellően tudatos felhasználói attitűd. Amiben/amivel kárt lehet okozni, az az adott felhasználó adatai, adat- és információbiztonsága, illetve a felhasználói bizalom.[29]

Adott alkalmazás az általunk használt eszköz különböző szolgáltatásait veszi igénybe annak függvényében, hogy az applikáció milyen szolgáltatást nyújt a felhasználónak. Teljesen természetes, hogy egy fényképkészítő alkalmazás hozzáférést igényel a telefon kamerájához, galériájához. Azonban egyes esetekben jogosan merül fel a felhasználókban a kérdés, hogy például egy játékszoftver miért kér engedélyt telefonkönyvünkhöz, vagy egy zseblámpa-alkalmazás miért kér hozzáférést helyadatainkhoz.[30] A fentiekben felsoroltak kisarkított példák, amikor szinte egyértelmű, hogy az adott applikáció olyan adatokat gyűjt, amely nem szükséges az általa kínált funkciók használatához, csupán a fejlesztőnek vagy harmadik félnek gyűjt az eszköz használójáról szenzitív információkat. Nem ilyen egyszerű felfedezni a nem kívánt adatgyűjtést más esetekben. Hiszen egy futáshoz használt fitneszalkalmazás esetén életszerű, ha a valós idejű helyadatainkat akarja gyűjteni. Azonban pont egy ilyen alkalmazás fedte fel véletlenül egyes amerikai katonai központok titkos helyzetét, mivel az ott állomásozó katonák is használták, így a bázison és az a körül történt futóedzések alapján könnyen beazonosítható volt a „senki földjén" lévő objektumok helyzete.[31] Jól látható, hogy a metaadatok bár önmagukban nem tűnnek nagy jelentőségű adatállománynak, azonban megfelelő rendszerezéssel és értékeléssel olyan információk nyerhetők ki, amelyek nem csupán a marketingesek, hanem más nem törvényes célokat szolgáló személyek, csoportok részére is hatalmas értékűek lehetnek. Ezen adatok a big data-elemzéssel igen pontos előrejelzést is adhatnak a felhasználó szokásairól, jövőbeli cselekedeteiről.[32]

[28] Central Computer and Telecommunation Agency (Egyesült Királyság) által kidolgozott kockázatelemzési és -kezelési módszertan *(CCTA Risk Analysis and Management Method)*.

[29] Horváth Zsolt – Kocsis István: A CRAMM módszer alkalmazásának kiterjesztése. In *Proceedings of 8th International Engineering Symposium at Bánki.* 2016.

[30] Bányász (2018a): i. m.

[31] Fehér-Polgár – Michelberger (2018): i. m.

[32] Bányász (2018a): i. m.

6. Metaadattal történő visszaélések megelőzése kockázatmenedzsment-alapú szemléletmód által

Végezetül a kockázatmenedzsment folyamatán keresztül kívánom bemutatni, hogy a felhasználói szinten milyen módon kellene végbe mennie a tudatos okoseszköz-használatnak.

Környezetkialakítás: első lépésként a felhasználónak ki kell alakítania a környezetet, azaz meg kell állapítania az alapvető kritériumokat, milyen szempont alapján értékeli a kockázatokat, mi az a kockázati nagyság, az a hatás, amely még belefér adott applikáció letöltésébe, telepítésébe, illetve használatába. Le kell fektetnie azokat az alapokat, amelyek alapján a továbbiakban megközelíti az applikációkat, azaz meg kell határoznia, hogy egy alkalmazás telepítésekor milyen kockázatok várhatók, lebontva az applikáció készítőjének megbízhatóságára, illetve arra, hogy egyes jogosultságok (GPS-koordináták, névjegyzék) megadása, az azokkal való visszaélés milyen kockázatokat rejt magában. A környezet kialakításakor fontos az előzetes tájékozottság, egyfajta kutatómunka szükséges. Álláspontom alapján a kutatómunkát e pontnál általánosságban az applikációkra kell végezni, egyes konkrét alkalmazások esetén is szükséges külön kutatás végrehajtása.

6.1. Kockázatfelmérés (kockázatazonosítás, kockázatelemzés, kockázatértékelés)

Jelen pontnál a felhasználónak az egyes applikációkat szükséges vizsgálnia. Azonosítania kell az alkalmazás telepítése előtt, hogy annak letöltése, telepítése és alkalmazása során milyen specifikus fenyegetésekkel kell szembenéznie, fel kell mérnie, hogy mennyiben tudja kontroll alatt tartani az adott applikáció által gyűjtött adatokat. Lehetséges úgy használni a Facebook Messenger applikációját, hogy nem engedélyezzük a mikrofonhoz való hozzáférést, ez a jogosultság később is engedélyezhető, kikapcsolható. Azonosítani szükséges, hogy mik azok a vagyonelemek a felhasználó tekintetében, amelyekre az alkalmazás kockázatot jelenthet, például személyes adatok, a készülék vírusmentes állapota stb. Amennyiben ezek megtörténtek, elemeznie kell a felhasználónak, hogy milyen valószínűséggel következhet be egy biztonsági incidens, ennek milyen hatásai lehetnek, azaz a várható hatást és a bizonytalansági faktort kell szem előtt tartania. Érdemes az applikációinkat kategorizálni, szintekre bontani egy esetlegesen bekövetkezhető információbiztonsági incidens alapján. Végül a fentiek megtétele után értékelni szükséges, hogy a várható negatív hatás mértéke és bekövetkezésének valószínűsége alapján érdemes-e az applikációt letölteni, telepíteni, illetve használni.

6.2. Kockázatkezelés

Amennyiben egy alkalmazás kapcsán felmerül a felhasználóban, hogy értékelése szerint kockázat áll fenn, akkor a kockázatmenedzsment jelen szakaszát kell alkalmaznia. Alapvetően háromféle kockázatkezelési lehetőséggel tud élni. Módosítja a kockázatot,

amennyiben lehetséges, egyes jogosultságokat megvon az applikációtól. Vagy fenntartja a kockázatot, tekintettel arra, hogy az alkalmazás elengedhetetlen, vagy olyan kényelmi funkciót tölt be, hogy a kockázat vállalása megéri a felhasználó számára. Illetőleg elkerülheti a kockázatot, jelen esetben törli, vagy nem tölti le az applikációt, ezzel a lehetséges kockázatot elkerüli. Minden esetben mérlegelni kell, bármelyik stratégiát is választjuk, hogy milyen mértékű lesz a maradványkockázat, ez alapján az előzetes kritériumok, az elemzési módszertan módosítása is szükséges lehet.

6.3. Kockázatelfogadás

Fontos, mint ahogy a fentiekben is többször említettük, hogy a felhasználói tudatosság nem nyújt teljes védelmet, azonban a kockázatok szintjét meghatározhatjuk, ezáltal biztonságosabbá tehető az alkalmazások használata. Jelen stádiumnál a felhasználónak a fentiek alkalmazása után, amennyiben elfogadhatónak ítéli a fennmaradó kockázatokat, azokat el kell fogadnia, és tisztában kell lennie azok lehetséges hatásaival, illetve a bekövetkezési valószínűséggel.

6.4. A kockázatok kommunikációjának konzultációja

Felhasználói viselkedésre történő átvezetése jelen kategóriánál nehezen értelmezhető, tekintettel arra, hogy ez a vállalatok egyes projektjeinél alkalmazható metódus. Azonban felmerülhet a biztonságtudatos magatartás esetén is, amennyiben az adott személy felmér bizonyos kockázatot, akkor azt jelezheti az applikáció fejlesztőinél vagy az értékesítés felületén, ahol az alkalmazást vásárolta. Ezáltal káros vagy nem kívánt adatgyűjtéssel foglalkozó applikációkat akár ki is szűrhet az által, hogy a fejlesztő nem tudatosan végezte ezt, mint az Uber, vagy az értékesítési felületet birtokló cég távolíthatja el az alkalmazást az adott webshopból.

6.5. Kockázat figyelemmel kísérése és átvizsgálás

Végezetül kijelenthető, hogy a fentiek elvégzése nem egyszeri cselekvés, folyamatnak kell lennie; egyes applikációk frissítéseivel változhat kockázati besorolásuk, vagy a felhasználó igénye is megváltozhat a biztonság terén. Így a felhasználónak fontos mindig monitoroznia, figyelemmel kísérnie az okoseszközén telepített alkalmazásokat.

7. Összefoglalás

Általánosságban elmondható, hogy a digitális világ kiszélesedésével az adatbiztonság, személyes információink védelme egyre fontosabb és nehezebb lesz, illetve az okoseszközök és a különböző, azokra letölthető applikációk használata információbiztonsági kockázatot hordoz magában, amellyel kapcsolatban megállapítható, hogy a kockázat

minimalizálása érdekében a felhasználóknak a lehető legtudatosabb viselkedést kell fenntartania. A különböző szereplők az ilyen alkalmazások által olyan metaadatokhoz juthatnak hozzá, amellyel következtetni lehet a felhasználó fogyasztási szokásaira, kapcsolati körére, annak struktúrájára. A kutatás során feltártak szerint a felhasználói tudatosság egyik módszere lehet a kockázatmenedzsment folyamata, azonban le kell szögezni, hogy a biztonságtudatos felhasználói magatartás sem nyújt százszázalékos védelmet a nem kívánt adatgyűjtéssel szemben. A kockázatmenedzsment mint komplex folyamat rutinszerűvé tétele az ember életében nagyban hozzájárulhat a különböző mobilapplikációk által végrehajtott, nem kívánt adatgyűjtés visszaszorításában.

Felhasznált irodalom

Abonyi János – Fülep Tímea: *Biztonságkritikus rendszerek.* Pannon Egyetem, 2014. Online: http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/

Bahtit, Hanane – Boubker Regragui: Risk Management for ISO 27005 Decision support. *International Journal of Innovative Research in Science, Engineering and Technology,* 2. (2013), 3. 530–538. Online: www.ijirset.com/upload/march/1_Risk%20Management%20for%20ISO%2027005.pdf

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatása. In Kállai Attila – Krajnc Zoltán – Kristóf Zoltán – Szűcs Pál – Kalmár István – Csengeri János – Szabó Csaba – Horváth Tibor – Katona Zoltán – Varga Zsolt et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése (Tanulmánygyűjtemény I., e-book)*. Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673.

Bányász Péter: Az okos mobil eszközök biztonsága. *Hadmérnök,* 13. (2018a), 2. 360–377. Online: http://real.mtak.hu/94336/1/182_25_banyasz.pdf

Bányász Péter: Social Engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018b), 1. 2–19. Online: https://doi.org/10.32561/nsz.2018.1.4

Erdős Gabriella: *Néhány gondolat az adatbiztonságról és az adatkezelésről az okos alkalmazások területén.* Budapest, Corvinus Egyetem, 2020.

Fehér-Polgár Pál – Beerger Michel: A sajáttulajdonú mobil eszközök információbiztonsági kockázatai. *International Journal of Engineering and Management Sciences,* 3. (2018), 4. 176–185. Online: https://doi.org/10.21791/IJEMS.2018.4.16.

Halczmann Attila: Kockázatmenedzsment követelménye irányítási rendszerekben. *International Journal of Engineering and Management Sciences,* 3. (2018), 3. 314–323. Online: https://doi.org/10.21791/IJEMS.2018.3.26.

Horváth Péter – Németh Edit: *Integrált kockázatkezelési rendszer alapjai.* Budapest, Dialóg Campus, 2018. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12824/651_integralt_kockazatkezelesi_rendszer.pdf; jsessionid=BDD265F0BBC90AE65A614A8185A72E86?sequence=1

Horváth Zsolt – Kocsis István: A CRAMM módszer alkalmazásának kiterjesztése. In *Proceedings of 8th International Engineering Symposium at Bánki.* Budapest, Óbudai Egyetem, 2016. 1–6.

Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom,* 17. (2017), 1. 55–71. Online: https://doi.org/10.22503/inftars.XVII.2017.1.4

Kovács László – Bednarik László: Digitális dokumentumok formátumai és az XSLT-FO. In Berke József (szerk.): *Multimédia az oktatásban konferencia.* Nyíregyháza, MTESZ Neumann János Számítógép-tudományi Társaság, *CD kiadvány,* 2010.

Resperger István: Biztonsági kihívások, kockázatok és fenyegetések 2030-ig. In Kobolka István (szerk.): *Nemzetbiztonsági alapismeretek.* Budapest, Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 31–33.

Székely Csaba: Stratégiai kockázatmenedzsment. *Taylor,* 7. (2015), 1–2. 103–118. Online: http://acta.bibl.u-szeged.hu/36270/1/vikek_018_019_103-118.pdf

Vizi Pál: Okostelefonok biztonsági kihívásai. *Hadmérnök,* 6. (2011), 3. 131–141.

Jogi források

2012.évi C. törvény a Büntetőtörvénykönyvről

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 157–168.
DOI: 10.32567/hm.2021.4.12

Nimsz Vivien[1]

A társkereső applikációk biztonsági kockázatai

The Security Risks of Dating Applications

Az ember társas lény, a digitális világ pedig újabbnál újabb megoldásokat kínál arra, hogy a felhasználók internetes felületen találják meg az ideális társat. Az információs társadalomban az online párkeresés jelenségéről és lehetőségéről mindenki tud, azonban a felhasználók közül csak kevesen beszélnek róla nyíltan, gátlások nélkül. Milyen veszélyekkel járhat a túlzott társkeresőalkalmazás-használat és a kevésbé biztonságtudatos attitűd? Lehetnek-e hatással a tárkereső alkalmazásokon közétett személyes adatok a leendő hivatásos állomány tagjainak karrierútjaira? Kutatásom során főként ezekre a kérdésekre kerestem a választ, amelynek során a Nemzeti Közszolgálati Egyetem tisztjelölt és civil hallgatóinak hozzáállását vizsgáltam, többek között információbiztonsági szempontból. A tanulmánnyal fel szeretném hívni a leendő közszférában dolgozó, társkereső alkalmazásokat igénybe vevő felhasználók figyelmét az adatbiztonság jelentőségére, a biztonságos attitűd fontosságára, és arra, hogy karrierjük előtt igazán érdemes körültekintően és megfontoltan dönteni a saját magukról publikált adatokkal kapcsolatban, különös tekintettel az esetleges visszaélések alapját képező különleges adatokra.

Kulcsszavak: információbiztonság, adatvédelem, social engineering, tudatosítás, társkereső alkalmazások

Humans are social beings. The digital world always provides newer solutions to find the ideal partner. In the information society everyone knows about the phenomenon and possibility of online dating, but few users talk about it openly, without inhibitions. What are the dangers of overuse and a less safety-conscious attitude? How can published personal data affect the career path? In order to find the answers to these questions, I examined the attitudes among the students of the University of Public Services. With this study, I would like to draw attention to the importance of data security and a secure attitude among the users who work or are going to work in the public sector.

[1] Nemzeti Közszolgálati Egyetem, hallgató, e-mail: nimszvivi@gmail.com

Keywords: **information security, data protection, social engineering, awareness, dating applications**

1. Bevezetés

Az információs társadalom és a digitális világ olyan gyökeres változásokat hozott az emberek mindennapi szokásaiban, amelyek hatást gyakorolnak többek közt az emberi kapcsolatokra, a viselkedési normákra és az ismerkedési szokásokra egyaránt. Általánosságban elmondható, hogy a digitális eszközök befolyása egyenesen arányos a digitális infrastruktúra fejlettségével. A közösségi oldalak folyamatos elterjedésével egy időben a felhasználók temérdek mennyiségű adathalmazt kezdtek megosztani a világhálón, mit sem sejtve a lehetséges kockázatokról, fenyegetettségekről. Az általános adatvédelmi rendelet[2] (*General Data Protection Regulation,* GDPR) új fejezethez lendítette az internetes kultúrát mind felhasználói, mind szolgáltatói aspektusból, azonban ettől függetlenül megállapíthatjuk, hogy a felhasználók többsége kevésbé érzékeny az adat- és információbiztonságára, így a növekvő internethasználat következtében rengeteg információt lehet összegyűjteni a kevésbé biztonságtudatos személyekről, legyen szó preferenciáikról, kapcsolati hálójukról, aktuális tartózkodási helyükről.[3] Ezen adatok, metaadatok idegen kézbe kerülése számottevő hátrányokat, károkat okozhat mind magánéletünk, mind karrierünk szempontjából. Továbbá fontos megemlíteni azt is, hogy gyakran párosul az állampolgárok alacsony felhasználói tudatossága mellé egyfajta kíváncsiságérzet, amely arra ösztönzi a jóhiszemű felhasználókat, hogy a mulatságos, ámde értelmetlen és kattintásvadász linkeket megnyissák. Ez a tevékenység egyúttal egyenes utat jelenthet ahhoz, hogy valaki social engineering támadás áldozatává váljon. A *social engineering* a kibertámadásoknak egy olyan típusa, amely során a támadók a humán tényezőn keresztül férnek hozzá a védett informatikai rendszerekhez, védekezni mégis rendkívül nehéz ellene, hiszen ehhez a legkevésbé változtatható tényezőt, az emberi személyiséget kellene megváltoztatni.[4]

Kutatásom középpontjában az Y és a Z generáció mindennapi szokásai közé befurakodó tárkereső alkalmazások állnak. De mit is nevezhetünk tárkereső alkalmazásoknak? A szakirodalom nem rendelkezik egységesen kialakított fogalomrendszerrel, így a meghatározást több publikáció álláspontja alapján ismertetem. Társkereső alkalmazásnak nevezzük azokat az applikációkat, amelyekre a felhasználók főképp – de nem kizárólag – párkeresés céljából regisztrálnak. A tárkereső alkalmazások általában sajátos algoritmussal rendelkeznek, amelyek segítségével a felhasználók által megosztott adatok és információk alapján ajánlanak fel potenciális partnereket.[5] Ezt

[2] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.

[3] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36.

[4] Bányász Péter: Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77.

[5] Francesca Comunello – Lorenza Parisi – Francesca Ieracitano: Negotiating Gender Scripts in Mobile Dating Apps: Between Affordances, Usage Norms and Practices. *Information, Communication & Society,* 24. (2021), 8. 1140–1156.

a fajta algoritmust gondolta tovább a *Fekete tükör* (ismertebb angol nevén: *Black Mirror*) elnevezésű televíziósorozat is a 4. évad 4. részében. Az epizód során a rendszer beállítottság és érdeklődési kör alapján választotta ki a legmegfelelőbb párosításokat, de a felek még képen sem látták egymást az első találkozóig. A sorozatban prezentált rendszer több ponton is elrugaszkodik a valóságtól, szinte már a valódi társkereső alkalmazások paródiájaként bukkant fel, azonban a készítők által bemutatott algoritmus emlékeztet a való életben alkalmazott algoritmusokra.

Napjainkban a tárkereső alkalmazások elsődleges célja, hogy első körben virtuális köteléket, azt követően pedig az offline térben is megvalósuló kontaktot alkossanak két fél között az online térben létrejövő írásbeli kommunikáció segítségével.[6] Ezek az applikációk szenzitív adatok sokaságát várják el tőlünk a használatért cserébe. Az átlagfelhasználó logikusan gondolhatja azt, hogy minél többet oszt meg saját profilján magáról, annál hatékonyabban vetheti bele magát a párkeresésbe, azonban az online tér tartogathat némi meglepetést az óvatlan felhasználók számára. Első hangzásra nem tűnhet olyan kockázatosnak személyes adatokat megosztani magunkról az internetes platformokon, vagy akár az online beszélgetéseinkben, azonban számos veszéllyel járhat. Olykor az emberek nem is gondolják, mennyire könnyen válhatnak adatlopás vagy egyéb más támadás áldozatává, továbbá, ha esetlegesen konkrét személy befolyásolása lenne a támadók fő célpontja, mi más jelenthetne optimális megoldást, mint a társadalom által gyakran tabutémaként kezelt társkereső alkalmazások nyújtotta nyílt forrású információgyűjtés, amellyel nagymértékben nő a felhasználói profillal rendelkezők körében a profilozás és zsarolás kockázata is.

Az OSINT[7] történetében új fejezetet nyitott a közösségi és társkereső oldalak megjelenése, hiszen meglehetősen átalakították, kiegészítették a hagyományos médiumokból történő hírszerzést.[8] De hogyan történhet meg a nyílt forrású információszerzés alkalmazása az egyik legnépszerűbb társkereső alkalmazáson, a Tinderen? Az applikáció alapvetően csak a felhasználók keresztnevét mutatja, de ha nem vagyunk elég körültekintőek, hamar kinyomozhatókká vállhatuk más platformokon egyaránt. Ennek egyik példája lehet az Instagram, amelyet szintén Tinderes profilunkhoz csatolhatunk. Az Instagramos profilok gyakran a felhasználó valós nevét tartalmazzák, ily módon akaratlanul is valós nevünkkel szerepelhetünk, ha figyelmetlenek vagyunk. Az oktatási intézmény, munkahely megadásával adatvédelmi szempontból nagymértében növeljük sebezhetőségünket, de az azonos profilkép használata is könnyítést jelenthet egy esetleges virtuális „kukkolónak".

A helyzetmeghatározásra támaszkodó applikációk nagy gyakorisággal jelennek meg mindannyiunk okostelefonján, de manapság már egyre több weboldal is engedélyt kér helyzetünk használatához. A helyzetmeghatározást használó felületek valóban kényelmesebbé, gyorsabbá tudják tenni internetes böngészésünk folyamatát, gondoljunk csak az étel-házhozszállítással foglalkozó platformokra, amelyek listázzák számunkra a legközelebbi éttermeket, de akár az e-közszolgáltatásokat nyújtó

[6] Randy Jay C. Solis – Ka Yee J. Wong: To Meet or Not to Meet? Measuring Motivations and Risks as Predictors of Outcomes in the Use of Mobile Dating Applications in China. *Chinese Journal of Communication,* 12. (2019), 2. 204–223.

[7] *Open source intelligence,* azaz nyílt forrású információszerzés.

[8] Bányász (2015): i. m.

mobilapplikációkat is idesorolhatjuk. A helyzetmeghatározáson kívül elterjedt metódusnak számít az a megoldás, amelynek során az applikációk Bluetooth használatával cserélnek kódot, kommunikálnak egy esetleges másik készülékkel. Ilyen módszerrel működik például a koronavírus-járvány során fejlesztett VírusRadar applikáció, amely a hatóságokat segítette kontaktkutatás alkalmával.[9] Ezek a megoldások, technológiák kényelmet tudnak biztosítani mindennapi életünkben, azonban a komfortot, nem mindig múlja felül a biztonságérzetünk.

A társkereső alkalmazások gyakorta egyfajta relevancián alapulnak. Korábban a már emlegetett közös érdeklődési kör jelentette az alapkövet – amelyet a regisztrációnál egyfajta kérdőívvel mértek –, azonban manapság releváns információnak számít a felek lokációja is. Három olasz kutató, Adriano Di Luzio, Alessandro Mei, Julinda Stefa – nem túl etikus módon – vette a bátorságot és letesztelte, hogy mekkora mértékű gondot jelent a Happn nevezetű társkereső alkalmazásról adatokhoz jutni illegális módon. A Happn szintén helyzetmeghatározásra alapozó applikáció, amelynek célja, hogy a felhasználók tudomást szerezzenek arról, hogyha egymás közelében tartózkodnak. A kutatók úgynevezett közbeékelődéses támadást *(man-in-the-middle attack)* produkáltak, amelynek során két fél közé (jelen esetben a felhasználó és a Happn alkalmazás) betolakodik egy harmadik fél is. Az ilyen és ehhez hasonló támadások során az alkalmazások és a weblapok azt hiszik, hogy a valós végponttal, azaz a felhasználóval kommunikálnak, a felhasználó pedig szintén azt hiszi, hogy csupán az alkalmazás számára szolgáltat adatokat. A kutatóknak sikerült ily módon, Róma területén több mint 10 000 ember adatait begyűjteni. A tanulmány végén hangsúlyozták, hogy harmadik félnek nem adták ki ezeket a személyes adatokat, illetve azokat a kutatás végéig egy titkosított adatbázisban tárolták, majd a kutatás végén mindet megsemmisítették.[10]

2018-ban egy izraeli információbiztonsággal foglalkozó cég által fény derült arra, hogy a Tinder-felhasználók minimális adat megosztásával is könnyen válhatnak megfigyelés, zsarolás áldozatává, ez pedig betudható annak a ténynek, hogy a Tinderen tárolt fotókat nem titkosított csatornán továbbítják. De hogyan is lehet ezt a biztonsági rést kihasználni? Aki közös wifihálózatra van csatlakozva a megfigyelni kívánt emberrel, nemcsak láthatja a képeket, hanem azt is megtudhatja az adatforgalom követésével, hogy kiket húzott jobbra, illetve kiket balra, és mikor van az illetőnek találata. (Az alkalmazáson belüli szimpátiát a jobbra pöccintéssel lehet kifejezni, ha pedig nem szeretnénk az adott felhasználóval kapcsolatba kerülni, balra kell húzni a profilt.) Ezzel a módszerrel kideríthető, hogy a megfigyelt személynek kik tetszenek, ezáltal pedig egyenes út vezethet egy esetleges érzelmi zsaroláshoz.[11] A szervezet demonstrálásképp megalkotott egy szoftvert, amely működés közben ezt a biztonsági rést vette alapul, és bemutatta azt a Tinder fejlesztőinek.[12]

[9] Attila Német – Sándor Magyar: An Investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible National Security application (PART1). *National Security Review Issue,* (2020), 2. 52–64.

[10] Adriano Luzio – Alessandro Mei – Julinda Stefa: Uncovering Hidden Social Relationships through Location-based Services: The Happn case study. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2018. 802–807.

[11] Tóth Balázs: Titkosítás nélkül pörögnek a képek a Tinderen. *Index.hu,* 2018. január 24.

[12] Andy Greenberg: Tinder's Lack of Encryption Lets Strangers Spy on Your Swipes. *Wired,* 2019. január 23.

Nem véletlen a mondás, miszerint információbiztonság szempontjából az ember a leggyengébb láncszem. Befolyásolhatóság, kíváncsiság, manipulálhatóság erőteljes emberi jellemzők. Ezek az emberi tulajdonságok mind-mind hozzájárulnak a social engingeering alapú támadások sikerességéhez. A social engineering során a bűnözök az információbiztonságot nem, vagy csak kevésbé ismerő, vakon együttműködő személyektől szereznek információt. Ezek az értesülések később gyakran akár védett rendszerekhez történő hozzáférés kulcsaként szolgálnak, vagy csak egyszerűen megkönnyítik a jogtalan hozzáférést.[13] A social engingeeringen belül megkülönböztethetünk két válfajt: a humán alapú támadásokat és az informatikai alapú támadásokat.[14] A humán alapú támadások kapcsán szóba jöhet például számos olyan példa, amelynek során az emberek érzelmeire próbál a támadó hatni. Így történt ez már a 2000-es évek elején is, amikor Anna Kurnyikova orosz teniszsztár állítólagos szerelmes levele terjedt el világszerte. A levél szövegében pikáns képeket ígértek a sportolóról, ám ez természetesen nem volt elérhető az ígért linken.[15] Ez a fajta „szerelmeslevél" ugyan maradandó károkat nem okozott azoknak, akik megnyitották, azonban kiváló módon szemlélteti, hogy olykor milyen olcsó trükkökkel lehet rávenni a mit sem sejtő felhasználót a kattintásra. Ezek alapján nem nehéz levonni a következtetést, hogy aki 2021-ben az érzelmeket kihasználva szeretne adatokhoz és információkhoz jutni, nagy eséllyel fordul a társkereső alkalmazásokhoz.

A social engingeering mint támadási forma megjelent már a társkereső alkalmazások vonatkozásában a hadműveleti területeken is. A Hamasz palesztin szervezet megbízásából tevékenykedő hackereknek az Izraeli Védelmi Erőknél (IDF) szolgáló katonák százait sikerült megvezetni dekoratív hölgyek képeivel, ennek eredményeképp az izraeli katonák egy alkalmazást töltöttek le eszközeikre, amelynek segítségével a palesztinok hozzáfértek a teljes mobiltelefon-készülékhez és a tartózkodási helyhez.[16] Ebben a példában a hadszíntéren használták ki az ellenfél kevésbé biztonságtudatos attitűdjét. Az Egyesült Államokban egy csalási hullám keretein belül több száz gyanútlan civil felhasználót sikerült átvernie azoknak a bűnözőknek, akik katonáknak adták ki magukat. A támadók főképp szenzitív üzenetekkel, az érzelmekre hatva jutottak el trükkösen odáig, hogy a felhasználók pénzt utaljanak nekik.[17]

2. Módszerek

A fentiekben bemutatott támadási formák, sérülékenységek rendkívül jól prezentálják, hogy a társkereső alkalmazások biztonsági kockázataival igenis szükséges foglalkozni. Mindezekre tekintettel kutatásomban a társkereső applikációk felhasználóinak motivációját, szokásait, hozzáállását vizsgáltam többek közt információbiztonsági szempontból,

[13] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37.

[14] Bányász–Bóta–Csaba (2019): i. m.

[15] Kurnyikova, a féregvírus. *Index.hu,* 2001. február 13.

[16] Molnár Csaba: Dekoratív hölgyek képével verték át a Hamász hekkerei az izraeli katonákat. *Index.hu,* 2020. február 17.

[17] Barb Chiles: Military Romance Scams: Are You a Target? *Military.com,* (é. n.).

a Nemzeti Közszolgálati Egyetem (NKE) hallgatóinak körében. Vizsgálódásom során két hipotézist fogalmaztam meg, amelyek a következők:

H1: Az NKE hallgatói jellemzően unalomból és szórakozásból regisztráltak társkereső alkalmazásokra, nem a párkeresés volt a fő cél.

H2: A NKE hallgatói nagyobb százalékban vallják magukat biztonságtudatosnak adatvédelmi szempontból, mint sem.

Munkám egyik központi elemét az általam készített kérdőív jelentette, amelyet csak és kizárólag a NKE hallgatói tölthettek ki. Felmérésem azért korlátozódott az NKE hallgatóinak körére, mert feltételezem, hogy a kitöltők egyetemi tanulmányaik elvégzését követően az állami szférában fognak munkát vállalni, akár a hivatásos állomány tagjaként, akár a civil állomány részeként, így amennyiben ezek a hallgatók nem részesülnek olyan, az adat- és információbiztonsági tudatossággal kapcsolatos oktatásban, amelynek segítségével felismerhetik a fenyegetéseket, magas fokú kockázatot jelentenek az őket foglalkoztató szervezet számára.[18]

A kérdéssor három részből állt, a kitöltők a demográfiai adatok megadásával kezdhették a válaszadást, itt főképp az életkort, a legmagasabb végzettséget, és azt vizsgáltam, hogy melyik kar hallgatója az adott illető. Ezt követően a társkereső alkalmazásokon felbukkanó jellemző viselkedési formákra, attitűdökre vonatkozó kérdések következtek, majd végül a harmadik részben adat- és információbiztonsági tudatossággal kapcsolatos kérdésekkel zárult a kérdőív.

Kérdőívem második részéhez és az interjúm során egyaránt Rhiannon B. Kallis *Understanding the Motivations for Using Tinder* című kutatásában szereplő felmérést ismételtem meg.[19] Empirikus vizsgálatában főképp nyitott kérdésekkel dolgozott, de zárt kérdések is felbukkantak. A kapcsolatot e-mailben vettem fel a szerzővel, amelynek során kifejtettem kutatásom célkitűzéseit, kérésemre még aznap választ kaptam. A harmadik részhez Kathryn Parsons és szerzőtársai 2017-ben végzett kutatásához kapcsolódó kérdőívét használtam fel, amelyet teljes egészében publikáltak a cikkben.[20] Ebben az írásban Tudás–Képesség–Viselkedés modell segítségével mérték fel a kitöltők kompetenciáit. Ez alapján a „Tudáshoz" soroljuk az ismeret jellegű elemeket (elvek, elméletek, tények ismeretét). A „Képesség" a „Tudás" alkalmazásának képességét jelöli, amelynek során az egyén megoldja a felmerülő problémákat. A „Viselkedés" a tényleges viselkedésformákat jelenti. A tudásra vonatkozó kérdések esetében a „tudom", „ismerem", „megértem", „azonosítom", „felismerem" jellegű állításokat, a képességre vonatkozó kérdések esetében a „képes vagyok felismerni", „képes vagyok figyelembe venni" stb. jellegű állításokat, míg a viselkedésre vonatkozó kérdések esetében „tudatosan használom", „törekszem" stb. típusú állításokat fogalmaztam meg.[21]

[18] Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2018.

[19] Rhiannon B. Kallis: Understanding the Motivations for Using Tinder. *Qualitative Research Reports in Communication,* 21. (2020), 1. 66–73.

[20] Kathryn Parsons et al.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers & Security,* 66. (2017), 40–51.

[21] Bányász (2019): i. m.

A kérdőíven felül fókuszcsoportos interjúkat végeztem, amellyel célzottan vizsgáltam hallgatótársaim motivációját a regisztrációhoz, attitűdjét az alkalmazás használata közben, és azt, hogy milyen adatokat osztanak meg az applikáció hatékony, sikeres használata érdekében. A fókuszcsoportos interjúk során minden karról meghallgattam három nő és három férfi hallgatótársamat, ezt követően pedig kontrollcsoportként vizsgáltam más felsőoktatási intézmények hallgatóinak hozzáállását is.

Kutatási eredményeim szöveges, statisztikai kiértékeléséhez Sajtos László *SPSS Kutatási és adatelemzési kézikönyv*ét hívtam segítségül. A válaszok értékelése során kereszttábla-elemzést alkalmaztam, amely széles körben elterjedt módszernek számít. Két vagy több változó közötti összefüggést vizsgál, illetve ezek kombinált gyakoriságát, eloszlását mutatja. Az elemzés során azt vizsgáljuk meg, hogy két nominális vagy ordinális változó kapcsolatban áll-e egymással, máshogy magyarázva a kereszttábla-elemzés nem más, mint két gyakoriságelemzés együttes vizsgálata két nem metrikus változó esetében. A kereszttáblával kapcsolatos statisztikák közül talán leggyakrabban használt a Pearson-féle khi-négyzet, amely a két változó összefüggésének szignifikanciáját méri. A mutatószám alapján megállapítható, hogy van-e statisztikai összefüggés a két változó között.[22] A khi-négyzet próba feltétele, hogy az elvárt gyakoriság minden egyes cellában minimum 5 kell legyen. A khi-négyzet próbán kívül elemzésem során figyelembe vettem még a Cramer's V együtthatót, amely egy asszociációs együttható és két nominális változó közötti kapcsolat szorosságát mutatja meg. Az érték 0 és 1 közötti intervallumban van, minél közelebb áll az 1-hez, annál erősebb statisztikai kapcsolatról beszélhetünk.[23]

3. Eredmények

A kérdőívemet összesen 198-an töltötték ki (n = 198), azonban fontos megemlíteni, hogy nem minden kérdésnél lehetett a válaszadást kiértékelni, ezért az egyes kérdések elemzésénél adattisztogatást végeztem (erről bővebben a továbbiakban fogok szólni). A kérdőív teljesen anonim formában volt elérhető. A válaszadók között 121 nő és 77 férfi volt. A kitöltők 86,4%-ának érettségi a legmagasabb végzettsége, 11,6%-nak alapszakos diploma, 1,5%-ának mesterszakos diploma és 0,5%-nak doktori fokozat. A legtöbb kitöltésszámról a karok megoszlásában az Államtudományi és Nemzetközi Tanulmányok Kar (ÁNTK) esetében beszélhetünk, számszerűsítve 69,2%. Az összes kitöltésszám (n = 198) 18,7%-át jelenti a Hadtudományi és Honvédtisztképző Kar tisztjelölt és civil hallgatóinak kitöltése, 11,6%-át a Rendészettudományi Kar hallgatói, 0,5%-át pedig a Víztudományi Karról érkezett 1 db kitöltés.

A H1 hipotézisem szerint a társkereső alkalmazások felhasználói jellemzően unalomból és szórakozásból regisztrálnak, nem a párkeresés a fő cél. A hipotézis vizsgálata közben kérdőívem kilencedik kérdését elemeztem IBM SPSS Statistics

[22] Sajtos László – Mitev Ariel: *SPSS kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.
[23] Khi-négyzet próba jelentése és alkalmazása az SPSS-ben: https://spssabc.hu/ketvaltozos-elemzes/khi-negyzet-proba

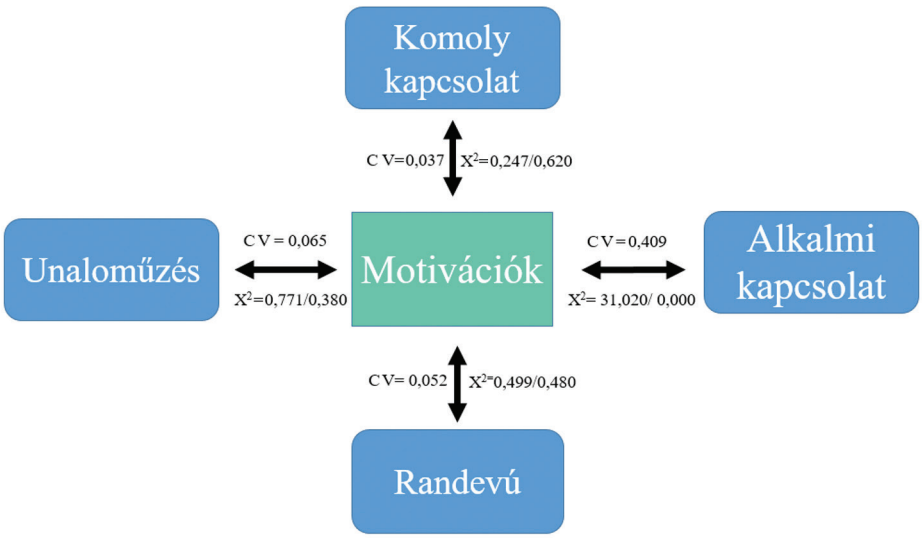
24 nevezetű programmal, amely így szól: Mi motiválta arra, hogy regisztráljon társkereső alkalmazásra?

A válaszok kiértékelése során a fentebb említett kereszttábla-elemzést alkalmaztam, szám szerint négyet, mivel négy különféle lehetséges opciót lehetett választani a válaszadás során, a kitöltők több motivációt is bejelölhettek válaszként. Ötödik opcióként megjelent az „egyéb" rovat, amelyben rendszerint komolytalan válaszok érkeztek, így végül ezt az opciót nem értékeltem ki. A motivációk esetében a nemmel összefüggésben vizsgáltam a kapott adatokat. Az összes, 198 kitöltés helyett 185 (n = 185) válaszadást tudtam értékelni. Az első vizsgálatom arra vonatkozott, van-e összefüggés a nemek és a között, hogy komoly kapcsolat szerzése érdekében regisztrált-e a platformra a kitöltő. A khi-négyzet teszt (x^2 = 0,247; df = 1) kétoldali szignifikanciaszintje 0,620, tehát nincs statisztikailag szignifikáns kapcsolat a két változó között, mivel a kétoldali szignifikanciaszint nem nagyobb mint 0,05. Ezt követően Cramer's V (C V) mutató segítségével is vizsgálódtam. Ahogy már említettem, C V mutató esetén a nullához való közelség függetlenséget, míg az egyhez való közelség erős kapcsolatot jelent a két változó között. Ebben a példában a következőképp alakult: A C V mutató értéke 0,037, ezáltal kijelenthetem, hogy a meglehetősen gyenge a két változó közötti kapcsolat.

Sorban a következő választási lehetőségként a „randevúk miatt regisztráltam" menüpontot adtam meg, az elemzés menete azonos volt. A khi-négyzet teszt (x^2 = 0,499; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,480, tehát statisztikailag szignifikáns kapcsolatról megint nem tudunk beszélni. A C V mutató értéke 0,052, tehát szintén gyenge kapcsolatot tudtam megállapítani.

A harmadik vizsgálatom bizonyult statisztikai szempontból a legizgalmasabbnak, amelynek során azt elemeztem, hogy a válaszadók neme és az „érzelemmentes alkalmi kapcsolat kialakítása céljából regisztráltam" opciót választók között van-e összefüggés. A khi-négyzet teszt (x^2 = 31,020; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,00, tehát statisztikailag szignifikáns kapcsolatról tudunk beszélni, vagyis a válaszadók neme befolyásolta azt, hogy érzelemmentes alkalmi kapcsolat motiválta a regisztrációra vagy sem. C V mutató értéke 0,49, tehát közepes kapcsolatot tudunk megállapítani a két változó között.

Végül, de nem utolsósorban analizáltam az „unaloműzésképpen regisztráltam" elnevezésű választási lehetőséget is a nemek vonatkoztatásában. A Khi-négyzet teszt (x^2 = 0,771; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,380, tehát ebben az esetben sem tudunk statisztikailag szignifikáns kapcsolatról beszélni, vagyis a válaszadók neme nem befolyásolta azt, hogy az unaloműzés motiválta a regisztrációra, vagy sem. C V mutató értéke 0,065, tehát gyenge kapcsolatot tudunk megállapítani a két változó között. A négy vizsgált motivációt összesítve az 1. számú ábrán mutatom be. Összegezve elmondható, hogy statisztikailag szignifikáns kapcsolatról tudunk beszélni az érzelemmentes alkalmi kapcsolat kialakításából eredendő motivációk és a nemek között, ezáltal igazoltam a H1 hipotézisemet.



1. ábra

Mi motiválta arra, hogy társkereső alkalmazásra regisztráljon?

Forrás: a szerző szerkesztése

Ezt követően a H2 hipotézisemre vonatkozóan végeztem vizsgálatot. H2 hipotézisem így hangzik: Az NKE hallgatói nagyobb százalékban vallják magukat biztonságtudatosnak adatvédelmi szempontból, mint sem. A korábbiakban már említett Tudás–Képesség–Viselkedés modell segítségével tettem fel kérdést H2 hipotézisemre tekintettel, amely így hangzott: Biztonságtudatosnak gondolja-e magát adatvédelmi szempontból? A válaszadók (n = 198) 75,8%-a gondolja magát adatvédelmi szempontból biztonságtudatosnak, míg 24,2%-a nem, ezzel H2 hipotézisemet alátámasztottam, továbbá vizsgáltam még a változók közti statisztikai kapcsolatokat, a nemmel összevetve. A Khi-négyzet tesztet itt is elvégeztem, amelynek eredménye statisztikailag szignifikáns kapcsolatról nem tudott beszámolni. (x^2 = 0,013; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,910, vagyis a válaszadók neme nem befolyásolta azt, hogy adatvédelmi szempontból biztonságtudatosnak vallották magukat a kitöltők, vagy sem. A C V mutató értéke 0,008 tehát nagyon gyenge kapcsolatot tudunk megállapítani a két változó között.

Érdekességképp megkérdeztem hallgatókat, hogy hallgattak-e az egyetemen adat- és/vagy kiberbiztonsági tudatossággal kapcsolatos kurzust (n = 198)? A válaszadók 57,6%-a nyilatkozta azt, hogy hallgatott korábban ezzel kapcsolatos kurzust, míg 42,4% nyilatkozta azt, hogy nem. Az interjúk végén megállapítottam, hogy kötelező óra keretein belül főképp a tisztjelölt hallgatóknak volt lehetőségük ilyen kurzuson részt venni, az ÁNTK hallgatói inkább szabadon választható tantárgy keretein belül tanulhattak adat- és/vagy kiberbiztonsági tudatosságról.

A kérdőívben szintén a Tudás–Képesség–Viselkedés modell segítségével mértem fel kitöltőim hozzáállását az információk online közlésével kapcsolatosan. Az arányok

a következőképp alakultak (n = 198): a kérdezettek 73,2%-a nyilatkozta azt, hogy mindig ellenőrzi egy weboldal megbízhatóságát, mielőtt információt közölne azon, 15,2% mondta azt, hogy amennyiben segíti a tanulásban, munkavégzésben, nem lényeges, hogy milyen információt közöl egy weboldalon, és a maradék 11,6% választotta azt az opciót, miszerint tudja, hogy rendben van mindenféle információ közlése a különböző weboldalakon, amennyiben az segít a tanulásban, munkavégzésben.

4. Következtetések

Munkám arra próbál rávilágítani, hogy a társkereső alkalmazások használatához rendszerint párosul kevésbé biztonságtudatos attitűd, amely elősegíti az esetleges támadások hatékonyságát.

T1 tézisem igazolta, hogy az NKE hallgatói körében a motivációt nem kizárólag a konkrét társkeresés jelenti, T2 tézisem pedig alátámasztotta, hogy az NKE diákjai nagyobb arányban vallják magukat biztonságtudatosnak adatvédelmi szempontból, mint sem. A kérdőív és az interjú más kérdéseit elemezve azt is láthattuk, hogy a válaszadók több mint fele részt vett eddigi tanulmányai során adat- és/vagy kiberbiztonsági tudatossággal kapcsolatos kurzuson, ennek ellenére a hallgatók rendszerint osztanak meg magukról olyan szenzitív adatokat pluszban, amelyeket a társkereső alkalmazások nem várnak el kötelező jelleggel.

Véleményem szerint mindenki számára komoly problémát jelenthet a társkereső oldalakon megosztott túlzott információhalmaz, hiszen ahogyan a korábbiakban szemléltettem, temérdek mennyiségű támadási módszer áll a támadók rendelkezésére, abban az esetben, ha adatokhoz szeretnének jutni illegális módon. Az NKE hallgatóinak különösen nagy figyelmet kellene fordítaniuk személyes adataik kezelésére az online felületeken, mivel nagy valószínűséggel az egyetemi tanulmányaik elvégzését követően az állami szférában fognak munkát vállalni, akár a hivatásos állomány tagjaként, akár a civil állomány részeként. Amennyiben ezek a fiatalok nem részesülnek olyan, az adat- és információbiztonsági tudatossággal kapcsolatos oktatásban, amelynek segítségével felismerhetik a fenyegetéseket, abban az esetben magas fokú kockázatot jelentenek az őket foglalkoztató szervezet számára. Ezért igazán érdemes körültekintően és megfontoltan dönteni a saját magukról publikált adatokkal kapcsolatban.

A biztonsági kockázatokon kívül azonban az a tény sem elhanyagolható, hogy a virtuális térben történő túlzott időtöltés erőteljesen képes befolyásolni személyiségfejlődésünk szakaszait, kialakított önképünk megítélését, illetve általános habitusunkat. A társkereső oldalak fogalmához gyakran párosul negatív sztereotípia, a külföldi szakirodalom számos esetben emlegeti a társkereső alkalmazásokat biológiai piacként, húspiacként. Nem szabad megfeledkeznünk az álprofilok diverzáns hatásairól sem, amelyek szinte minden közösségi médiában jelentkeznek, annak ellenére, hogy ezt az oldalak közösségi irányelvei szigorúan tiltják.

Felhasznált irodalom

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36. Online: https://doi.org/10.32561/nsz.2015.2.2

Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12483/banyasz_peter_doktori_ertekezes_2018.pdf?sequence=1

Bányász Péter: Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77. Online: https://doi.org/10.32561/nsz.2018.1.4

Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Chiles, Barb: Military Romance Scams: Are You a Target? *Military.com,* (é. n.). Online: www.military.com/spouse/military-life/military-romance-scams-are-you-target.html

Comunello, Francesca – Lorenza Parisi – Francesca Ieracitano: Negotiating Gender Scripts in Mobile Dating Apps: Between Affordances, Usage Norms and Practices. *Information, Communication & Society,* 24. (2021), 8. 1140–1156. Online: https://doi.org/10.1080/1369118X.2020.1787485

Greenberg, Andy: Tinder's Lack of Encryption Lets Strangers Spy on Your Swipes. *Wired,* 2019. január 23. Online: www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/

Kallis, Rhiannon B.: Understanding the motivations for using Tinder. *Qualitative Research Reports in Communication,* 21. (2020), 1. 66–73. Online: https://doi.org/10.1080/17459435.2020.1744697

Kurnyikova, a féregvírus. *Index.hu,* 2001. február 13. Online: http://index.hu/tech/net/anna/

Luzio, Adriano – Alessandro Mei – Julinda Stefa: Uncovering Hidden Social Relationships through Location-based Services: The Happn Case Study. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).* 2018. 802–807. Online: https://doi.org/10.1109/INFCOMW.2018.8406866

Molnár Csaba: Dekoratív hölgyek képével verték át a Hamász hekkerei az izraeli katonákat. *Index.hu,* 2020. február 17. Online: https://index.hu/techtud/2020/02/17/izrael_hadsereg_idf_hamasz_hekkerek_adathalasz_atveres_kamu_nok/

Parsons, Kathryn – Dragana Calic – Malcom Pattinson – Marcus Butavicius – Agata McCormac – Tara Zwaans: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers & Security,* 66. (2017), 40–51. Online: https://doi.org/10.1016/j.cose.2017.01.004

Randy Jay C. Solis – Ka Yee J. Wong: To Meet or Not to Meet? Measuring Motivations and Risks as Predictors of Outcomes in the Use of Mobile Dating Applications in China. *Chinese Journal of Communication,* 12. (2019), 2. 204–223. Online: https://doi.org/10.1080/17544750.2018.1498006

Sajtos László – Mitev Ariel: *SPSS kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.

Tóth Balázs: Titkosítás nélkül pörögnek a képek a Tinderen. *Index.hu,* 2018. január 24. Online: https://index.hu/tech/2018/01/24/titkositas_nelkul_porognek_a_kepek_a_tinderen

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 169–182.
DOI: 10.32567/hm.2021.4.13

György Tóth[1]

Electronic Documentation and Digital, IT Technology in Pre-Hospital Emergency Care

In recent years Hungarian healthcare including outpatient and inpatient medical institutions and the Emergency Medical Services providing emergency care have undergone numerous IT improvements. In addition to patient health documentation, electronic digital technology provides a telemedicine opportunity for at-the-scene care, helping and supporting care, diagnosis and patient path-related decisions. The National Emergency Services are involved in the development and implementation of mobile applications that assist at-the-scene first aid provided by non-professionals in cases where early intervention can be life-saving for the patient. By providing the possibility of requesting direct assistance in unexpected situations, not only can the request for assistance be made easier and simpler, but the scene of the medical emergency or injury can also be precisely determined without the assistance of the person who reports the emergency case.

Keywords: **electronic documentation, electronic health service system, electronic case record, Heart City, life-saving application**

1. Introduction

The use of information and digital technology that directly supports not only patient care, but also activities related to care is essential for the development of the quality of health care.

As a research objective, this paper presents the essential elements of health documentation, the advantages and disadvantages of electronic documentation together with its usability in everyday practice, and its additional services compared to paper-based documentation. The hypothesis assumes that electronic patient documentation and digital technology assist at-the-scene care for professionals and can

[1] National Ambulance Services, Northern Great Plain Regional Ambulance Services, Senior Paramedic at the ambulance station; University of Public Service, Doctoral School of Military Engineering, PhD student, e-mail: toth.gyorgy@mentok.hu

also be used by non-professionals. The paper tends to support the hypothesis with international examples. A further aim is to draw attention not only to the present but also to potential applications in the future.

The outdated paper-based documentation, which also means storage, processing and archiving difficulty, has been replaced by electronic patient documentation in pre-hospital emergency care as well. In addition, safe patient care requires a decision-support system that also provides consultation opportunities. This system assists at-the-scene care for professionals and additionally mobile applications provide at-the-scene support from the Emergency Medical Services for non-professionals.

2. Documentation during emergency care

In any field of health care, including out-of-hospital emergency care, medical documentation is prepared on the examination and care of the patient during, after and in parallel with the treatment. According to the law, this documentation is a record or information or data recorded in any way, that contains health and personal information which have come to the knowledge of the person providing care in the course of treatment, regardless of its medium or form.[2]

In the course of documentation, health information is collected about the patient, i.e. all personal information about his or her physical or mental condition, including information on health services provided to the person that carries information about the person's condition, which also means the classified information mentioned above[3] (GDPR Article 4, point 15).

The documentation applied during the emergency task contains the following as a mandatory element in accordance with the legal requirements (Health Act):

- the patients personal identification data
- medical history
- the result of the examination and the diagnosis
- the time of the performed interventions and their results
- medication and other therapies, as well as their results
- information about the patient's drug hypersensitivity
- the name of the healthcare professional who performed the registration and the time of the registration
- any other information and facts that may affect the patient's recovery[4]

The documentation by the Emergency Medical Services outside the hospital was recorded on rescue documentation and travel account before joining the Electronic Health Care System which contained information about the ambulance team, the rescue tasks and the given patient. Detailed information on patient care was recorded on the case record by the head of the ambulance team:

[2] 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről.
[3] Általános adatvédelmi rendelet (GDPR), 4. cikk 15. pont.
[4] 1997. évi CLIV. törvény az egészségügyről.

- the relevant time of the rescue task (reporting of the emergency case, departure, arrival at the scene)
- the history of the event and the conditions observed at the scene
- the patient's condition and the results of the examination
- the treatment provided to the patient, change in his/her condition
- additional treatment provided to the patient and the change in the patient's condition during the transportation
- the place and time of the patient transfer[5]

Additional medical documents, like the Declaration of the Refusal of Patient Care, Inventory of Valuables Police Force Claim Form, and other professional medical information forms (Utstein template, ACS, Intubation) as part of the patient documentation were prepared during the patient care as necessary annexes.

The difficulty of paper-based documentation was the necessary administration at the scene, during transportation, or at the transfer destination of the patient, thus they greatly affected the readability of the documents. In addition, the proper storage of patient records was an ongoing issue.[6]

3. Introduction of electronic documentation and the related IT system during the at-the-scene emergency care

In the emergency patient care outside the hospital the introduction and application of electronic patient documentation was implemented with the nationwide extension of the EESZT (Electronic Health Service System), involving healthcare providers in the system. Its deadline was 1 November 2018.

A dispatcher IT system has been operated by the National Emergency Medical Services since 2014. With the help of this system different information of the incoming emergency calls, e.g. the exact location of the emergency case, contact information of the person reporting the medical emergency, the patient's name, his or her current complaint, etc. are stored on an electronic rescue documentation, which can immediately be transmitted to the Intelligent On-Board Terminal (IFT) of the given ambulance team.

An important part of the dispatcher system is the electronic rescue documentation opened by the dispatcher at the time of reporting the medical emergency. It contains all the important information from information gathered from the person reporting the medical emergency (Figure 1). The dispatcher is assisted by the protocol of questions, which, when it is opened in parallel with the rescue documentation, follows the individual steps of the at-the-scene patient examination, so that in a short time sufficient information can be obtained about the patient's condition and adverse health effects.

[5] 37/2011. (VI. 28.) NEFMI rendelet a mentésről szóló 5/2006. (II. 7.) EüM rendelet és a betegszállításról szóló 19/1998. (VI. 3.) NM rendelet módosításáról.

[6] Gábor Csató, 'Modernitás a mentőszolgálatban: Mitől lesz modern egy egészségügyi intézmény?', Interdiszciplináris Magyar Egészségügy 16, no 5 (2017), 6–7.

If a patient requires immediate intervention (e.g. resuscitation, provision for an unconscious patient, hemostasis, foreign body in the respiratory system), the dispatcher stays on the phone and provides first aid advice to the person who is reporting the medical emergency and who is still at the scene until professional help arrives. Protocols for telephone assistance are also available which can be used during first aid counselling (Figure 2).[7]

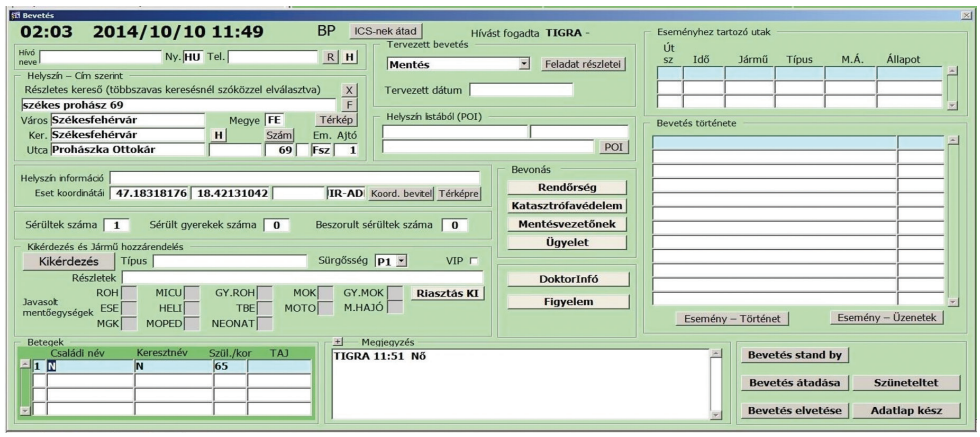


Figure 1

Electronic rescue documentation

Source: http://demin.hu/files/userfiles/DEMIN_XV/DEMIN-XV-E/2-1-2-DEMIN-XV-PGY-1.pdf

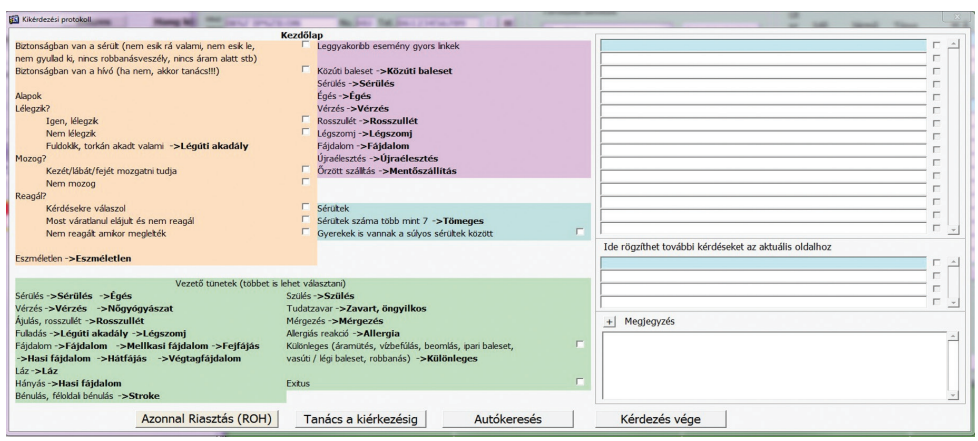


Figure 2

Protocol for dispatchers to ask questions

Source: http://demin.hu/files/userfiles/DEMIN_XV/DEMIN-XV-E/2-1-2-DEMIN-XV-PGY-1.pdf

[7] György Pápai, Új minőségbiztosítási feladatok az OMSZ-nál 2, s. a.

Within the dispatcher system, the GIS (Geographic Information System) application supports the identification of the scene. It helps the arriving ambulance team to reduce the arrival time, and the GPS transmitter in the ambulance identifies the current location of the ambulances, alerting the deployable ambulance team closest to the reporting location (Figure 3).

The primary goal of the development of the dispatcher system, the introduction of the CAD (computer aided dispatch system), is to increase efficiency. One of its objective measures is the arrival time, i.e. the arrival time of the rescue units from the report of the medical emergency.

Optimally, the European goal is to meet the arrival time of 15 minutes at least 90% of the time.[8] Prior to the development of the IT system this goal was reached between 60 and 70% of the time.[9] In 2018 it rose to 78% and in 2019 to 82%.[10]

Even with the Covid pandemic which increased the number of patients and additional tasks that weighed heavily on the National Emergency Service, a small improvement, 1–2% was achieved in meeting the European goal. This was primarily due to the development of additional ambulance teams, to the increase in the number of those participating in the rescue process, as well as to the opening new ambulance station.

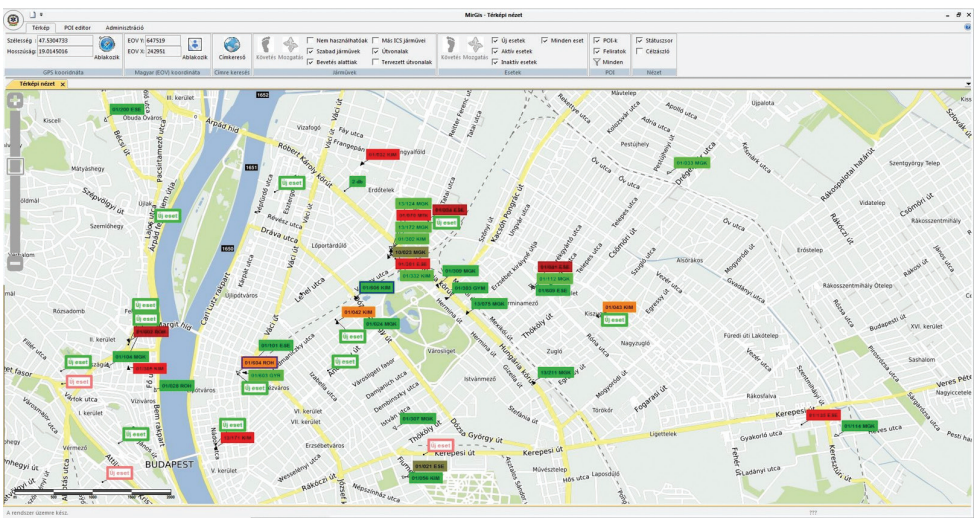


Figure 3

GIS application of the dispatcher system

Source: http://obsz.njszt.hu/ifi/images/2015/21.pdf

8 Eric Lucas dos Santos Cabral et al., 'Response time in the emergency services. Systematic review', Acta Cirúrgica Brasileira 33, no 12 (2018), 1110–1121.

9 László Domokos, 'A „vészhelyzeti" betegellátás rendszerének ellenőrzése', Állami Számvevőszéki jelentés, 2019. Ikt sz.: EL-1599-001/2019.

10 Bence Rétvári, 'Miként alakul a mentők kiérkezési ideje megyénként?' Emberi Erőforrások Minisztériumának Államtitkára, 2020. Ikt.: III/101-1/2020/PARL.

The dispatcher system includes an IT terminal assigned to the ambulance team (IFT). Its purpose is to transmit the electronic rescue documentation to the alerted ambulance team, furthermore, the at-the-scene patient documentation can also be implemented.

Tablets placed on the ambulance receive the information of the emergency call about the scene of the accident in parallel with the alerted dispatcher. The rescue team complete the electronic case report documentation on the tablet, too. This report contains all the details they notice at the scene as well as the patient care they perform at the scene. The case record software, as an electronic patient documentation, contains all the requirements that are determined by the law, replacing the paper-based documentation (Figure 4).

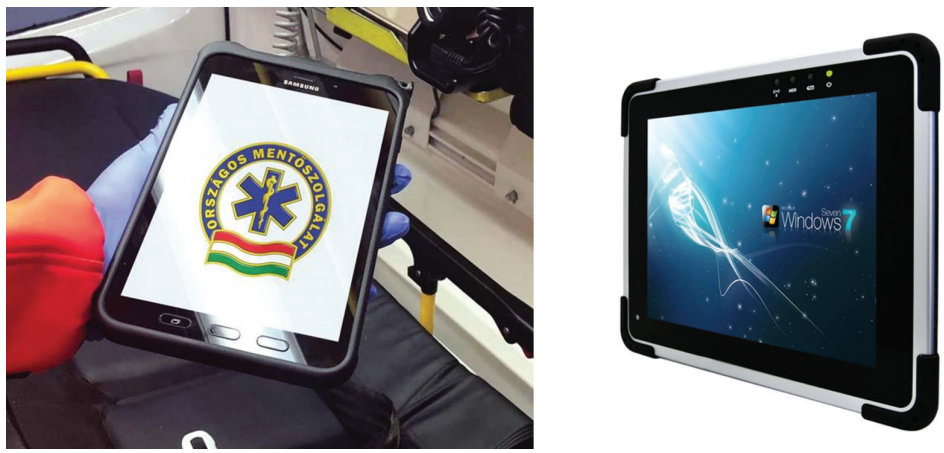


Figure 4

Intelligent On-Board Terminal (IFT)

Source: http://docplayer.hu/159559890-Veddeszreamentot-orszagos-mentoszolgalat.html; http://demin.hu/files/userfiles/DEMIN_XV/DEMIN-XV-E/2-1-2-DEMIN-XV-PGY-1.pdf

The electronic application of the rescue documentation and travel account, as well as the case record is opened by sending the details of the rescue task to the tablet.

With completing the forms, the information of the ambulance team, the distance and time emergency run kilometre and time, and the patient's personal information and information about patient care is uniform. The electronic patient documentation is completed by recording the patient's transfer to the medical institution and the care performed at the scene (Figures 5, 6).

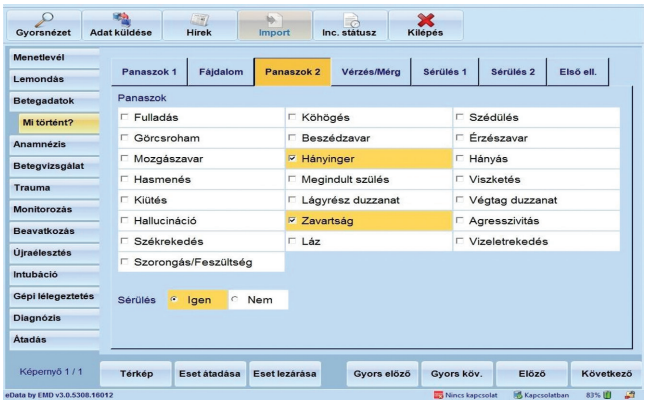


Figure 5

Electronic case record interface 1

Source: http://obsz.njszt.hu/ifi/images/2015/21.pdf

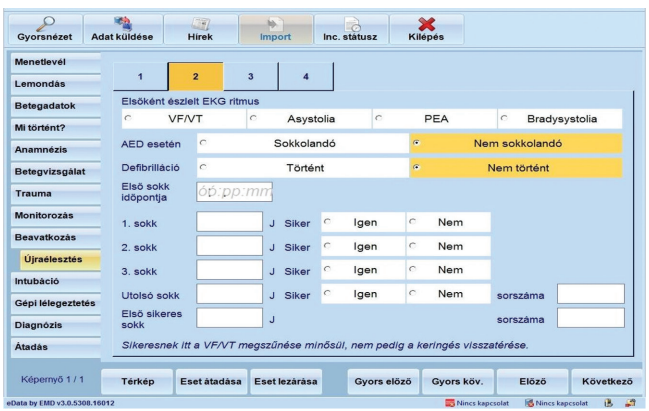


Figure 6

Electronic case record interface 2

Source: http://obsz.njszt.hu/ifi/images/2015/21.pdf

The advantage of the electronic documentation is its simple and permanent data storage, easy access for those who have permission to use it, the possibility to create and quickly access to various databases, statistical and operational data, and the possibility of adding or changing data if necessary.

Its disadvantage is the continuous use of the right quality and quantity of equipment, which, in terms of the number of ambulances means 1,000 Intelligent On-Board Terminals, as well as the operation of the entire IT and digital equipment of the country's 20 dispatcher groups 24 hours a day.

Continuous availability and adequate security protection as a critical aspect of infrastructure require priority resources, quick replacement in case of failure, continuous

IT support and stable internet connection provided availability in a moving ambulance anywhere in the country.

A further improvement opportunity could be the introduction of the uploading function of the paper-based documents (e.g. results of ECG, Code summary, Declaration, Inventory of Valuables) that are completed during the at-the-scene care and their attachment to the electronic case record.

4. Emergency and dispatcher systems in Europe

The IT-based deployment dispatcher system was developed and implemented by the older EU member states between 2005 and 2008. In some places this same system is also integrated with the fire brigade and the police (e.g. the Weserbergland Cooperative Regional Command Center in Hameln-Pyrmont in Lower Saxony, Germany).

With slight differences but following the same principle, the following system works in different places: emergency calls are processed with computer support, the dispatcher can usually visually follow the location of the call/event using the advanced location GIS. The nature of the event is determined by a carefully developed software including algorithms.

The algorithm categorises the event according to the degree of urgency and severity, then it offers to alert the free ambulance capacity recorded online. The scene, the nature of the emergency case, the accessibility, and other information from the person who reports the case are transmitted to the ambulance team via audio or digital signals. Feedback on at-the-scene activity, patient data, diagnostic and examination results is received by both the dispatcher and the institution that is supposed to treat the patient.

All data related to the performance of an emergency case (from the beginning of the emergency call to the end of the case) is time-stamped and recorded online in the IT system. IT systems include similar systems, like the Advanced Medical Priority Dispatch System (AMPDS) commonly used in the U.K. and in Germany.

The AMPDS includes systematised call answering, advice to the person who reports the case, and protocols for coordinating the type and severity of the injury or illness with the alerted ambulance. Additionally it has an Advanced Quality Assurance (AQUA) software tool to measure the performance of the dispatcher.[11]

Zenit system, used in the SOS Alarm centres in Sweden, operates similarly. It controls and coordinates the entire chain of emergency activities, and makes it possible to perform statistics and assessments, similar to the SITREM (full solution for emergencies treatment) system used in Spain.

European systems show significant similarities with the later introduced and launched domestic system, which also includes GIS, electronic documentation and communication applications, supplemented by the protocol of questions and consultation as well as the alert protocol that the dispatcher is expected to apply.[12]

[11] Az EU tagországok mentési rendszereinek jellemzői (Budapest: Informatikai és Rendszerelemzési Főigazgatóság, Rendszerelemzési Főosztály, 2014), 36–37.

[12] Gyula Kincses et al., Mentési- és mentésirányítási rendszerek Európában (Budapest: Egészségügyi Stratégiai Kutatóintézet, 2009), 4–5.

5. Joining the EESZT system

The National Emergency Medical Services also joined the Electronic Health Service System from 1 November 2018, thus the at-the-scene electronic patient documentation is available to the medical institution via an IT network, and it is also uploaded to the patient's medical documents.

The new system allows all healthcare institutions (GPs, outpatient and inpatient institutions, pharmacies) to upload patient health records to the system as well as to access their previous documents.

Patients can track and check their own medical history and take their electronically completed prescriptions at the pharmacy.

During the at-the-scene emergency care, the patient's known medical history can sometimes be of great help in making the diagnosis and performing certain interventions, as known diseases, medications taken by the patient, previous ECG abnormalities and other findings help to recognise a new or changed condition.

Health records stored by the EESZT system can be easily accessed with the help of IFTs used by ambulance teams. Currently it means an area under development.[13]

6. Telemedicine at the Emergency Medical Services

A decision support tool and system were introduced in the Northern Great Plain region of the National Emergency Medical Services in 2007. It helps to screen for cardiological diseases requiring acute care, to provide patients with at-the-scene care and to transport them to a medical institution providing definitive care.

From 2014, each Hungarian ambulance team has TTEKG, i.e. transphone telephony ECG (Figure 7).

The ECG image taken by this transphone telephony ECG can be transmitted in the form of a digital signal via the TETRA system of the ambulance team to the nearest Cardiology Centre where the cardiologist evaluating the Electrocardiogram on the computer can consult the ambulance team treating the patient at the scene.[14]

During the consultation, the cardiological diagnosis can be confirmed on the basis of the patient's complaints and the transmitted image, thus the therapy, and the patient's path can also be determined (Figure 8).

Overall, the TTEKG system enables faster patient admission to the medical institution providing final care, that is, it optimises the patient path, significantly reduces infarct mortality, provides ongoing consultation, and increases patient safety and the quality of care.

The improvement of digital and IT technology has made it possible for the new digital TTEKG device to send the image to the tablet of the ambulance team or to the cardiology centre via the Internet.

[13] Gábor Csató, 'Digitalizáció a sürgősségi betegellátásban', Interdiszciplináris Magyar Egészségügy 18, no 3 (2019), 4–6.

[14] Gyorgy Papai et al., 'Transtelephonic electrocardiography in the management of patients with acute coronary syndrome', Journal of Electrocardiology 47, no 3 (2014), 294–299.

The image is also uploaded as an attachment to the patient's electronic documentation via the EESZT system and additionally previous ECG recordings can also be displayed at the scene.

From 2019 the introduction of a new generation of the devices has been improving the quality of the recording and has been strengthening the connection of the devices in order to improve evaluation and consultation.[15]

Figure 7

TTEKG device

Source: http://sumegmento.ucoz.hu/news/uj_tt_ekg_allt_rendszerbe_az_allomason/2019-06-28-388

Figure 8

ECG image recorded by TTEKG on the Intelligent On-Board Terminal

Source: http://medicalonline.hu/gyogyitas/cikk/kulonleges_magyar_ujitas_segithet_tulelni_az_infarktust

7. Mobile applications to support at-the-scene emergency medical care

By operating and supporting mobile phone applications, the National Emergency Medical Services assist in providing at-the-scene first aid assistance prior to the arrival of the ambulance team and additionally the users are provided the opportunity to request direct assistance.

Szív (Heart) City mobile application has been available since October 2017. With the help of this application first aid providers who download, register and log in to the application on their phone can be sent to the public areas as soon as possible to treat medical emergencies and start resuscitation.[16]

The application operates like this: after reporting the medical case, in parallel with the alerted ambulance team, voluntary users – professional or non-professional

[15] György Pápai, Az Országos Mentőszolgálat Észak-alföldi régiójában kidolgozott betegút modell és cardiobeeperes, prehospitalis döntéstámogató rendszer hatása az acut coronaria syndromás betegek morbiditási és mortalitási mutatóinak változására (Laki Kálmán Doktori Iskola, Doktori [PhD] értekezés tézisei, 2018).

[16] György Tóth, 'Tömeges káresemények és katasztrófák következményeinek egészségügyi felszámolását végző és támogató szervezetek tevékenysége', Hadmérnök 15, no 3 (2020), 233–234.

first aid providers – who are within 500 meters of the scene, receive a message from the dispatcher of the Emergency Medical Services about the exact location of the medical emergency, thus the care for patients can begin before the arrival of the ambulance. With the help of the application, the steps of resuscitation can be mastered. Additionally, the first aid provider can be informed about the availability of a nearby defibrillator, which is essential for care.

If more than one first aid providers are close to the patient, through the application the dispatcher can also request assistance in taking the available defibrillator to the scene of the medical emergency (Figure 9).[17]

It allows for both early resuscitation and the at-the-scene use of the defibrillator before the ambulance arrives. From October 2017, more than 50,000 users have downloaded the application, more than 2,200 alarms have been received by first aid providers, and more than 40 successful resuscitation assistance have been provided in several parts of the country.[18]

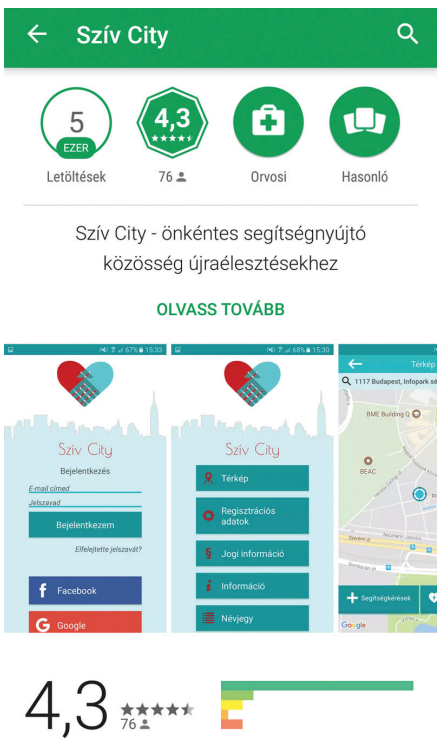


Figure 9

Interface of Szív (Heart) City application

Source: http://8200.hu/index.php/hirek/belfold/item/2929-elindult-a-sziv-city-eletmento-mobilalkalmazas

[17] 'Szív City: Életmentő mobilalkalmazás', 17 October 2017.
[18] 'Szív City application'.

With the help of the Életmentő (Life Saving) application, the person reporting the medical emergency can contact the Dispatcher group of the National Emergency Medical Services without dialling the emergency centre. It is enough to use the Alarm function and in parallel with the call the location and other pre-recorded health information are transmitted in the form of a message.[19]

The advantage of the application is the direct contact, the determination of the location of the person reporting the medical emergency with the help of GPS coordinates, which is especially important if the reporting person cannot determine the exact location. In addition to the telephone connection, a message is also sent to the dispatcher group, so even in case of communication difficulties, the request for help can be realised together with the exact location and the connection can be established even by exchanging SMS messages.

Basic first aid knowledge can also be obtained from the application, as well as public information on hospitals, clinics, pharmacies and information about defibrillators placed in public areas is also available. The application also works in Austria and in the Czech Republic, as well as in certain areas of Slovakia, thus help is available even from abroad (Figure 10).

Figure 10

Lifesaving mobile application interface

Source: https://motorrevu.hu/cikkek/az-a%E2%80%B0letmenta-app-minden-motorosnak-ajanlott/

[19] 'Életmentő application'.

8. Summary, conclusions

In recent years, Hungarian healthcare including outpatient and inpatient medical institutions and also the Emergency Medical Services providing emergency care have undergone numerous IT improvements.

The electronic documentation has been introduced as part of the IT support for pre-hospital emergency care, which, together with the digital technology for dispatcher service, has become a modern system that increases patient safety.

The aim of this paper was to introduce and study the essential elements of electronic documentation. Easy data storage, easy access and management, the possibility of changing data and the introduction of additional applications can be mentioned as the advantages of electronic documentation. However, it has some disadvantages as well: setting portable devices which require a permanent, continuously available, stable internet connection.

Electronic, digital technology increases efficiency, which is clearly reflected in the continuous improvement of the at-the-scene arrival rates within 15 minutes, which is also relevant in Europe.[20] Telemedicine facilities improve at-the-scene care, support patient care, diagnosis and patient path decisions, and increase patient safety. This evidence supports my hypothesis.

The National Emergency Medical Services are also involved in the improvement and implementation of mobile applications that assist at-the-scene first aid for non-professionals in cases where early intervention can be life-saving for the patient.

In parallel with the possibility of requesting direct assistance in unexpected situations, the scene of the medical emergency or injury may be more easily accessible.

In summary, IT and digital technology increase patient safety, facilitate access to and transmission of health records, and provide support to both non-professionals and health care professionals.

The introduction of Electronic death certificate and the support of uploading health documents during the at-the-scene care (ECG, Code summary, other paper-based documents) to the patients' electronic documentation are expected to be introduced in the near future.

References

Az EU tagországok mentési rendszereinek jellemzői. Budapest: Informatikai és Rendszerelemzési Főigazgatóság, Rendszerelemzési Főosztály, 2014, 36–37.

Csató, Gábor, 'Digitalizáció a sürgősségi betegellátásban'. Interdiszciplináris Magyar Egészségügy 18, no 3 (2019), 4–6.

Csató, Gábor, 'Modernitás a mentőszolgálatban: Mitől lesz modern egy egészségügyi intézmény?' Interdiszciplináris Magyar Egészségügy 16, no 5 (2017), 6–7.

Domokos, László, 'A „vészhelyzeti" betegellátás rendszerének ellenőrzése'. Állami Számvevőszéki jelentés, 2019. Ikt sz.: EL-1599-001/2019.

[20] Nuffield Trust, 'Ambulance response times', s. a.

'Életmentő application'. Online: www.mentok.hu/ha-baj-van/eletmento-app/
Kincses, Gyula et al., Mentési- és mentésirányítási rendszerek Európában. Budapest: Egészségügyi Stratégiai Kutatóintézet, 2009, 4–5.
Lucas, Eric dos Santos Cabral et al., 'Response time in the emergency services. Systematic review'. Acta Cirúrgica Brasileira 33, no 12 (2018), 1110–1121. Online: https://doi.org/10.1590/s0102-865020180120000009
Nuffield Trust, 'Ambulance response times', s. a. Online: www.nuffieldtrust.org.uk/resource/ambulance-response-times
Pápai, György, Az Országos Mentőszolgálat Észak-alföldi régiójában kidolgozott betegút modell és cardiobeeperes, prehospitalis döntéstámogató rendszer hatása az acut coronaria syndromás betegek morbiditási és mortalitási mutatóinak változására. Laki Kálmán Doktori Iskola, Doktori (PhD) értekezés tézisei, 2018.
Papai, Gyorgy et al., 'Transtelephonic electrocardiography in the management of patients with acute coronary syndrome'. Journal of Electrocardiology 47, no 3 (2014), 294–299. Online: https://doi.org/10.1016/j.jelectrocard.2014.02.007
Pápai, György, Új minőségbiztosítási feladatok az OMSZ-nál 2, s. a.
Online: https://docplayer.hu/3575621-Uj-minosegbiztositasi-feladatok-az-omsz-nal-2-papai-gyorgy-regio-igazgato-orszagos-mentoszolgalat-ear.html
Rétvári, Bence, 'Miként alakul a mentők kiérkezési ideje megyénként?' Emberi Erőforrások Minisztériumának Államtitkára, 2020. Ikt.: III/101-1/2020/PARL.
'Szív City application'. Online: http://szivcity.hu
'Szív City: Életmentő mobilalkalmazás', 17 October 2017. Online: http://medicalonline.hu/informatika/cikk/sziv_city__eletmento_mobilalkalmazas
Tóth, György, 'Tömeges káresemények és katasztrófák következményeinek egészségügyi felszámolását végző és támogató szervezetek tevékenysége'. Hadmérnök 15, no 3 (2020), 231–239. Online: https://doi.org/10.32567/hm.2020.3.13

Legal sources

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
Általános adatvédelmi rendelet (GDPR), 4. cikk 15. pont
1997. évi CLIV. törvény az egészségügyről
37/2011. (VI. 28.) NEFMI rendelet a mentésről szóló 5/2006. (II. 7.) EüM rendelet és a betegszállításról szóló 19/1998. (VI. 3.) NM rendelet módosításáról. Online: www.hbcs.hu/uploads/jogszabaly/808/fajlok/37_2011_nefmi.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA
16. évfolyam (2021) 4. szám 183–199.
DOI: 10.32567/hm.2021.4.14

Török Péter[1]

NATO-tagországok hadseregeiben rendszeresített digitáliskatona-rendszerek C4I alrendszereinek bemutatása

Presentation of the C4I Subsystems of Digital Military Systems in the Armies of NATO Member Countries

A mai fegyveres konfliktusok irányítását a hálózatközpontú hadviselés jellemzi. Ebben a megközelítésben az információkat szerző érzékelő hálózatok, a döntéshozói hálózat és a végrehajtói hálózat egy közös rendszerben integrálódik. Így a végrehajtó katonák hozzáférnek más felderítési forrásból származó információkhoz. A katonák által használt eszközrendszerben a C4I (*command, control, communications, computers, intelligence,* vezetés, irányítás, híradás, informatika és hírszerzés) rendszerek azok az elemek, amelyekkel ez megvalósul. Ezek a rendszerek szolgáltatnak harctéri információkat a parancsnokok számára a döntések meghozatalához és a katonai erők ellenőrzéséhez, a küldetések végrehajtásához. Ebben a cikkben a NATO- (North Atlantic Treaty Organisation) tagországok hadseregeiben már rendszeresített DSS- *(Dismounted Soldier System)* program C4I rendszereit mutatom be.

Kulcsszavak: digitális katona, DSS, Nett Warrior, Félin, VOSS, ISS, IdZ, NORMANS, Futuro Soldato, C4I

The management of today's armed conflicts is characterised by network-centric warfare. In this approach, the sensor networks that obtain the information, the decision-making network, and the executive network are integrated into a common system. Thus, executive soldiers have access to information from other reconnaissance sources. In the tool system used by soldiers, C4I (Command, Control, Communications, Computers, Intelligence) systems are the elements by which this is accomplished. These systems provide battlefield information to commanders to make decisions and control

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktori hallgató, e-mail: torok.peter@uni-nke.hu

military forces to carry out missions. In this article, I present the C4I systems of the DSS (Dismounted Soldier System) program, which are already systematised in the armies of NATO (North Atlantic Treaty Organization) member states.

Keywords: **digital soldiers, DSS, Nett Warrior, FÉLIN, VOSS, ISS, IdZ, NORMAN, Futuro Soldato, C4I**

1. Bevezetés

Korunk jellemző hadviselési formája a negyedik generációs hadviselés. A generációváltás a Szovjetunió szétesésének idejében kezdődött, de a mai napig folyamatosan fejlődik és alakul a megjelenő új kihívások, fenyegetések és szemben álló felek megjelenésére reagálva, az alkalmazott eszközök, technológiák és technikák adaptálásával.[2]

A technikai forradalmon kívül szemléletváltás is történt a hadviselésben. A mobil hadviselést a hálózatközpontú hadviselés váltotta. Ennek alapgondolata az, hogy a számítógépek adatfeldolgozási képességeit és a hálózat kommunikációs technológiáit kihasználva biztosítani lehet az információmegosztást, ami növeli a hadsereg működtetésének hatékonyságát. A 21. század első két évtizedében folytatódott és gyorsult az infokommunikációs forradalom. A használt eszközök mérete csökkent, a teljesítményük nőtt. Az adatátvitel sebessége gyorsabb, a kapcsolat megbízhatóbb és biztonságosabb lett. Így ugyanazon a hálózaton adat-, hang-, videó- stb. kommunikáció egyaránt megvalósítható.

A különböző kommunikációs formák egységesítése további előnyökkel is járt. Az egységes környezet egyrészről költségcsökkentést jelent, mivel ugyanaz a hardver lát el számos feladatot.[3] Másrészről a különböző rendszerek közötti interoperabilitás fenntartása kérdéses, mert a különböző katonák taktikája és fegyverrendszere eltérő, de a szabványosított protokollok használata megkönnyíti a szövetséges erők közötti együttműködést.

A katonák által használt eszközrendszerben a C4I rendszerek azok az elemek, amelyek intenzíven használják az informatikát és a kommunikációt. Ezek olyan katonai információs rendszerek, amelyek metodikájuk szerint komplex vezetési rendszerként viselkednek.[4] Egységesítik az információgyűjtés, a kommunikáció, a tervezés, a hírszerzés, és a döntéshozatal folyamatát. Meghatározó az információs fölény elérésében, ebből adódóan a hadműveleti fölény megszerzésében is.[5]

A C4I rendszerek harctéri információkat szolgáltatnak a parancsnokok számára a döntések meghozatalához és a katonai erők ellenőrzéséhez a küldetések végrehajtásához.[6] Kezdetben ezek a rendszerek statikus architektúrákon alapultak, feladatspecifikusak voltak a magas megbízhatóság biztosítása és a valós idejű információk támogatása érdekében. Ezekből a rendszerekből azonban hiányoztak az informatika legújabb fejleményei által biztosított dinamikus adatok.

[2] Jobbágy Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai. – fogalmi kitekintő. *Hadmérnök,* 12. (2017), 1. 212.

[3] Előházi János: Védelmi célú informatikai rendszerek feladatai és fenyegetettségei a hálózatközpontú hadviselésben. *Hadmérnök,* 2. (2007), 3. 70–80.

[4] Előházi (2007): i. m.

[5] Haig Zsolt –Várhegyi István: *Hadviselés az információs hadszíntéren.* Budapest, Zrínyi, 2005. 197.

[6] Farkas Tibor – Hronyecz Erika: Digitális Katona Rendszer a Katasztrófavédelmi Műveletekben. *Műszaki Tudományos Közlemények,* 7. (2017), 147–150.

A modern C4I rendszerek megkövetelik, hogy mind a statikus, mind a dinamikus adatok rendelkezésre álljanak a megbízhatóság, a valós idejű támogatás, az újrafelhasználhatóság és az interoperabilitás megkönnyítése érdekében.[7] Az informatika, a kommunikáció és az adatfeldolgozás közelmúltbeli fejlődése alkalmassá tette a különböző elemek integrálását a C4I rendszerekben.[8]

A bemutatott rendszerek értékeléséhez ismerni kell a katonai C4I rendszerekkel szemben támasztott követelményeket:

- „valós idejű felderítési adatok megszerzése harctéri érzékelők, földi, légi és műholdas adatszerző eszközök, rendszerek segítségével;
- adatok adatfeldolgozó központokban való gyűjtése, fuzionálása, számítógépes kiértékelése;
- nyílt és zárt távbeszélő, géptávíró, fax- és adatátviteli összeköttetés béke elhelyezésben és tábori körülmények között;
- adatátvitel a törzsön belüli és a törzsek, valamint a csapatok közötti számítástechnikai hálózatokon belül és azok között;
- álló és mozgó, fekete-fehér és színes képátvitel és videókonferencia lehetősége nyílt és zárt átviteli utakon keresztül;
- elektronikus megjelenítők (nagy méretű kivetítők) széles körű alkalmazása a helyzet, térképek, tervek megjelenítésére;
- digitális terepadatbázis és nagypontosságú navigációs (GPS) rendszerek segítségével helymeghatározás, útvonalképzés, távolság-, magasság meghatározás, láthatóságvizsgálat stb. Ezek alapján pontos célmegjelölés, harc- és tűzvezetés megvalósítása;
- a rendszer elemeinek nagy mozgékonyságú gyors konfigurálhatósága;
- beépített együttműködési lehetőség a haderőnemek, fegyvernemek és szakcsapatok között;
- számítógéppel támogatott harcászati-hadműveleti tervezés szakértői rendszerek segítségével. Automatikus döntés-előkészítés, döntési változatok felkínálása a parancsnoknak."[9]

2. A vizsgált rendszerek bemutatása

Nett Warrior

A Nett Warrior az Amerikai Egyesült Államok hadseregének egyik modernizációs programja. A projekt célja „a katonák helyzetismeretének és kommunikációjának javítása".

A korábbi Land Warrior projekt eredményeit és tapasztalatait felhasználva alakították ki a koncepciót. A klasszikus, fő- és alvállalkozókból álló hierarchikus fejlesztési

[7] Farkas Tibor: A védelmi tevékenységeket támogató MH Kormányzati Célú Elkülönült Hírközlő Hálózat fejlesztési lehetőségeinek vizsgálata a honvédelmi és haderőfejlesztési program (Zrínyi 2026) tükrében – Hazai/nemzetközi szakirodalmi összefoglaló. *Hadtudományi Szemle,* 12. (2019), 4. 5–16.

[8] Mariusz Chmielewski – Jaroslaw Koszela: The Concept of C2 Systems Data Integration for Planning Joint Military Operations Based on JC3 Standard. In *Conference: Military Communications and Information Systems Conference MCC'2008 Volume: 1.* 2008. 3; Tibor Farkas: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289; Tibor Farkas: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15.

[9] Haig Zsolt: *Információs műveletek*. Prezentáció.

rendszer helyett, a követelményeknek megfelelő COTS[10] (*commercial off the shelf,* kereskedelmi forgalomban kapható) megoldásokat keresnek, és integrálják a rendszerben levő katonai eszközökkel. A program másik alappillére a végfelhasználókkal együtt végrehajtott folyamatos terepi tesztek. Így azonnali és közvetlen visszajelzés volt a rendszer használhatóságáról és a szükséges módosításokról.

A rendszer alapkiépítésben egy rádiót, EUD-t (*end user device,* felhasználói eszköz) és egy viselhető akkumulátort, valamint az eszközöket összekötő kábeleket tartalmaz. A rádió egy AN/PRC-154A,[11] ehhez kapcsolódik energia- és adatelosztó hub. A hubhoz kapcsolódik az EUD, amely eredetileg egy Samsung Galaxy Note 2 volt. Ez az eszköz az, amely leghamarabb elavul a rendszerben, így folyamatos fejlesztése indokolt. Itt mutatkozik meg a COTS-megoldások előnye. Egyszerűen cserélhető egy hasonló felépítésű, de nagyobb teljesítményű eszközre. A rendszer modernizálásának ezt a lehetőségét ki is használják a fejlesztés során. Az évek folyamán többször változott az EUD a Samsung Galaxy sorozatának egy-egy újabb típusára. 2019-től az S9 verziót használják a rendszerhez, de már tesztelik az S20 típust is.[12] Szintén a hubhoz csatlakozik a taktikai mellényben viselt akkumulátor, amely akár 20 órára elegendő energiát biztosít a rendszer számára. Az adatkapcsolat a rádió és az EUD között USB 3.1 szabvány szerint történik, ami szintén megkönnyíti az eszköz modernebbre cseréjét.[13] Tervezik az EUD-ban rejlő lehetőségek használatát, az LTE-t *(long term evolution),* a Wifit *(wireless fidelity)* és a Bluetoothot.[14]

A rendszer nem látható komponense az Androidon futó speciális szoftver, az ATAK *(Android Tactical Assault Kit)*.[15]

1. ábra

A Nett Warrior C4I készlete

Forrás: www.aresdifesa.it/wp-content/uploads/2020/12/s20_lifestyle_KV_7-map-1536x1025.jpg

[10] Négyesi Imre: COTS rendszerek alkalmazási lehetőségeinek vizsgálata. *Hadtudományi Szemle,* 4. (2011), 4. 113.
[11] The office of the Director, Operational Test and Evaluation: *Nett Warrior*. Director, Operational Test and Evaluation (DOT&E), 2018.
[12] Chris Balcik: Government and Industry Meet to Transform Tactical Operations. *Samsung Insights,* 2019. február 15.
[13] Dan Milliken – José Collazo: *USB 3.1 Capabilities and Considerations for the Dismounted Soldier.* Power Sources 2018 Digest. 2018. 220.
[14] Alex Dixon – Julia Henning: Nett Warrior gets new end-user device. *Army.mil,* 2013. július 23.
[15] *ADR ATAK Plugin*. Ds2.com.

Félin

A Félin *(fantassin à équipements et liaisons intégrés)* a francia hadsereg gyalogos katona modernizációs programja által kidolgozott rendszer. A teljes rendszer a Sagem mint integrátor által vezetett konzorcium által lett kifejlesztve (monolit rendszer).

A Félin kombinálja a módosított FAMAS puskát számos egyéb elektronikával, ruházattal, sisakkal és testpáncélzattal. A hordozható elektronikus platform (*portable electrical platform,* PEP) a rendszer központi része. A rendszer összes elektronikus berendezése csatlakozik a PEP-hez. Ezek a taktikai rádió, a fegyverre és a sisakra szerelt, valamint a kézi optikai eszközök, a parancsnok BMS (*battle management systems,* csatairányítási rendszer) terminálja és az akkumulátorok.

A PEP egy viselhető számítógépet tartalmaz, amely kommunikációs és navigációs egységgel történő adatkommunikációra USB 2.0 interfészt használ. A ruházatban két vezetékes hálózat található. Az egyik továbbítja az elektromos energiát minden rendszerbe. A másik pedig az adatkapcsolatot biztosítja.[16]

A rendszer kommunikációs eszköze a Thales cég TRC-9100 hang- és adatrádiója. A rádió ingetrált GPS-vevővel rendelkezik.[17] A parancsnok készletéhez tartozó SitComdé tactical terminallal csatlakozik a harcjárműre telepített SITEL harci irányító rendszerhez. A színes érintőképernyővel ellátott eszköz lehetővé teszi a vezető számára a taktikai helyzet kezelését, integrált üzenetküldéssel és barát/ellenség helyzet kijelzésével (BFT/RFT – kék és vörös erő követése). Integrálja a szenzorok adatait és videóit.[18]

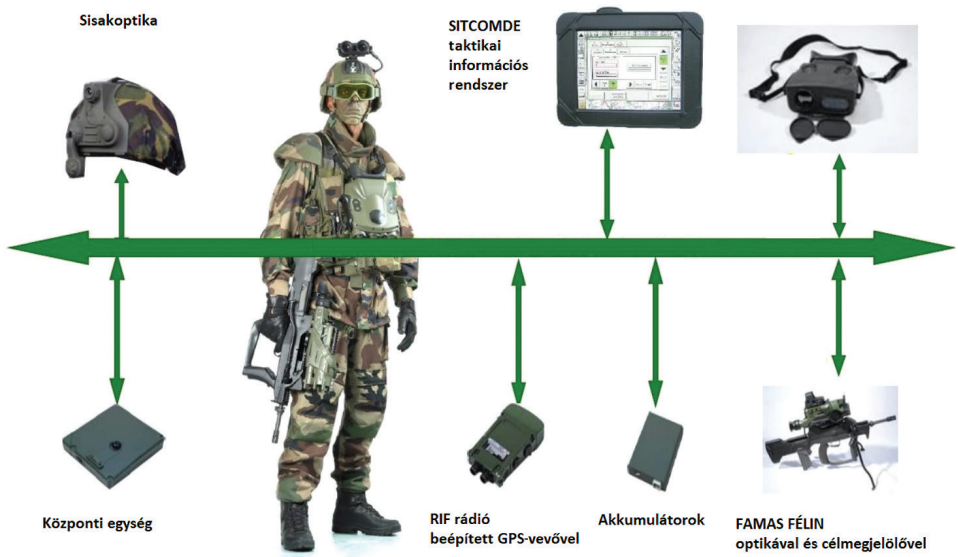
A kézi optika a JIM LR *(long range)* hordozható multifunkciós infravörös távcsöve, amely a Sagem JIM moduláris optika család tagja. Ezek az eszközök opcionális szolgáltatásokkal és funkciókkal is felszerelhetők a követelményeknek megfelelően. Így a digitális csatatér szerves része a szabványos interfészeinek köszönhetően. De már standard kiépítésben tartalmazza a nagy nagyítású optikát, az infravörös képérzékelőt és a nagy teljesítményű képalkotó szoftvert. Standard kiépítésben a nagy teljesítményű képalkotó szoftvert és a képet továbbítja a PEP-nek.

Hasonló módon, a fegyverre szerelt optika is alkalmas infravörös tartományban is működni, és a képe továbbítható.[19]

A holland katona modernizációs program neve VOSS *(verbeterd operationeel soldaat systeem)*. A rendszer eredetileg, a 2008-as indulásakor a következő elemekből épült fel:

- okosmellény;
- kommunikációs rendszer;
- C2 rendszer.

[16] Portable Electronic Platform – A Digital Brain Integrates with FELIN. *Defense Update,* 2006. június 20.
[17] Thomas Withington: Time to Accessorize. *Armada International,* 2017. július 26.
[18] Walter Christian Håland: FÉLIN – Future Infantry Soldier System, France. *Small Arms Defense Journal,* 9. (2017), 3.
[19] SAFRAN: 'Boar's Head' Exercise with the British Army: FELIN makes European début. *Soldier Modernisation,* 9. (2012), 32–35.



2. ábra

A Félin-rendszer C41 rendszere

Forrás: a szerző szerkesztése NATO: Overview of Dismounted Soldier Systems. The NATO Science and Technology Organization, 2018. 2–15. alapján

VOSS

A haditechnika fejlődése itt is változásokat hozott. Új elemként bekerült az integrált fejvédelem, egy moduláris felépítésű sisak. Ebben helyezték el a fejhallgatót és a mikrofont, valamint a fenyegetéstől függően fül- és arcvédő is felszerelhető a sisakra.[20]

Később a programhoz csatlakozott a belga BEST és a luxemburgi COMPASS program is, elsősorban a közös C4I rendszerelem kifejlesztéséhez.[21] A mellény az Elbit Systems Dominator rendszerén alapul, amely könnyű és moduláris, valamint úgy alakították ki, hogy a már rendszeresített eszközök kapcsolódni tudjanak hozzá. A rendszer az Elbit System E-Lynx Soldier Radiot, a PNR-1000-t használja.[22]

A rendszerhez használt Elbit Raptor viselhető számítógépe egy all-in-one megoldás. Az eszközön a TORCH2H BMS fut. A hardver és a szoftverek egy gyártótól származnak és kimondottam a Dominatorhoz készültek. A 4,3" érintőképernyőn a katonák láthatják egymás helyét, hozzáférhetnek az érkező információkhoz, és maguk is küldhetnek. A GPS-vevővel ellátott rádiónak köszönhetően a katonák közvetlenül kommunikálhatnak a parancsnoksággal és más egységekkel a számítógép segítsége nélkül is.

A végfelhasználói visszajelzések alapján a rendszerből kivették az integrált fejvédelmet, mert túl nehéznek bizonyult. Az új sisak kiválasztása külön programban

[20] VOSS begins in earnest. *Soldier Modernisation,* 1. (2008).
[21] Parlementaire Monitor: Brief regering; D-brief over het project Verbeterd Operationeel Soldaat Systeem (VOSS) – Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2015.
[22] Paolo Valpolini: The Netherlands: VOSS close to delivery. *EDR online,* 2018. október 30.

történik. A tavalyi év folyamán viszont új elemmel bővült a rendszer. Az Elbit XACT nv32 éjjellátó rendszerét adták hozzá.[23]

3. ábra

A VOSS rendszerhez használt Elbit Raptor

Forrás: www.armyrecognition.com/images/stories/news/2015/july/Elbit_Systems_will_deliver_combat_vest_including_radio_and_C4I_capabilities_to_Benelux_countries_640_002.jpg)

ISSP *(Integrated Soldier System Project)*

Az ISSP a kanadai haderő gyalogos katona modernizációs programja. Azzal a céllal hozták létre, hogy javítsa az egyes katonák helyzetismeretét, korszerűsített és biztonságos kommunikációs és navigációs képességeket biztosítson számukra. Az ISSP integrálható a kanadai hadsereg szárazföldi parancsnokság támogató rendszerébe.[24] Az ISSP is azt a fejlesztési elvet követi, hogy egy integrátor által vezetett konzorcium végzi. A kanadai kormány a Rheinmetall Canadát bízta meg a rendszer kifejlesztésével. A Rheinmetall Canada a Saab AB kijelző és energiarendszerét és az Invisio fülhallgató-technológiáját használja.[25]

A C4I képességet a Saab 9Land Soldier rendszermegoldás biztosítja, amely információs támogatást nyújt az egyes harcosoknak és a szakaszparancsnokoknak harchelyzetekben.[26] De a hangkommunikáció az elsődleges képesség, a számítógépes eszköz csak kiegészítő berendezés. A rendszer központja a Saab által gyártott sPad nevű, könnyű, érintőképernyős kézi számítógép, amely a 9Land BMS fut. A kommunikációhoz kezdetekben a Radmor PSR 35010 típusú rádiókat használták.[27] Majd

[23] Dutch Army Procures Elbit XACT nv32 micro Night Vision Systems. *Defense World,* 2020. december 19.
[24] Government of Canada: *Integrated soldier system project* (é. n.).
[25] Chris Thatcher: Instant impact: Integrated soldier system suite will change platoon and company tactics. *Canadian Army Today,* 2018. november 26.
[26] 9Land Battle Management System. Saab.
[27] World Premiere for SAAB Soldier C2 and personnal radio integration at MSPO 2012. *Army Recognition,* 2012. szeptember 8.

2015-ben lecserélték a Harris RF-7850S típusra (USB port).[28] Ez a rádió beépített GPS-vevővel rendelkezik, így nincs szükség külön eszközre.[29]

Az ISSP-n kívül Kanada folytatja a korábban elkezdett *Advanced Soldier Adaptive Power* (ASAP) koncepció fejlesztési projektjét. Az ASAP egy taktikai mellény, amely gerincét képezi a katona által szállított eszközök és áramforrások közötti energiaellátásnak és adatcserének.[30]

4. ábra

Saab sPad kézi számítógép

Forrás: http://2.bp.blogspot.com/-yAlOgnR5khs/UE2RG9U_nUI/AAAAAAAALtk/D5-MJCBbVG8/s1600/sPad_unit.jpg

Infanterist der Zukunft

A német IdZ rendszer egy első generációs modernizációs program. Klasszikus fejlesztési elvek alapján készült, fővállalkozó a Rheinmetall. A következő modulokat tartalmazza:

- ruházat, védőeszközök és személyes felszerelések;
- fegyverek, kijelzők és érzékelők;
- C4I.

A C4I alrendszer Solar 400EG-E UHF[31] rádióból, fejhallgatóból, viselhető számítógépből, sisak kijelzőből, fegyverre szerelhető vezérlőegységből, GPS-vevőből, éjjellátóból, digitális iránytűből és az akkumulátorokból áll.[32] A parancsnok készlete még tartalmaz egy VHF csapatrádiót és egy PDA-t, amelyen a TacNet Soldier TMS *(Tactical Management System)* szoftver fut.[33]

[28] Thatcher (2018): i. m.
[29] Falcon III® RF-7850S SPR™ Advanced Wideband Secure Personal Radio. *L3Harris.*
[30] NORMANS pursues core functionality. *Soldier Modernisation,* 2008.
[31] Paolo Valpolini: Soldier systems evolution by Rheinmetall. *EDR online,* 2019. szeptember 19.
[32] Lásd: www.defence-and-security.com/uploads/newsarticle/5711059/images/483458/small/gladius.jpg
[33] Rheinmetall – leading supplier of soldier systems and expert partner for network-enabled operations. *EDR online,* 2019. szeptember 10.

A C4I alrendszer kijelzőjén, a digitális térképen megmutatja a katona saját helyzetét, társainak helyzetét, az aknamezők és más veszélyzónák helyzetét, a célt és célirányt, a célkoordinátákat és az ellenség helyzetét. Az aktuális helyzetadatokat magasabb szintről kapják. A digitális hang- és adatrádió-kommunikáció azonnali parancsokat és felderítési adatokat szolgáltat a katonának.[34]

5. ábra

IdZ rendszer kijelzője

Forrás: www.spartanat.com/wp-content/uploads/2019/06/IDET-Gladius-2.0-4.jpg

NORMANS

NORMANS a norvég katona modernizációs programja a *Norwegian Modular Arctic Network Soldier* (NORMANS). A tervezésében a modularitás volt a fő szempont, majd az első tesztek után a harchatékonyságra és a biztonság növelésére összpontosítottak, a fejlesztést a Thales végezte.

Két konfiguráció létezik: a NORMANS Light, amely egy egyszerű navigációs és kommunikációs egység, amely növeli a katona helyzetismeretét, és NORMANS Advanced, amely a parancsnoki rendszer. A tervezés a mobilitásra és a könnyű használatra összpontosít.

NORMANS Light: kis méretű, monokróm grafikus kijelzővel rendelkező egység, amely a katona számára megadja a csapattagok relatív helyzetét, megfigyeléseket, útpontokat. És olyan, a küldetéshez fontos, előre definiált üzeneteket, mint például:

- Hol vagyok?
- Merre megyek?
- Hol van a csapatom?
- Hol van az ellenség?
- Mik a feladataim?[35]

[34] IdZ (Infanterist der Zukunft) Future Soldier System. *Army Technology* (é. n.).
[35] NATO: *Overview of Dismounted Soldier Systems*. The NATO Science and Technology Organization, (2018). 2–23.

6. ábra
A NORMANS Light kijelzője
Forrás: NATO (2018): i. m. 2–24.

A NORMANS Advanced egy parancsnoki rendszer, ahol a felhasználók szükség szerint hozzáadhatnak különböző funkciókat. Folyamatosan friss képet nyújt az aktuális helyzetről, erősíti az irányítást és növeli a parancsnoki képességet. A rendszer a következő komponenseket tartalmazza: az adatkezelést és adatfeldolgozást végző egység integrált GPS-vevővel és 3D digitális iránytűvel, a színes kommunikációs megjelenítő és a taktikai rádió.[36]

7. ábra
A NORMANS Light kijelzője
Forrás: a szerző szerkesztése NATO (2018): i. m. 2–25. alapján

[36] Soldier Modernisation (2008): i. m.

A NORMANS Advanced tartalmaz egy interaktív tervezési eszközt, ahol az útpontokat, területeket, útvonalakat és egyéb kritikus információkat feljegyzik a térképre és továbbítják a katonáknak. A rendszer megkönnyíti a gyors küldetéstervezést, a könnyen kommunikálható megrendeléseket, a gyors és pontos jelentéstételt és a helyzetfelismerést.[37]

A Light rendszerhez használt rádió a Harris RF-7800S-TR. Ebben beépített GPS-vevő található, ez alapján állapítja meg a koordinátákat. Ez a készlet USB és RS232 kommunikációs protokollokat támogat. Az Advanced kiépítés ezenkívül Kongsberg MH300 rádiót is tartalmaz. A színes kijelzős egység sokkal több és fejlettebb, protokollkészlettel rendelkezik: USB és USB OTG, Ethernet, RS232, RS422, RS485, Bluetooth 2.1 + EDR, WLAN 802.11G.[38]

Soldato Futuro

A Soldato Futuro rendszer kifejlesztését az olasz védelmi minisztérium kezdeményezte. A kiírt tendert a Selex által vezetett olasz cégcsoport nyerte. A C4I alrendszer tervezését és fejlesztését a Leonardo cég végzi.[39] A cégcsoporton belüli együttműködés eredménye, hogy a Freccia 8×8 páncélozott harci járművel összhangban működik, és a járművet használja adatkapcsolati átjáróként.[40]

A rendszer központja egy viselhető számítógép, amelyen a Land Tactical C2SA szoftver fut.[41] Ehhez csatlakoznak a rendszer elemei, a taktikai rádió és a sisakra szerelhető optika. Ezeken kívül a készlet kiegészül egy külső érintőképernyős kijelzővel.

A rádió a Selex ES gyártó Swave terméke.[42] Ez egy SDR rádió, ennek köszönhetően 30 MHz-512 MHz frekvenciatartományban üzemel. Így feleslegessé teszi a két rádió használatát, és mindig a körülményeknek legmegfelelőbb hullámhossztartományt lehet kiválasztani a kommunikációhoz.[43]

A rendszer érintőképernyőt használ az információk küldésére és fogadására mind szöveges, mind grafikus/kép üzenetek formájában, valamint taktikai helyzeteket, navigációs adatokat, globális helymeghatározó rendszer adatait jeleníti meg digitális térképeken. Az érintőképernyő egy zseb méretű számítógéphez van csatlakoztatva, amely szabványos ember-gép interfészt (MMI, *man machine interface)* használ. A számítógép adatátvitelre USB, a járműben Ethernet 10/100 Base T protokollt használ.[44]

[37] Soldier Modernisation (2008): i. m.
[38] NATO: (2018): i. m. 2–25.
[39] Leonardo Company: C4I SYSTEMS (2018). 3.
[40] Soldato Futuro: Concept, Development and Experimentation Phase Begins. *Soldier Modernisation,* 7.(2011), június.
[41] Leonardo Company (2018): i. m. 21.
[42] Leonardo: Selex ES signs new contracts worth around €60m for the Italian Army's „Soldato Futuro" programme (2014. március 25.).
[43] Lásd: http://usa.selex-comms.com/internet/localization/IPC/media/docs/SWave-Handheld-Radio-v1-2012Selex.pdf
[44] NATO (2018): i. m. 2–21.

8. ábra

Futuro Soldato rendszer viselhető számítógépe és kijelzői

Forrás: www.leonardocompany.com/o/adaptive-media/image/3276609/h_480/original_LRT_440_new.jpg

3. Következtetések

Az ismertetett rendszerek közös jellemzője, hogy az egymás közötti kommunikációra VHF és UHF rádiókat használnak. De az alkalmazott készülékek között jelentős különbségek vannak. A táblázat a használt rádiók frekvenciatartományait mutatja be.

1. táblázat

A bemutatott rendszerekben használt rádiók frekvenciatartományai

Forrás: a szerző szerkesztése

Rendszer	Gyártó	Típus	Frekvenciatartomány
Nett Warrior	Thales	AN/PRC-154A	• UHF: 225–450 MHz L sáv: 1250–1390 MHz; 1750–1850 MHz
Félin	Thales	TRC-9100	• VHF: 30–88 MHz
VOSS	Elbit System	PNR-1000	• UHF: 225–512 MHz
ISSP	Harris	RF-7850S	• UHF: 225–512 MHz
IdZ-ES	Thales	SOLAR 400 EG-E	• UHF: 225–400 MHz
NORMANS	Harris	RF-7800S-TR	• UHF: 350–450 MHz
Futuro Soldato	Selex ES	Swave	• VHF: 30–300 MHz • UHF: 300–512 MHz

Látszik az adatokból, hogy a hét rádióból hat között lehetséges a kommunikáció, mert van közös frekvenciatartományuk, és a NATO vezetési rendszereiben alkalmazott

rádiókészülékek esetében előírás az F3 üzemmódú rádióforgalmazás.[45] Így, ha korlátozottan is, de együtt tudnak működni. A Félin esetében ez sajnos nem mondható el.

A használt központi egységek között megtalálható COTS eszköz, de még jellemzőbb a saját fejlesztés.

2. táblázat

A bemutatott rendszerekben használt kommunikációs protokollok

Forrás: a szerző szerkesztése

Rendszer	**Gyártó**	**Típus**	**Kommunikációs protokollok.**
Nett Warrior	Samsung	Galaxy S9	802.11 a/b/g/n/ac, Bluetooth, NFC, USB Type-C 3.1
Félin	Sagém	PEP	USB
VOSS	Elbit System	Raptor	USB, USB OTG és RS232
ISSP	Saab	Spad	–
IdZ-ES	Thales	NavICom	–
NORMANS	Thales	Normans	USB és RS232 / USB 2.0 és USB OTG, Ethernet, RS232, RS422, RS485, Bluetooth 2.1, EDR, 802.11g
Futuro Soldato	Larimart	LRT-440	Ethernet, USB, RS-232, Bluetooth, Audio AC97[46]

Azok a rendszerek, amelyek rendelkeznek külső rendszerek felé adatátviteli támogatással, azoknál általános az USB-protokoll támogatása. Ez megteremti az IoT rendszerekkel való kommunikációs lehetőséget egy illesztő modul alkalmazásával. Ezzel kihasználható az IoT katonai alkalmazásának egyik legnagyobb előnye, hogy nagy méretű szenzorhálózat építhető ki. Így a korábbi megoldásoktól eltérően sokkal több adat gyűjthető az ellenségről, illetve a harctéri környezet változásáról.[47] Ezenkívül több rendszer támogatja a vezetékes átvitelek közül az RS-232 protokollt, a vezeték nélküli átvitelek közül a Bluetooth és a 802.11 támogatása jellemző.

A kijelzőknél a négy coll alatti az általános, ami elég a szükséges információk megjelenítéséhez. De megkülönböztethetjük a lövész és a parancsnok készletét. Ahol két értéket tartalmaz a táblázat, ott különbözik a két változathoz tartozó kijelző. A parancsnoki készlet tartalmaz nagyobb 5-6"-os kijelzőt, amit a vezetéshez szükséges többletinformáció megjelenítése indokol. Ez alól a Nett Warrior COTS eszköze kivétel, amely egységesen a nagyobb kijelzőt tartalmazza.

[45] Hóka Miklós: *A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO-tagországok rádiórendszereinek vizsgálata tükrében.* Doktori (PhD-) értekezés. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2005. 52.

[46] LRT-440 System. *Larimart.it* (é. n.).

[47] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialógus Campus, 2018. 111.

3. táblázat
A bemutatott rendszerekben használt EUD-k kijelzőinek méretei
Forrás: a szerző szerkesztése

Rendszer	Gyártó	Típus	Kijelző mérete
Nett Warrior	Samsung	Galaxy S9	5,8"
Félin	Sagém	SITCOMDE	?
VOSS	Elbit System	Raptor	4,3"
ISSP	Saab	Spad	3,7"
IdZ-ES	Thales	NavICom	-/?"
NORMANS	Thales	Normans	2"/5"
Futuro Soldato	Larimart	LRT-440	3,5"/6,4"[48]

4. Összegzés

Ebben a cikkben bemutattam az amerikai, a francia, a holland, a kanadai, a német, a norvég és az olasz hadsereg által rendszeresített moduláris, integrált katona rendszerek C4I alrendszereinek összetevőit. Összehasonlítottam a használt rádiók frekvenciatartományát, az alkalmazott központi egységek kommunikációs protokolljait és a felhasználói végberendezések kijelzőinek méreteit. Ez a rövid áttekintés segítség lehet a digitáliskatona-rendszerek IoT eszközökkel való bővítésének vizsgálatához. További kutatásaimat ebben az irányban kívánom folytatni.

Felhasznált irodalom

9Land Battle Management System. *Saab.* Online: www.saab.com/products/9land-bms
ADR ATAK Plugin. *Ds2.com.* Online: www.ds2.com/solutions/atak
Balcik, Chris: Government and Industry Meet to Transform Tactical Operations. *Samsung Insights,* 2019. február 15. Online: https://insights.samsung.com/2019/02/15/government-and-industry-meet-to-transform-tactical-operations/
Chmielewski, Mariusz – Jaroslaw Koszela: The Concept of C2 Systems Data Integration for Planning Joint Military Operations Based on JC3 Standard. In *Conference: Military Communications and Information Systems Conference MCC'2008 Volume: 1.* 2008. Online: www.researchgate.net/publication/233859423_THE_CONCEPT_OF_C4I_SYSTEMS_DATA_INTEGRATION_FOR_PLANNING_JOINT_MILITARY_OPERATIONS_BASED_ON_JC3_STANDARD/link/0fcfd50c45e428514f000000/download
Defensie (X) voor het jaar 2015. Online: www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vjui9jaz40x1

[48] LRT-440 System. (é. n.) i. m.

Dixon, Alex– Julia Henning: Nett Warrior gets new end-user device. *Army.mil,* 2013. július 23. Online: www.army.mil/article/107811/nett_warrior_gets_new_end_user_device

Dutch Army Procures Elbit XACT nv32 micro Night Vision Systems. *Defense World,* 2020. december 19. Online: www.defenseworld.net/news/28590/Dutch_Army_Procures_Elbit_XACT_nv32_micro_Night_Vision_Systems#.YJMBaOe8pPY

Előházi János: Védelmi célú informatikai rendszerek feladatai és fenyegetettségei a hálózatközpontú hadviselésben. *Hadmérnök,* 2. (2007), 3. 70–80. Online: www.hadmernok.hu/archivum/2007/3/2007_3_elohazi.html

Falcon III® RF-7850S SPR™ Advanced Wideband Secure Personal Radio. *L3Harris.* Online: www.l3harris.com/all-capabilities/falcon-iii-rf-7850s-sprtm-advanced-wideband-secure-personal-radio

Farkas Tibor: A védelmi tevékenységeket támogató MH Kormányzati Célú Elkülönült Hírközlő Hálózat fejlesztési lehetőségeinek vizsgálata a honvédelmi és haderőfejlesztési program (Zrínyi 2026) tükrében – Hazai/nemzetközi szakirodalmi összefoglaló. *Hadtudományi Szemle,* 12, (2019), 4. 5–16. Online: https://doi.org/10.32563/hsz.2019.4.1

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289. Online: https://doi.org/10.2478/raft-2020-0034

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15. Online: https://doi.org/10.2478/raft-2021-0002

Farkas Tibor – Hronyecz Erika: Digitális Katona Rendszer a Katasztrófavédelmi Műveletekben. *Műszaki Tudományos Közlemények,* 7. (2017), 147–150. Online: https://doi.org/10.33895/mtk-2017.07.29

Government of Canada: *Integrated soldier system project* (é. n.). Online: www.canada.ca/en/department-national-defence/services/procurement/integrated-soldier-system-project.html

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialógus Campus, 2018.

Haig Zsolt: *Információs műveletek.* prezentáció. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/infoops-i.original.pdf

Haig Zsolt – Várhegyi István: *Hadviselés az információs hadszíntéren.* Budapest, Zrínyi, 2005.

Hóka Miklós: *A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO-tagországok rádiórendszereinek vizsgálata tükrében.* Doktori értekezés. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2005. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9747/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y

Håland, Walter Christian: FÉLIN – Future Infantry Soldier System, France. *Small Arms Defense Journal,* 9. (2017), 3. Online: www.sadefensejournal.com/wp/felin-future-infantry-soldier-system-france/

IdZ (Infanterist der Zukunft) Future Soldier System. *Army Technology* (é. n.). Online: www.army-technology.com/projects/idz/

Jobbágy Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő. *Hadmérnök,* 12. (2017), 1. 203–213. Online: https://doi.org/10.32567/hm.2017.1.16

Leonardo Company: *C4I SYSTEMS* (2018). Online: www.leonardocompany.com/documents/20142/3163315/body_Land_Naval_C4I_Systems_LQ_mm08781_.pdf

Leonardo: *Selex ES signs new contracts worth around €60m for the Italian Army's „Soldato Futuro" programme* (2014. március 25.). Online: www.leonardocompany.com/en/press-release-detail/-/detail/sdr-italian-army

LRT-440 System. *Larimart.it.* Online: www.larimart.it/en/computers-displays/wearablel-solutions/

Milliken, Dan – José Collazo: USB 3.1 Capabilities and Considerations for the Dismounted Soldier. In *Power Sources 2018 Digest.* 2018. 219–221. Online: www.powersourcesconference.com/Power Sources 2018 Digest/docs/12-5.pdf

NATO: *Overview of Dismounted Soldier Systems.* The NATO Science and Technology Organization, (2018). Online: https://apps.dtic.mil/sti/pdfs/AD1064371.pdf

Négyesi Imre: COTS rendszerek alkalmazási lehetőségeinek vizsgálata. *Hadtudományi Szemle,* 4. (2011), 4. 111–116. Online: http://epa.oszk.hu/02400/02463/00011/pdf/EPA02463_hadtudomanyi_szemle_2011_4_111-116.pdf

NORMANS pursues core functionality. *Soldier Modernisation,* 2008. Online: www.soldiermod.com/summer-08/prog-normans.html

Parlementaire Monitor: *Brief regering; D-brief over het project Verbeterd Operationeel Soldaat Systeem (VOSS) – Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2015.* Online: www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vjui9jaz40x1

Portable Electronic Platform – A Digital Brain Integrates with FELIN. *Defense Update,* 2006. június 20. Online: https://defense-update.com/20060620_felin-com.html

Rheinmetall – leading supplier of soldier systems and expert partner for network-enabled operations. *EDR online,* 2019. szeptember 10. Online: www.edrmagazine.eu/%E2%96%BA-rheinmetall-leading-supplier-of-soldier-systems-and-expert-partner-for-network-enabled-operations

SAFRAN: 'Boar's Head' Exercise with the British Army: FELIN makes European début. *Soldier Modernisation,* 9. (2012), 32–35.Online: www.soldiermod.com/volume-9/safran-sagem.html

Soldato Futuro: Concept, Development and Experimentation Phase Begins. *Soldier Modernisation,* 7. (2011), június. Online: www.soldiermod.com/volume-7/soldato-futuro.html

Thatcher, Chris: Instant impact: Integrated soldier system suite will change platoon and company tactics. *Canadian Army Today,* 2018. november 26. Online: https://canadianarmytoday.com/instant-impact-integrated-soldier-system-suite-will-change-platoon-and-company-tactics/

The office of the Director, Operational Test and Evaluation: Nett Warrior. *Director, Operational Test and Evaluation* (DOT&E), 2015. Online: www.dote.osd.mil/Portals/97/pub/reports/FY2015/army/2015nettwarrior.pdf

Valpolini, Paolo: The Netherlands: VOSS close to delivery. *EDR online,* 2018. október 30. Online: www.edrmagazine.eu/the-netherlands-voss-close-to-delivery

Valpolini, Paolo: Soldier systems evolution by Rheinmetallhe. *EDR online,* 2019. szeptember 19. Online: www.edrmagazine.eu/soldier-systems-evolution-by-rheinmetall
VOSS begins in earnest. *Soldier Modernisation,* 2008. Online: www.soldiermod.com/summer-08/prog-voss.html
Withington, Thomas: Time to Accessorize. *Armada International,* 2017. július 26. Online: https://armadainternational.com/2017/07/time-to-accessorize/
World Premiere for SAAB Soldier C2 and personnal radio integration at MSPO 2012. *Army Recognition,* 2012. szeptember 8. Online: www.armyrecognition.com/mspo_2012_show_daily_news_pictures_video_uk/world_premiere_for_saab_soldier_c2_and_personnal_radio_integration_at_mspo_2012.html

HADMÉRNÖK
FÓRUM
16. évfolyam (2021) 4. szám 201–214.
DOI: 10.32567/hm.2021.4.15

Mészáros István,[1] Bognár Balázs[2]

Üzletmenet-folytonossági tervezés kórházi környezetben I.

Üzleti hatáselemzés

Business Continuity Planning in a Hospital Environment 1

Business Impact Analysis

Hazánkban 2016-ban kezdődött meg az egészségügyi ágazatban, azon belül is fekvőbeteg-ellátás alágazatban a létfontosságú rendszerelemek azonosítása és kijelölése. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, illetve végrehajtási rendelete, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet, a kijelölt rendszerelemek üzemeltetői számára Üzemeltetői Biztonsági Terv készítését írják elő. Az üzemeltetői biztonsági tervezéshez bevált, nemzetközi gyakorlatban alkalmazott ISO 22301 szabvány áll rendelkezésre, amely az üzletmenet-folytonossági menedzsmentrendszerek *(business continuity management system,* BCMS) tervezését írja le. Az egészségügyi ágazatra vonatkozó további előírásokat az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet határozza meg. A közigazgatásban és így az egészségügyben a profitorientált, így a „termelés" fenntartására fókuszáló szemléletmód gyakorlati alkalmazása nem megszokott, a profit és a termelés fogalma nehezen alkalmazható. A tanulmány a BCM alapjainak, a Stakeholder-elemzés és az üzleti hatáselemzés *(business impact analysis,* bia) közegészségügyben történő alkalmazási lehetőségeit vizsgálja.

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, doktori hallgató, e-mail: meszaros.istvan.mail@gmail.com
[2] Vas Megyei Katasztrófavédelmi Igazgatóság, igazgató, e-mail: balazs.bognar@katved.gov.hu

Kulcsszavak: **létfontosságú rendszerelem, kritikusinfrastruktúra-védelem, egészségügy, fekvőbeteg-ellátás, üzemeltetői biztonság, üzletmenet-folytonosság, stakeholderelemzés, üzleti hatáselemzés**

In Hungary, the identification and designation of the critical infrastructures of the healthcare sector began in 2016, including the inpatient care sub-sector. Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities and its implementing decree, Government Decree 65/2013 (III.8.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities requires operators of designated system components to prepare an Operator Security Plan. The ISO 22301 standard, which has been proven in international practice for operator security planning, is available and describes how professionals can design Business Continuity Management Systems (BCMS). Additional requirements for the health sector are set out in Government Decree 246/2015 (IX.8.) on the identification, designation and protection of health-critical systems and facilities. In public administration and thus in the healthcare sector, the practical application of a profit-oriented approach, and the focusing on the maintenance of 'production', is not the common practice. The concepts of profit and production are difficult to apply. The study examines the fundamentals of BCM, thus the Stakeholder Analysis and Business Impact Analysis (BIA) in public health.

Keywords: **critical infrastructure protection, healthcare sector, in-patient care, operational safety, business continuity, Stakeholder-analysis, business impact analysis**

1. Problémafelvetés

Hazánkban a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.), illetve végrehajtási rendelete, a 65/2013. (III. 8.) Korm. rendelet (Vhr.) a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szabályozza a kritikus infrastruktúrák, azaz a létfontosságú rendszerelemek azonosításával, kijelölésével és védelmével kapcsolatos feladatokat. A jogszabály a már beazonosított és hatósági határozattal kijelölt létfontosságú rendszerelem üzemeltetője számára többek között Üzemeltetői Biztonsági Terv (ÜBT) készítését és folyamatos felülvizsgálatát írja elő. Az ÜBT alapvető tartalmi elemeit az Lrtv. 2. sz. mellékletében határozta meg a jogalkotó. Ezenkívül egyes ágazati jogszabályok további kötelező tartalmi elemeket írhatnak elő. Jelen tanulmányban tárgyalt egészségügyi ágazat, fekvőbeteg-ellátás alágazatára vonatkozó további előírásokat az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet határozza meg.

Az ÜBT készítése, a versenyszférában a nemzetközi szakmai terminológia alapján a *Business Continuity Planning* (BCP) tervezési gyakorlatra, azaz az üzletmenet-folytonossági átfogó megközelítésű szemléletre épül, amely alapvetően vállalatirányítási, folyamatalapú megközelítés, dinamizmust ad a tervnek és a terv „karbantartásának". Ezt a dinamizmust pedig az alapfolyamatok azonosítása és az azok ciklikus igazgatása, azon belül is ciklikus tervezése adja.

Az ilyen típusú tervezési és irányítási feladatokra leginkább a szabványosított minőségirányítási rendszerek alkalmasak. Az üzletmenet-folytonossági tervezési és irányítási rendszer alapjait az MSZ EN ISO 22301:2020 *Társadalmi biztonság, Üzletmenet-folytonossági irányítási rendszerek* című szabvány írja le.

Jelen tanulmányban a szabvány közegészségügyi, azon belüli is a fekvőbeteg-ellátó környezetbe történő bevezetésének lehetőségeit kívánom megvizsgálni, megalapozni, az üzletmenet-folytonossági szemléletmód és a tervezés első lépéseinek rendszerbe illesztésével.

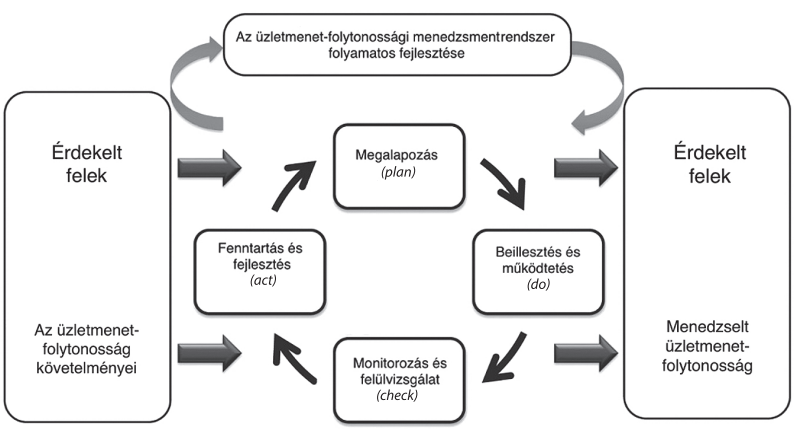
2. Az üzletmenet-folytonossági rendszer fenntartásának ciklikussága

Az igazgatás és a közigazgatás is ciklikus folyamatokra épül, amelyek biztosítják, hogy a megfelelően kitűzött célt a megfelelő erőforrások bevonásával érjük el, az egyes ciklusokat, kifejezetten a végrehajtást ellenőrizzük, hatékonyságát mérjük, és akár az adott folyamatot, akár a ciklust újrakezdve a megfelelő módosító intézkedéseket megtegyük. A közigazgatás ciklikusságát a szakirodalom két, egymással ekvivalens képlettel írja le, ezek a

- POSDCoRB *(planning, organizing, staffing, directing, co-ordinating, reporting, budgeting)*, és a
- CITDöVKE (célkitűzés, információszerzés, tervezés, döntés, végrehajtás, koordinálás, ellenőrzés)

A két képlet, bár más-más szemszögből és részfolyamatokat kiemelve fedi le teljesen az igazgatás ciklikusságát, látható, hogy a tervezés, a végrehajtás és annak irányítása, a visszaellenőrzés és a ciklus újraindításával a beavatkozás meghatározó elemei.

A minőségirányítási rendszerek ciklikus igazgatása szintén ezeket az alapelemeket rögzíti. Az ISO minőségirányítási rendszerek alapja a minőségirányítási ciklus, amelyet klasszikusan a PDCA *(plan, do, check, act)* képlettel ír le a szabvány.



1. ábra

Üzletmenet-folytonossági rendszerek fenntartásának folyamata

Forrás: MSZ EN ISO 22301:2020 *Társadalmi biztonság, Üzletmenet-folytonossági irányítási rendszerek.* 19.

3. A tervezést megelőző lépések

Jelen tanulmány a tervezés előtti első lépéséig, az üzleti hatáselemzés rendszerbe illesztéséig elemzi a szabvány szerinti folyamatokat.

A tervezést megelőzően, ahogyan a fent tárgyalt igazgatási ciklusok is meghatározzák, célkitűzés és információszerzés, illetve a vizsgált, tervezett rendszer, folyamat megfigyelése, elemzése szükséges. A szabvány ezt az üzleti hatáselemzéssel és kockázatértékelések készítésével éri el.

Azonban a két folyamat lefolytatása előtt, kifejezetten egy közigazgatási rendszerben, a fekvőbeteg-ellátásban elengedhetetlen a célok kijelölése, az üzleti folyamatok azonosítása, ami jelentősen meghatározza a teljes rendszerfenntartási ciklus minden elemét.

3.1. Célkitűzés: Mit tervezek?

„Az egészségügyi létfontosságú rendszerelemek esetében fennálló üzemeltetői biztonsági tervezési feladatok és az egészségügyi válsághelyzeti tervezési feladatok egymáshoz és magához a rendkívüli eseményhez fűződő viszonyainak megértéséhez az ún. kritikus infrastruktúra eseményciklus áttekintésével, értelmezésével juthatunk el."[3]

2. ábra

Kritikus infrastruktúra eseményciklus

Forrás: a szerző szerkesztése

A rendkívüli esemény, amely köré a ciklus épül a jogszabály szerint:

- „a létesítmény, intézmény esetében előreláthatóan 2 órát meghaladó közműkimaradás,

[3] Major László: *A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai.* Budapest, Semmelweis, 2019. 66.

- az infrastruktúrát érintő, külön jogszabályban meghatározott minden olyan esemény, amely a működéshez szükséges feltételek leállásához vagy az alaptevékenység átalakításához vezet,
- az infrastruktúrát érintő, külön jogszabályban meghatározott minden olyan rendkívüli esemény, amely a működéshez szükséges feltételek leállásához vagy az alaptevékenység átalakításához vezet,
- az, ha az illetékes hatóság a kijelölt létfontosságú rendszerelemnél egészségügyi zárlatot rendel el,
- a humánerőforrás olyan mértékű kritikus hiánya, ami a tevékenység leállításához, szüneteltetéséhez vezethet."[4]

„A rendkívüli esemény előtti időszak tervezési feladatai, az üzemeltetői biztonsági tervezésen keresztül kiterjednek a rendkívüli eseményt megelőzendően követendő üzemeltetői magatartásra, szervezési feladatokra, illetve ezen folyamatok kockázatainak folyamatos mérésére, értékelésére és már az üzemeltetői biztonsági tervezésen kívül, az adott szervezet ügyrendjének megfelelő beavatkozásokra is. Ebben az időszakban szükséges megalkotnunk a külső vagy belső indíttatású rendkívüli esemény során, illetve bekövetkezése után az esemény kezeléséhez, a kár elhárításához, mérsékléséhez és a helyreállításhoz, illetve az ezek melletti továbbüzemeltetéshez szükséges magatartásokra, szervezési feladatokra vonatkozó terveket és eljárásrendeket is"[5]

3. ábra

A védelmi típusú tervek egymásra épülése

Forrás: Brenda D. Phillips – Mark Landahl: *Business Continuity Planning: Increasing Workplace Resilience to Disasters.* Oxford, Elsevier, 2021. 13.

[4] 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[5] Major (2019): i. m. 66.

A védelmi tervezés tehát ideális esetben egy esemény bekövetkezése előtt preventíven történik, és a rendkívüli esemény emberi életre és a működés alapfolyamataira gyakorolt lehetséges hatásainak csökkentésére irányul.

3.2. Célkitűzés: Minek a védelmére tervezek?

A létfontosságú rendszerelemek sajátja, hogy e létesítményeknek, az itt zajló folyamatoknak minden körülmények között működnie kell, hiszen az azonosítás és kijelölés feltételrendszere alapján e folyamatok működtetése elengedhetetlen az ország gazdasága, társadalma szempontjából. A tervezés, a védelem fókuszpontjában tehát a rendszerelem alapvető folyamatai, a szabvány alapján „üzleti folyamatai" kell hogy álljanak.

Minden új igazgatási rendszer bevezetésekor elsődleges fontosságú a döntési és intézkedési kompetenciával rendelkező menedzsment bevonása és meggyőzése.

Az üzletmenet-folytonossági tervezés támogatása érdekében szükséges, hogy a menedzsment tisztában legyen a rendszer bevezetésének előnyeivel.

- A küldetés teljesítése. Szervezeteket különféle célokra hoznak létre, a gyártástól a szolgáltatásig. Minden esetben alapvetés a profit termelése.
- A pénzügyi eredmény. Talán az a legfontosabb előnye a BCP-rendszereknek, hogy egy-egy rendkívüli esemény után az alapfolyamatok visszaállítása menynyi idő alatt és milyen költségek mellett érhető el, illetve a termelés leállása milyen profitkiesést eredményez.
- A veszteség mérséklése. A BCP-folyamat a potenciális veszteségek alapos vizsgálatát igényli a környezeti veszélyek és fenyegetések esetleges bekövetkezése esetére.
- Ügyfélalapú szemléletmód. A hatóságok, a vállalkozások, a szervezetek az ügyfelekre, vevőkre támaszkodnak, szükséges, hogy az ügyfelek, a betegek, a hallgatók túléljék a katasztrófát és visszatérjenek a szolgáltatás igénybevételéhez.
- Humán erőforrás. Minden vállalkozás elsődlegesen azokra az emberekre támaszkodik, akik ott dolgoznak. Mivel a vállalkozások az emberi erőforrásaikba fektetnek be, a vállalkozások etikai felelőssége igen nagy nemcsak az emberek, hanem a befektetett idő és költségek megóvása érdekében is.[6]

Az üzletmenet-folytonossági tervezés fenti alapvetései új szemléletmódot hozhatnak a fekvőbeteg-ellátó kritikus infrastruktúrák tervezési gyakorlatába, azonban véleményem szerint ez a szemléletmód tovább formálandó, finomítható, bővíthető. Elsősorban azonosítani szükséges, hogy mit vizsgálok, minek a védelmére tervezek, tehát mi az alapfolyamatom. Természetesen lehet mérni a pénzügyi veszteséget is, azonban egy egészségügyi létfontosságú rendszerelem esetében nem jöhet szóba, hogy egy-egy zavaró hatás, rendkívüli esemény, katasztrófaesemény alapfolyamatokra gyakorolt hatását üzleti mérlegeredményben mérjem. Természetesen ezek a szempontok is

[6] Phillips–Landahl (2021): i. m. 16–18.

vizsgálandók az igazgatási ciklus során az erőforrások tervezése, rendelkezésre állása szempontjából. Azonban le kell szögezni, hogy egy fekvőbeteg-ellátó intézmény esetében az egyetlen profit, amelynek termelésére védelmi tervet készíthetek, az a betegellátás folytonossága. Tanulmányomban ezen alapfolyamatra támaszkodva kívánom bemutatni a folyamatorientált BCP-rendszerek bevezetésének lehetőségeit.

3.3. Információszerzés: Kivel tervezek?

A bevonáshoz elsősorban az értékgazdák, azaz a stakeholderek azonosítása szükséges, hiszen a tervezést, az alapfolyamatok és részfolyamataik elemzését a későbbiekben velük fogjuk elvégzeni.

Az alábbi módszertan alapján végezhető el egy fekvőbeteg-ellátó intézmény általános stakeholderelemzése, amelyben egyesével felsoroljuk, azonosítjuk és elemezzük a fontosabb külső és belső szereplőket.

Példa egy stakeholder tulajdonságainak értékelésére:

1. táblázat

Stakeholderelemzés táblázatos megjelenítésének részlete

	Személyes érintettség	**Támogatás mértéke**	**Befolyás a változásra**	**Befolyásolhat általunk**
(Fő)igazgató	Nagy – elkötelezett a klinikája/kórháza iránt	Támogató – eszközrendszerén belül mindent megtesz a működésért	Közepes – költségvetési keretek között a központi irányítás elvei mentén	Alig – szervezeti egysége irányításáért felel, vezetőként úgy érzi, minden helyzetben képes irányítani

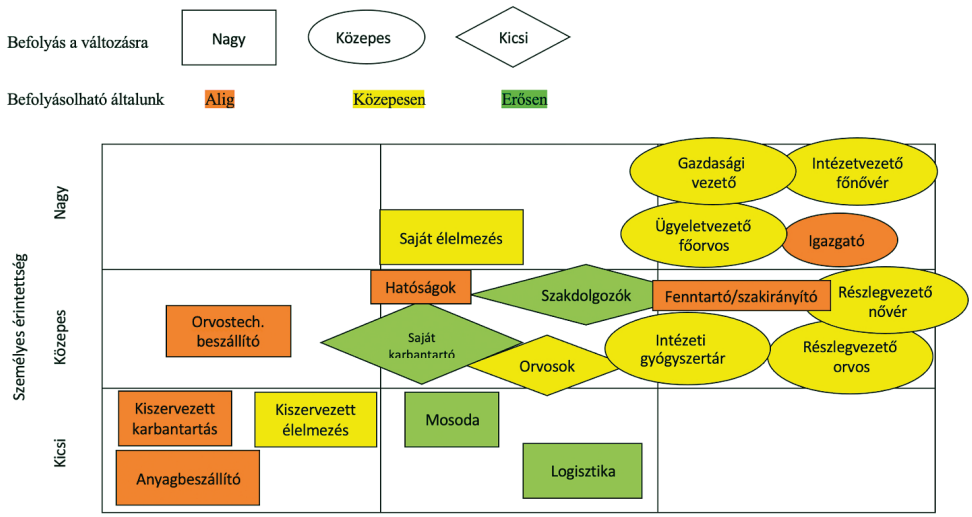
Forrás: a szerző szerkesztése

A fenti elemzés vizuális megjelenítése során az értékgazdák elhelyezhetők egy olyan koordináta-rendszerben, amely a jelölésekkel kvázi négydimenzióssá tehető.

Ebben a koordináta-rendszerben a résztvevők személyes érintettsége és a támogatásuk mértéke alapján elhelyezhetők, és ebből a két értékből egyértelműen azonosítható, hogy a tervezés során stratégiai vagy operatív módon kell őket bevonni, esetleg kizárólag utasítás adása, illetve szerződéses kötelmeik megkövetelése a feladatunk.

A szín és a forma meghatározza, hogy a tervezés során mennyire hagyatkozhatunk az elképzeléseikre, szokásaikra, reflexszerű reakcióikra, illetve a tervezés után a befolyásolhatóság alapján milyen módon és mértékben szükséges számukra a tervet visszaoktatni, módosítani a reakcióikat.

Az alábbiakban példa látható egy átlagos fekvőbeteg-ellátó intézmény stakeholder-elemzésének vizuális megjelenítésére.



4. ábra

Stakeholderelemzés vizuális megjelenítése

Forrás: a szerző szerkesztése

Az elemzés már rávilágít a rendszer függőségeire, és azonosítja az ellátási lánc kiemelt és kritikus szereplőit is. Az elemzés után az értékgazdákkal interjúk készítése szükséges, aminek javasolt módszertana a jobb felső sarokból lefelé és balra indulva elkészíteni az interjúkat, hiszen ezen értékgazdáknak a legnagyobb a személyes érintettsége, a leginkább támogató az attitűdjük, és ezek által ők ismerik leginkább a rendszerelem folyamatait.

3.4. Információszerzés: Üzleti hatáselemzés (business impact analysis, BIA)

Az üzleti hatások elemzése lehetővé teszi a szervezet számára, hogy prioritásokat állítson fel a megzavart tevékenységek folytatásához. Fő célja, hogy lehetővé tegye a szervezet számára minden olyan tevékenység azonosítását és rangsorolását, amely sürgős beavatkozásra szorulhat, amennyiben megszakad vagy megzavarják, mert az adott tevékenység gyors folytatásának, helyreállításának elmulasztása elfogadhatatlan szintű káros hatásokat eredményezhet.[7]

[7] MSZ EN ISO 22301:2020 *Társadalmi biztonság, Üzletmenet-folytonossági irányítási rendszerek.* 20.

Az üzleti hatáselemzés öt lépése:

- vezetői támogatás megszerzése;
- a szervezet megértése;
- BIA-eszközök alkalmazása;
- BIA-folyamat;
- BIA-eredmények.

Az üzleti hatáselemzés fő céljai:

- az üzleti hatáselemzés (BIA) szükséges az üzletmenetfolytonosság-menedzsmentrendszer fejlesztéséhez;
- kulcsfontosságú a szervezet kontextusának megértéséhez;
- az üzleti hatáselemzés azonosítja a szervezet üzleti funkcióinak pénzügyi és működési veszteségét;
- adatokat szolgáltat a maximálisan tolerálható leállás (*maximum tolerable downtime,* MTD), helyreállítási idő célok (*recovery time objectives,* RTO) és a helyreállítási pont céljainak (*recovey point objectives,* RPO) megállapításához;
- a BIA alapot nyújt a menedzsment számára a legköltséghatékonyabb folytonossági stratégiák kiválasztásához;
- azonosítja a megelőzés, a felkészültség, a reagálás, az enyhítés és a helyreállítás hiányosságait.[8]

Ehhez elsősorban az értékgazdákkal folytatott interjúkon keresztül juthatunk el. Az interjúk célja a fenti definíciónak megfelelően a mindennapi műveletek, az erőforrásigények, a kötelezettségek és egy zavaró esemény lehetséges hatásainak feltárása.

Az interjúkon kívül további alkalmazandó módszerek:

- dokumentációk felülvizsgálata;
- felmérés, kérdőív készítése;
- műhelyvita megtartása;
- forgatókönyv-alapú gyakorlat megtartása és értékelése.[9]

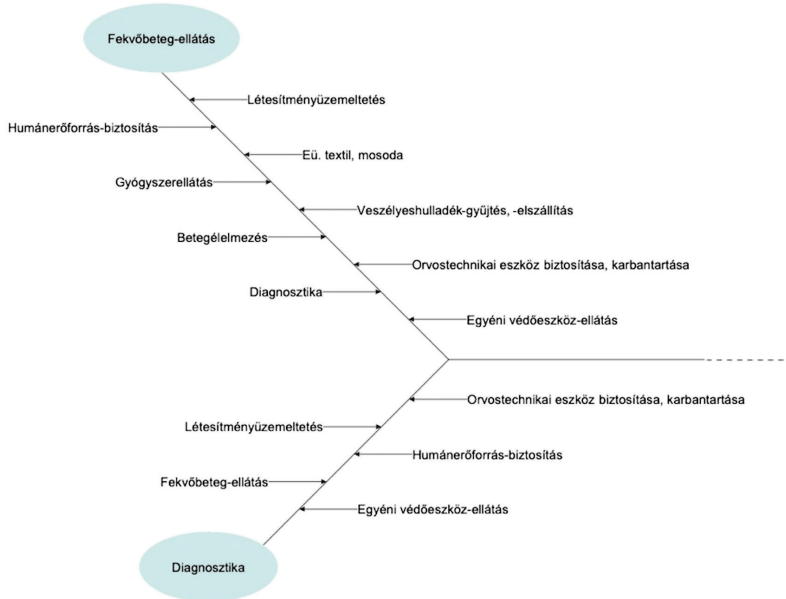
3.4.1. Folyamatábrák

Az információszerzés során beszerzett információk alapján az üzleti hatáselemzés folytatásához, a feltárt folyamatok szemléltetéséhez célszerű folyamatábrákat készíteni, amelyeken jelöljük az azonosított alap- és részfolyamatokat, amelyek hatáselemzését elvégezzük.

Egy általános kórház/klinika azonosított folyamatait az alábbi ábrák szemléltetik:

[8] Eugene Tucker: *Business Continuity from Preparedness to Recovery.* Oxford, Elsevier, 2021. 70.

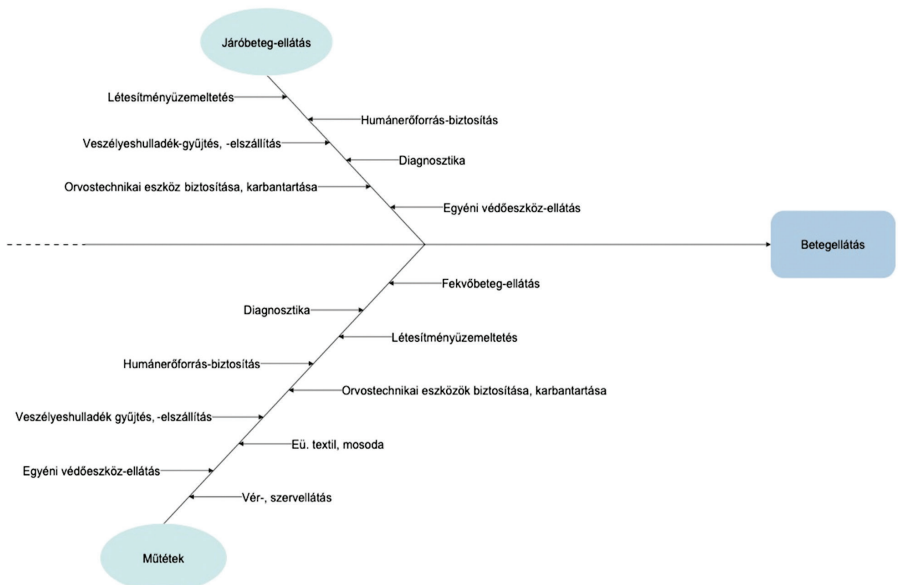
[9] ISO/TS 22317:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA) – Annex C 20.



5. ábra

Kórházi alapfolyamatok azonosítása – ábra 1. része

Forrás: a szerző szerkesztése



6. ábra

Kórházi alapfolyamatok azonosítása – ábra 2. része

Forrás: a szerző szerkesztése

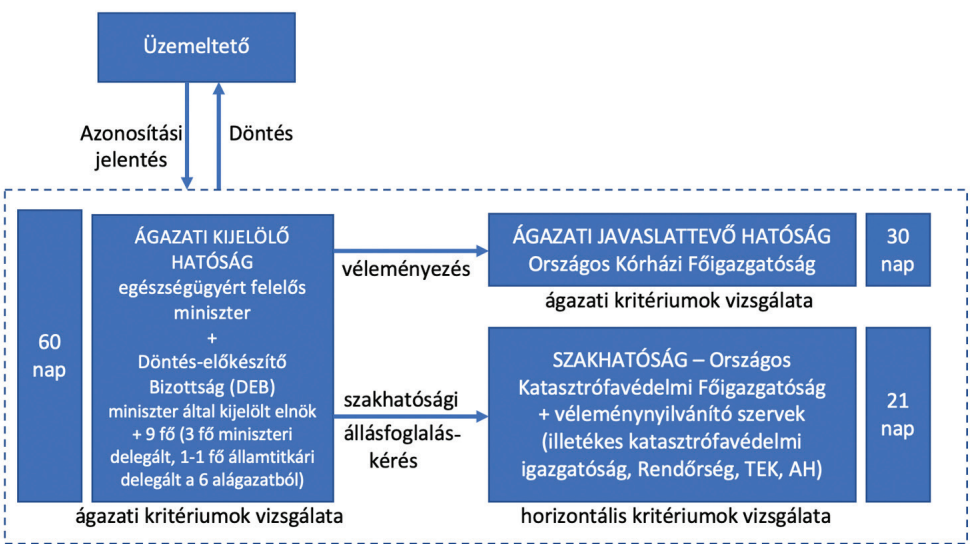
A folyamatábrából nemcsak az alapfolyamatot támogató kritikus folyamatok, hanem az azokat támogató részfolyamatok is látszanak. A tervezést az összes részfolyamatra el kell végezni, még akkor is, ha a részfolyamatok többsége megjelenik több alapfolyamatnál is. Azonban ugyanazon részfolyamat megzavarásának különböző hatásai lehetnek az adott alapfolyamatra, illetve a helyreállítási értékek meghatározása is eltérhet, amire az adott részfolyamatok esetében az adott alapfolyamatnak megfelelően kell tervezni.

Ezen túl az ábrából az egyes folyamatok dependenciái is jól látszanak. Ezt jól szemlélteti például a diagnosztika és a fekvőbeteg-ellátás kölcsönös függősége, hiszen a fekvőbeteg-ellátás során a további terápia, illetve a beteg státusának meghatározásához különböző diagnosztikai eljárásokra (labor, képalkotó stb.) van szükség, a diagnosztizált kórkép pedig szükségessé teheti a beteg fekvőbeteg-ellátásba történő utalását. Ezen interdependenciák további vizsgálatot követelnek meg a tervezés során.

3.4.2. Kritikusság rangsorolása

A kritikusság rangsorolása a folyamatok mérőszámokkal történő ellátását jelenti, amelyhez kritériumrendszer felállítása szükséges. A kritikusság rangsorolása elsősorban az alapfolyamatunk, az elérendő célunkra gyakorolt hatás alapján tehető meg, ami természetesen megköveteli, hogy az adott folyamatra értelmezve tegyük meg. Azonban a kritériumrendszer meghatározásához a jogszabályi környezet is ad alapot, amely meghatározza a létfontosságú rendszerelemmé történő kijelölés horizontális és ágazatspecifikus kritériumait is.

Az azonosítási eljárás során a döntésben részt vevő szervek e kritériumrendszer alapján döntenek a létfontosságú rendszerelemmé történő kijelölésről.



7. ábra

Azonosítási eljárás a fekvőbeteg-ellátó alágazatban

Forrás: a szerző szerkesztése

A Vhr. alapján a horizontális kritériumok:

- a veszteségek kritériumai;
- a gazdasági hatás kritériuma;
- a társadalmi hatás kritériuma;
- a politikai hatás kritériuma;
- a környezeti hatás kritériuma;
- és a védelem kritériuma.

Elengedhetetlen, hogy ezt a komplex kritériumrendszert a menedzsment is képes legyen kórházi környezetben, az azonosított folyamatokra alkalmazni. Így továbbra is a betegellátás áll a fókuszban. Nehéz ebben az esetben az egyes zavarok hatását mérhetővé tenni, hiszen ha a betegek ellátását, gyógyulását vesszük alapul, akkor nyilvánvalóan nem mérhető és nem is elfogadható annak mérése, hogy egy-egy zavaró hatás esetében hány beteg nem gyógyul meg, esetleg az elmaradó kezelés hatására milyen negatív személyes következmények érik. Ellenben a folyamatok, részfolyamatok vizsgálata során az országos ellátás, illetve az adott intézmény területi ellátási kötelezettségi szintjén az azonosított folyamat egészében, illetve további részfolyamatokra bontásával vizsgálható, hogy milyen esetben, melyik folyamat, milyen mértékű veszteséget szenvedhet.

Jó példa erre a jelenlegi koronavírus okozta világjárvány, amelyre bár nem léteztek tervek, a szakirányítás döntéseiben mégis az üzleti hatáselemzés folyamatai azonosíthatók. A koronavírus-megbetegedésben szenvedő betegek ellátásának biztosítása érdekében (humánerőforrás- és ágykapacitás-biztosítás) először a szűrővizsgálatokat, majd később a nem akut ellátást igénylő fekvőbeteg-ellátási formákat és műtéti tevékenységeket függesztették fel. A megfelelő tervezés azonban elengedhetetlen, mert bár a folyamatok kritikusságának rangsorolása a szakirányító által ad hoc módon is megtörténhet, tervezni szükséges a leállított folyamatok hosszú távú hatásaival, megállapítandó többek között a leállás maximálisan tolerálható értéke a fenti kritériumrendszer alapján.

3.4.3. A tolerálható leállás és visszaállítás mérőszámai

A fentiek alapján tehát minden egyes folyamatra és részfolyamatra meg kell határozni és értékkel kell ellátni a maximálisan tolerálható leállás mértékét, a helyreállítási pontot, ahol még a helyreállítás megkezdhető és a szükséges helyreállítási időt.

A folyamatok azonosítása után a leginkább érintett, stratégiai értékgazdákkal szükséges meghatározni az alábbi értékeket minden egyes folyamatra:

- MAO *(maximum tolerable outage)*/MTD *(maximum tolerable downtime)*: az adott folyamat maximálisan tolerálható kiesése;
- RTO *(recovery time objective)*: a helyreállításhoz szükséges idő;
- RPO *(recovey point objective)*: a helyreállítási pont, ahol a folyamat helyreállítása az RTO figyelembevételével az MTD-n belül megtörténhet.

Ezen értékek meghatározása és rangsorolása után kezdődhet csak a kockázatértékelés.

4. Összefoglalás

Az egészségügyi ágazat és alágazatai létfontosságú rendszereinek és rendszerelemeinek, jogszabály által előírt, üzemeltetői biztonsági tervezésében a szemléletmódváltás elérhető. A tervezés, illetve az üzemeltetés hatékonysága növelhető minőségirányítási rendszerek, azon belül is az üzletmenet-folytonossági menedzsmentrendszerek alkalmazásával.

A szemléletmódváltás szükségességére rámutatnak a jelenlegi koronavírus-világjárvány okozta veszélyhelyzet körülményei, lefolytatott komplex egészségügyi válsághelyzeti gyakorlatok kiértékelései és az egészségügyi infrastruktúrák magas biztonsági szinten történő folyamatos üzemeltetésének napi kihívásai.

Az üzletmenet-folytonossági menedzsmentrendszereket külföldön nemcsak a kritikus infrastruktúrák esetében, hanem azon kívül is alkalmazzák, hiszen ezek a menedzsmentrendszerek biztosítják és tartják fenn a szervezet igazgatásának ellenőrzött ciklikusságát. Ez az alapfolyamatok működésbiztonságának és így a profit maximalizálásának, minden körülmények között történő fenntartásának, a kiesés minimalizálásának szem előtt tartásával történik. Az egészségügyi ellátó rendszerekben, azonban nemcsak a szabvány alkalmazásához, hanem a szabvány értelmezéséhez is szemléletváltás szükséges. Egy fekvőbeteg-ellátó intézmény esetében a profit nem értelmezhető, nem mérhető pénzügyi mérlegeredményben. A profit ebben az esetben az alaprendeltetés biztosítása, a gyógyító/rehabilitáló tevékenység folyamatossága, a betegek ellátása. Amennyiben ehhez a típusú profithoz a betegellátást mint célt és alapfolyamatot azonosítjuk, a működés fenttartásának többi folyamata erre rászervezhető, mérhető és védelmi szempontból tervezhető rendszerré állhat össze.

Az üzletmenet-folytonossági rendszerek működtetésének első mérföldköve a tervezés, amelyet azonban a célkitűzésnek és az információszerzésnek meg kell előznie. Ehhez elsődleges fontosságú a menedzsment meggyőzése, az értékgazdák azonosítása, akik megfelelő információkkal tudnak ellátni és a tervezésben is részt vesznek. Ezen értékgazdákkal közösen azonosítandók az alapfolyamatok és azok zavarainak üzleti hatáselemzése, tehát az alapfolyamatra gyakorolt hatásának feltárása. Az üzleti hatáselemzés után kezdődhet csak a kockázatértékelés, amelynek minden egyes folyamatra ki kell terjednie, és amelyben a megállapított maximálisan elfogadható leállási értékek alapján rangsorolhatók a kritikus nyomvonalak, az egyes kockázatok, fenyegetések. Az azonosított kockázatokra a kritikusság rangsorolása, az interdependenciák figyelembevétele, illetve a tolerálható leállási és szükséges helyreállítási idő alapján készülhet el a komplex intézkedési terv, majd léphetünk ki a tervezés fázisából.

Felhasznált irodalom

ISO/TS 22317:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA).

Major László: *A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai.* Budapest, Semmelweis, 2019.

MSZ EN ISO 22301:2020 *Társadalmi biztonság, Üzletmenet-folytonossági irányítási rendszerek*.
Phillips, Brenda D. – Mark Landahl: *Business Continuity Planning: Increasing Workplace Resilience to Disasters*. Oxford, Elsevier, 2021. Online: https://doi.org/10.1016/B978-0-12-813844-1.00009-9
Tucker, Eugene: *Business Continuity from Preparedness to Recovery*. Oxford, Elsevier, 2021.

Jogi források

1997. évi CLIV. törvény az egészségügyről
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
521/2013. (XII. 30.) Korm. rendelet az egészségügyi válsághelyzeti ellátásról
246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

HADMÉRNÖK
FÓRUM
16. évfolyam (2021) 4. szám 215–231.
DOI: 10.32567/hm.2021.4.16

Zsákai Zsolt[1]

Az emberi térd, csípő és gerinc biomechanikai jellemzői, valamint terhelés hatására létrejött elváltozásainak áttekintő elemzése

2. rész: A térdízület biomechanikája

An Overview of the Biomechanical Characteristics of the Human Knee, Hip and Spine, as well as the Changes Caused by Exercise

Part 2 – Biomechanics of the Knee Joint

Cikksorozatom második részében a térdízület biomechanikai elemzését végzem. Irodalmi példákon fogom bemutatni, hogy a megnövekedett terhelés, testsúly, genetika és egyéb tényezők milyen nagy hatással vannak a térdpanaszok kialakulására. A kiképzéssel és bevetéssel járó megterhelés ellensúlyozására fontosnak tartom a megfelelő preventív szempontok alapján történő stratégia kialakítását, növelve ezáltal a kezelés hatékonyságának fokát, végeredményként pedig csökkentve a térdbetegségek kialakulásának kockázatát.

Kulcsszavak: **térdízület, biomechanika, degeneratív betegség, térd arthrosis, keresztszalag sérülés**

In the second part of my article series, I perform a biomechanical analysis of the knee joint. I will use examples from the literature to show what a significant effect increased load, body weight, genetics and other factors have on the development of knee complaints. To counterbalance the burden of training and deployment,

[1] Borsod-Abaúj-Zemplén Megyei Központi Kórház és Egyetemi Oktató Kórház, főorvos, e-mail: zsakaizsolt@zsakaizsolt.com

I consider to develop a strategy based on appropriate preventive factors to be important, thereby increasing the effectiveness of treatment and ultimately reducing the risk of developing knee diseases.

Keywords: **knee joint, biomechanics, degenerative disease, knee arthrosis, cruciate ligament injury**

1. Bevezetés

Doktori kutatásomban az aktív katonai állomány mozgásszervi panaszait vizsgálom. Cikkemben szeretnék képet adni a térdízületet jellemző biomechanikai sajátosságokról és a túlterheléssel összefüggő problémák fontosságáról. Az anatómiai és biomechanikai ismeretek, valamint az egyes betegségek leírását csak a szükséges mértékben kívánom bemutatni, hangsúlyozva, hogy sem kutatásom, sem jelen írásom nem ezek részleteiben hivatott elmélyülni, ugyanakkor a könnyebb érthetőség kedvéért feltétlenül fontosnak tartom fentiek ismertetését. Bízom benne, hogy szakirodalmi példákkal alátámasztva szemléltetni tudom a probléma fontosságát, a prevenció és a hatékony, időben elkezdett kezelések szükségességét. Meggyőződésem, hogy megelőzéssel és korai, hatékony kezelésekkel a panaszok súlyosbodásának kockázata, valamint a panaszok megszűnése után az aktív szolgálatba való visszatérés ideje csökkenthető.

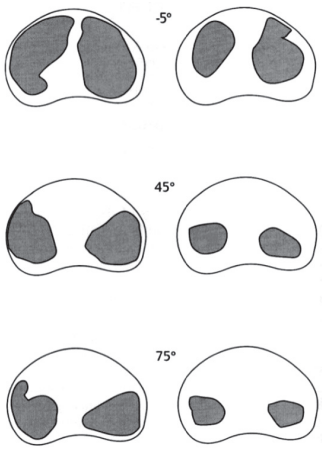
2. A térdízület anatómiája

A térdízület 3 részből álló, úgynevezett trochoginglymus ízület, amelyet a térdkalács és a combcsont közti *(patellofemoralis)* rész, valamint a belső és külső combcsont–lábszárcsont illeszkedő felszínei *(medialis* és *lateralis femorotibialis)* alkotnak. A combcsont térdízületet adó részének külső és belső felszínei *(medialis* és *lateralis femurcondylusok)* kisebb görbülettel rendelkeznek, mint a lábszárcsont ízfelszíneinek *(tibiacondylusok)* megfelelő vájulata, ezért csak kis felszínen érintkeznek egymással, és mozgás közben mind csúszó, mind pedig gördülő mozgást végeznek.[2] Az ízületet szalagok stabilizálják. Az oldalszalagok – külső *(lateralis)* és belső *(medialis)* – az oldalirányú kitéréseket akadályozzák meg és így biztosítják a térd ilyen irányú stabilitását. A keresztszalagok (elülső és hátulsó keresztszalag) részt vesznek a térdízület oldalstabilizálásában, a lábszárcsont *(tibia)* előre, illetve hátrafelé csúszásának megakadályozásában, valamint biztosítják a gördülő-csúszó mozgás tengelyét.[3] Az ízületi porcfelszínek közti csúszó mozgás együtthatója 0,005 és 0,02 közötti értékben található, ami gyakorlatilag azt jelenti, hogy csúszó hatás szinte alig érvényesül. Ez az alacsony súrlódás rendkívül fontos a térdízület mechanikájában.[4]

A centrális stabilizáló elemeknek, a térdközi porcgyűrűnek *(meniscusoknak)* és a keresztszalagoknak nagyon fontos szerepük van térdünk biomechanikájában. A meniscusok

[2] Szendrői Miklós (szerk.): *Ortopédia.* Budapest, Semmelweis, 2005. 355.
[3] Szendrői (szerk.) (2005): i. m. 356.
[4] J. Charnley: The Lubrication of Animal Joints in Relation to Surgical Reconstruction by Artrhroplasty. Annals of *Rheumatic Diseases,* 19. (1960), 1. 10–19.

az ízfelszínek közti téraránytalanságot csökkentik és a terhelési felületet növelik. Ezt szemlélteti az 1. ábra.



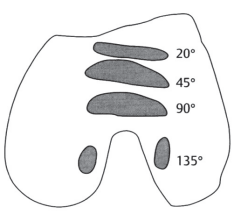
1. ábra

A meniscusok jelenléte és azok nélküli térdízületi érintkezési felszín sematikus ábrázolása a térd különböző hajlított helyzeteiben

A kép bal oldalán látható a meniscusok jelenlétében, jobb oldalon pedig azok hiányában kialakuló érintkezési felület. Látható, hogy a meniscusok milyen jelentős mértékben megnövelik az ízületben az érintkezési felszínt, ezáltal optimális nyomásviszonyokat hoznak létre.

Forrás: Brinckmann, Paul – W. Frobin – Gunnar Leivseth: *Musculoskeletal Biomechanics.* Stuttgart – New York, Thieme, 2002. 86.

A combcsont–térdkalács közti ízületben *(patellofemoralis)*,[5] a térdkalács és a szemben fekvő combcsont porcrésze közti érintkezési felszínen nincs teljes, a porcfelszín egészére kiterjedő érintkezés.[6] Ezt a 2. ábra szemlélteti, ahol látható, hogy különböző hajlítási *(flexio)* tartományok során hol és milyen területen érintkezik a két porcfelszín egymással.



2. ábra

A patellofemoralis ízület érintkezési felszíne a térdízület különböző hajlítottsági állapotában

A patellofemoralis ízületben, a térd különböző hajlított helyzetében létrejövő érintkezési felszínek sematizálása során látható, hogy ebben az ízületrészben – 20, 45, 90 és 130 fokos helyzetben ábrázolva – a porc csak kis területére esik nyomás.

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 87.

[5] A patellofemoralis ízület térdünk külön tárgyalandó része, amelyet a betegségek, térdízületi panaszok, illetve biomechanikai jellemzők alapján is önálló entitásként kell kezelni.

[6] B. B. Seedholm et al.: Mechanical Factors and Patellofemoral Osteoarthrosis. *Annals of the Rheumatic Diseases,* 38. (1979), 4. 307–316.

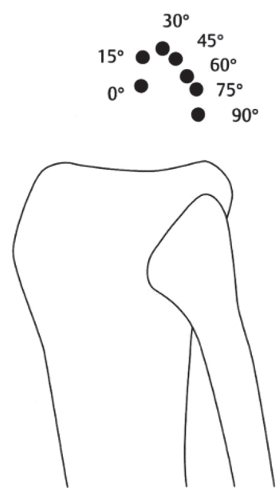
3. A térdízület biomechanikai összefüggései

A térdízület fő mozgása a hajlítás és a nyújtás *(flexio* és *extensio)*. Egészséges szalagrendszerrel rendelkező térdízületnél oldalirányú mozgás nincs, a hajlításon és nyújtáson kívül minden más irányba történő mozgathatóság kórosnak számít. A hajlítás *(flexio)* mértéke egyénenként változik, értéke körülbelül 130°.[7]

A térdízület is kétkarú emelőként viselkedik, amelynek tengelye, a combcsont condylusai anatómiai kitüremkedéseinek összekötéséből *(epicondylusok)* adódó tengely. Azonban a forgástengely két oldalán két különböző nagyságú erő hat, különböző hosszúságú erőkarokkal, így csak abban az esetben tud megfelelően működni, ha a két erő forgatónyomatéka egyenlő. A combcsont condylusainak főbb része a súlyvonal mögött helyezkedik el, a lábszárcsont ízfelszíne pedig a vízszinteshez képest 5-7 fokban lejt. Ez a helyzet azt biztosítja, hogy a járás bizonyos fázisában a combcsont ne csússzon előre a lábszárcsont ízületi felszínén.

Az anatómiai részben is említettük, de fontossága miatt szeretném megint hangsúlyozni, hogy térdünk megfelelő mozgásához a térdízület szalagrendszerének épsége elengedhetetlen, azok stabilizáló szerepe nélkül megbomlik a normál biomechanikai egység.

Mérések alapján a térd forgástengelye nem állandó tengely, hanem folyamatosan változik a különböző hajlítottsági tartományokban. Ezen változásokra a 3. ábra mutat példát.[8]



3. ábra

Különböző mértékű flexionál a térdízület forgástengelyének elhelyezkedése

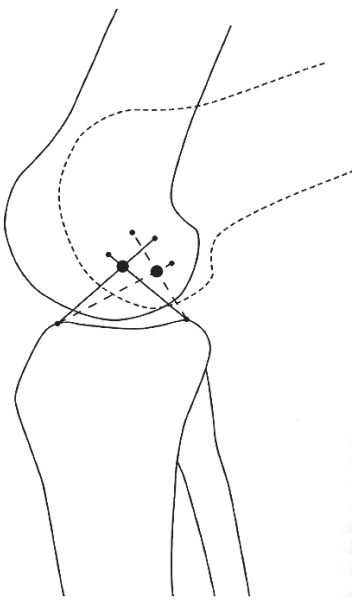
0, 15, 30, 45, 60, 75, 90 fokos flexio esetén a térd forgástengelyének sematikus ábrázolása.

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 88.

[7] Szendrői (szerk.) (2005): i. m. 356.

[8] Gary L. Smidt: Biomechanical Analysis of Knee Flexion and Extension. *Journal of Biomechanics,* 6. (1973), 1. 79–92.

A csúszó-gördülő mozgás kivitelezéséhez nagyon jól megalkotott biomechanikai összhang szükséges, amelyet részben a csontok anatómiai kialakulása, részben pedig a szalagok stabilizációja lát el.[9] Menschik vizsgálatából tudhatjuk, hogy a flexio különböző fázisaiban, a keresztszalagok kereszteződési pontja adja a pillanatnyi rotációs tengelyt abból adódóan, hogy a keresztszalagok hossza állandónak tekinthető. Ha az oldalszalagok által meghatározott rotatios tengelyt is megvizsgáljuk, akkor látni fogjuk, hogy a pillanatnyi rotációs centrumot ez a tengely szintén keresztezi flexio folyamán.[10] Ennek szemléltetésére a 4. és 5. ábra szolgál.

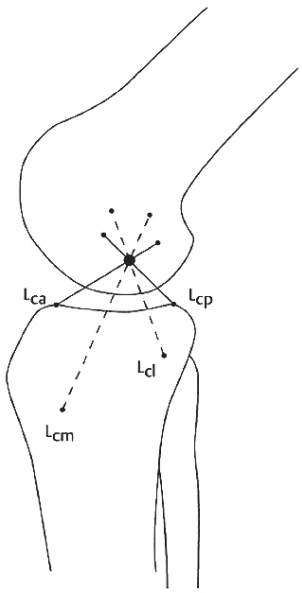


4. ábra

A keresztszalagok által kialakított rotációs tengely

A keresztszalagok által „vezetett" rotációs központ változása.

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 88.



5. ábra

Az oldalszalagok által meghatározott rotációs tengely viszonya a keresztszalagok által meghatározott rotációs tengelyhez

Az aktuális, keresztszalagok által meghatározott forgáspont egybeesik az oldalszalagok rotációs pontjával egészséges biomechanikai és anatómai helyzet esetben. L_{ca}: elülső keresztszalag *(ligamentum cruciatum anterius)*; L_{cp}: hátulsó keresztszalag *(ligamentum cruciatum posterius)*; $L_{cm:}$ belső oldalszalag *(ligamentum collaterali tibiale)*; L_{cl}: lateralis oldalszalag *(ligamnetum collaterale fibulare)*

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 89.

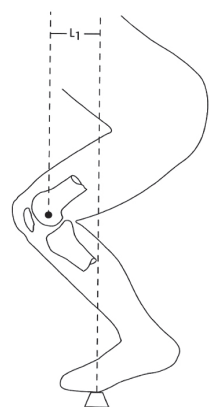
[9] A csontos anatómiai jellemzőre példa a lábszárcsont ízfelszínének 5-7 fokos hátrafelé irányultságú lejtése, valamint, hogy a combcsont condylusainak főbb része a súlyvonal mögött helyezkedik el.

[10] A. Menschik: Mechanik des Kniegelenks. Teil 1. *Z. Orthop,* 112. (1974), 448–495.

Fuss tanulmányában tovább finomította a korábbi méréseket és megállapította, hogy flexio során csak a keresztszalagok egy része kerül feszültség alá.[11] Woo és munkatársai szerint az életkor előrehaladtával a keresztszalagok erőbíró képessége gyengül.[12] Piazza és Cavanagh vizsgálata pedig nyilvánvalóvá tette, hogy a térd extensiója során, annak az utolsó 20 fokos tartományában, a tibia a hossztengelye mentén egy körülbelül 15 fokos kifordulást *(kirotatiot)* hajt végre a nem pontosan illeszkedő ízületifelszín-egyezés *(kongruencia)* miatt.[13] A korábbi kutatások mérési eltéréseit is ezzel a mozgásjelenséggel magyarázta.

Látható, hogy térdünk egyszerűnek tűnő mozgása során – amelyet külső szemlélőként hajlítás-nyújtás váltakozásaként írhatunk le – tulajdonképpen csúszó-gördülő-forduló mozgás jelenik meg. Térdünk működése elengedhetetlen életmódunkban, hiszen helyváltoztató mozgásunk egyik fő terhelő ízülete. Azonban vizsgálatakor a terhelés mértékétől, illetve az erőbehatásoktól függően kell értelmezni az alap biomechanikai összetevőket, hiszen a térdpanaszok kialakulásában, különösen a túlterhelődéssel járó betegségek megjelenésében, ezeknek van hatalmas szerepe.

A térdízület terhelésére jellemző, hogy a benne fellépő nyomás a térd hajlított állapotától is függ. A testre ható gravitációs erő erőkarja a térdízület forgó központjához viszonyítva majdnem nulla nyújtott térdízület és egyenes testtartás esetén, majd fokozatosan nő a térd hajlítása során. A gravitációs erő centruma hajlított térdízülettel történő állásnál az előlábat terheli, a térdhez viszonyítva pedig a térdízülettől hátrébb elhelyezkedő síkban *(posterior)* helyezkedik el, ahogy azt a 6. ábra is mutatja.



6. ábra

A gravitációs központ helyzete a térdhez viszonyítva hajlított térddel való állás esetén

L_1: a gravitációs erő erőkarja. A térd hajlítottsági állapotától függően, nyújtott törzs esetén változik a törzsre ható gravitációs erő erőkarja.

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 91.

[11] Franz K. Fuss: Anatomy of the Cruciate Ligaments and Their Function in Extension and Flexion of the Human Knee Joint. *American Jorunal of Anatomy,* 184. (1989), 2. 165–176.

[12] Savio L. Woo et al.: Tensile Properties of the Human Femur-Anterior Cruciate Ligament-Tibia Complex: The Effects of Specimen Age and Orientation. *The American Journal of Sports Medicine,* 19. (1991), 3. 217–225.

[13] Stephen J. Piazza – Peter R. Cavanagh: Measurement of the Screw-Home Motion of the Knee is Sensitive to Errors in Axis Alignement. *Journal of Biomechanics,* 33. (2000), 8. 1029–1034.

Az egyensúlyi helyzetet ebben a hajlított térdízülettel történő helyzetben a quadriceps izom biztosítja, amely egy fontos ínnal tapad a lábszárcsont tuberositasán. Itt szeretném megemlíteni a térdkalácsunk *(patella)* kialakulásának fontosságát. Mérésekkel igazolták, hogy ha nem lenne jelen a patella, akkor nagyobb izomerő kellene a megfelelő egyensúlyi helyzet kialakításához az ín lefutása miatt. A térdkalács megfelelő helyzete tehát fontos az izomműködés és a térd biomechanikája szempontjából, hiszen befolyásolja a térdben ható erőket.[14] A patella és combcsont közti ízületben a porcra ható erők eloszlanak a két ízületi felszín közt, és a térdízület hajlított állapotától függően más értéket mutatnak, amely erőnagyság az erőbehatás időtartamától is függ.[15] Ez annak a következménye, hogy hosszabb időtartamú nyomás fennállása esetén a porcszövetben kis mértékben deformálódik, emiatt pedig az érintkezési felszín növekszik.[16] A femoropatellaris ízületben végzett vizsgálatok egy részénél a porc alatti csontállomány sűrűségét *(densitását)* is vizsgálták és azt találták, hogy ebben a régióban megnövekedett a csont sűrűsége.[17] A térdkalács alatti ín *(ligamentum patellae)* irányával szintén összefüggést mutat a patellofemoralis ízületben fellépő erőnagyság. Az ín iránya ráadásul a lábszárcsont mozgás közbeni rotációja miatt relatívnak tekinthető a combcsonthoz viszonyítva, hiszen az elfordulás közben a térben leírható módon változik.[18]

Ebből a korántsem teljes képből is látható, hogy a térdízület mozgása nagyon bonyolult folyamat. A térdben fellépő erőhatások számos, együttesen fellépő hatás eredőjeként jönnek létre, amely folyamatban bármiféle eltérés kóros mozgást és ennek következtében betegségek, panaszok kialakulását eredményezheti. Nagyon fontos annak vizsgálata – a megelőzés szempontjából és a kezelési stratégiák kialakítása miatt egyaránt –, hogy mozgásszervrendszerünk milyen anatómiai, biomechanikai eltéréseket mutat, valamint, hogy ezen eltérések milyen hatással vannak a tünetek megjelenésére. A normál mozgás, az erőviszonyok és a biomechanikai jellemzők megismerése, valamint a terhelés során fellépő erők, biomechanikai hatások vizsgálata elengedhetetlen a kóros folyamatok megértése szempontjából, hiszen – mozgásszervrendszerünket egy egységként tekintve – egymással összefüggő viszonyrendszerről van szó.

Fajunk alapvetően egységes anatómiával rendelkezik, azonban kijelenthetjük, hogy mozgásszerveink számos egyedi anatómiai variációt hordoznak. Véleményem szerint ezen „egyediség" miatt a terhelés sablonszerű alkalmazása – nélkülözve az egyedi anatómiai, biomechanikai jellemzők feltérképezését és figyelembevételét – megnöveli a túlterhelés kockázatát. Ezen írásomban a térdízület összefüggéseit vizsgáltam, főként annak biomechanikai változását megnövekedett terhelés esetén.

[14] Paul Brinckmann – W. Frobin – Gunnar Leivseth: *Musculoskeletal Biomechanics.* Stuttgart – New York, Thieme, 2002. 90–97.

[15] A. M. Ahmed – D. L. Burke – A. Yu: In-Vitro Measurement of Static Pressure Distribution in Synovial Joints. Part II: Retropatellar Surface. *Journal of Biomechanical Engineering,* 105. (1983), 3. 226–236; H. J. Hehne et al.: Eine neue Methode zur Ermittlung lastabhangiger Druck- und Kontaktverlaufe an Grenzflachen. *Morphol Med.,* 1. (1981), 95–106; H. J. Hehne et al.: Analoge Druck- und Kontaktflachenmessung des Femoropatellargelenkes mit optisch sensibler Druckmessfolie. *Z Orthop,* 120. (1982), 513.

[16] Brinckmann–Frobin–Leivseth (2002): i. m. 96–97.

[17] M. Müller-Gerbl et al.: Die Darstellung der subchondralen Dichtemuster mittels der CT-Osteoabsortiometrie (CT-OAM) zur Beurteilung der individuellen Gelenkbeanspruchung am Lebenden. *Z Orthop.,* 128. (1990), 128–133.

[18] Brinckmann–Frobin–Leivseth (2002): i. m. 97.

Az irodalmat áttekintve számos utalást találtam arra vonatkozólag, hogy a túlterhelés következtében fellépő változások milyen negatív hatást okoznak ebben az anatómiai régióban.

Wikstrom és munkatársai tanulmányában olvashatjuk, hogy a női populációban szignifikánsan növekedett értékű a csípő nyújtás *(extensio)* és a térdhajlítás *(flexio),* valamint ezzel ellentétben a térd extensiója kisebb végértéket mutat hölgyek esetében. A flexio és extensio során fellépő izomerő mértéke a férfi populációban mértekhez képest csökkentebb. A vizsgálatokból az is kiderült, hogy az egyensúlyi helyzet fenntartásában a nők jobbak, mert hölgyek esetén a gravitációs központra ható erő- és testtömegarány kisebb. Ugyanakkor a férfiak az egyensúlyi feladatok nehézségi szintjének növelésével javuló értékeket mutattak azokban az esetekben, amikor dinamikus testtartási stabilitással összefüggő gyakorlatokról volt szó.[19]

Katelyn és munkatársai kimutatták, hogy a BMI-értékek, valamint a testzsírszázalék értékei a nők esetén magasabbak, valamint, hogy ugrás során a talajérési fázisban a hölgyek esetében nagyobb csípő flexio és térd oldalirányú eltérés *(valgisatio)* tapasztalható.[20]

Witvrouw és munkatársai tanulmányukban azt vizsgálták, hogy a fokozottabb terhelésnek alávetett atlétikai sportolók közt milyen arányban fordul elő patella íngyulladás, bizonyos faktorok, mint a combizomzat-feszesség, izomerő, valamint bizonyos antropometriai változók jelenlétében. Azt találták, hogy a combizomzat csökkent rugalmassága *(flexibilitás)* szignifikánsan patella íngyulladáshoz vezet megterhelés esetén.[21]

Szintén Witvrouw és munkatársai munkájában találhatjuk meg, hogy a combizomzatot és térdízületet nagyobb megterhelésnek kitevő labdarúgók esetén a megnövekedett combizomzat-feszesség, magasabb rizikótényezőt jelent mozgásszervi sérülések kialakulásában.[22]

Egy másik tanulmányukban Witvrouw és munkatársai leírták, hogy atlétikai sportolóknál a combizomzat feszessége, a belső combizomzat reflex válaszidejének megváltozása, a hipermobilis térdkalács[23] nagyobb kockázatot jelentenek az elülső térdfájdalmak kialakulásában.[24]

A professzionális sportolók, nehéz fizikai munkát végzők esetén végzett kutatások eredményei azért lehetnek az aktív katonai szolgálatot teljesítő állomány esetén is elfogadhatók – vagy legalábbis figyelemre méltók –, mert katonák esetén a mozgásszervrendszert érő megterhelések nyilvánvalóan nagyobbak, mint az átlag populációban. Ilyen irányú szakirodalmat kutatva például McWilliam és munkatársai

[19] Erik A. Wikstrom et al.: Gender and Limb Differences in Dynamic Postural Stability during Landing. *Clinical Journal of Sports Medicine,* 16. (2006), 4. 311–315.

[20] Katelyn F. Allison et al.: Musculoskeletal, Biomechanical, and Physiological Gender Differences in the US Military. *US Army Medical Department Journal,* (2015), 22–32.

[21] Erik Witvrouw et al.: Intrinsic Risk Factors for the Development of Patellar Tendinitis in an Athletic Population. A Two-Year Prospective Study. *The American Journal of Sports Medicine,* 29. (2001), 2. 190–195.

[22] Erik Witvrouw et al.: Muscle Flexibility as a Risk Factor for Developing Muscle Injuries in Male Professional Soccer Players. A Prospective Study. *The American Journal of Sports Medicine,* 31. (2003), 1. 41–46.

[23] Hipermobilis patella: a normálistól nagyobb mértékben eltérő oldalirányú mozgathatósága térdkalácsunknak.

[24] Erik Witvrouw et al.: Intrinsic Risk Factors for the Development of Anterior Knee Pain in an Athletic Population. A Two-Year Prospective Study. *The American Journal of Sports Medicine,* 28. (2000), 4. 480–489.

munkájából kiderül, hogy szignifikáns összefüggés van bizonyos nehezebb fizikai megterheléssel járó munkák, professzionális sporttevékenységek és a térdpanaszok kialakulása közt.[25] Deacon és munkatársai pedig a professzionális ausztrál labdarúgók esetén találtak vizsgálatuk során megnövekedett kockázatot a térd kopásának kialakulása szempontjából.[26]

Jordaan és munkatársa az alapkiképzésen részt vevő katonáknál vizsgálta a túlterheléses sérülések incidenciáját. Azt találták, hogy a legtöbb esetben a lábszárcsont stresszreakciója (stresszfájdalma) és a térdkalács környékén kialakult *(patellofemoralis)* fájdalom fordultak elő. Vizsgálatukból kiderült, hogy a sérülések több mint 80%-a a térdet, lábszárat és a bokát érintette.[27]

Culvenor és munkatársai szerint a futási technika optimalizálása és a fizikai terhelés során viselt brace[28] használata hatékonyan csökkenti a patellofemoralis fájdalom kialakulásának valószínűségét.[29]

Taanila és munkatársai közléséből tudjuk, hogy a katonai szolgálat idején, a 18–28 éves férfi katonák közt, a deréktájéki fájdalmak után az alsó végtagi fájdalmak fordultak elő leggyakrabban, valamint a visszatérően ismétlődő sérülések közül a hát és a térd sérülései jelentek meg a legnagyobb számban.[30]

Prodromos és munkatársai tanulmányukban leírták, hogy a kosárlabdázó és labdarúgó hölgyek esetén a férfiakhoz képest háromszor nagyobb valószínűséggel alakul ki elülsőkeresztszalag-sérülés. Kutatásukból kiderül, hogy röplabda esetén a kockázat e sérülés vonatkozásában alacsony.[31]

Reiman és munkatársai munkájából kiderül, hogy a csípőízület és annak mozgási, biomechanikai eltérései is a térdpanaszok és -sérülések kialakulásához vezethetnek.[32] Ez a tény pedig rendkívül érdekes összefüggésre mutat rá. Véleményem szerint nem csak célzottan az adott ízület vizsgálata, hanem komplex mozgásszervi státuszfelmérés szükséges, hogy képet kapjunk a kockázat mértékéről. A prevenció során ezen összefüggések felmérése nélkülözhetetlen a megfelelő, hatásos eredmények elérése érdekében.

Fentebb említettem, hogy térdünk alapvető funkciója a helyváltoztatásban mutatkozik meg leginkább. Járás során a saroktámasztást követő, a járásciklus 10%-át kitevő időszakban a csípőízületben hajlítás *(flexio)*, közelítés *(adductio)* és befelé

[25] D. F. McWilliams et al.: Occupational Risk Factors for Osteoarthritis of the Knee: A Meta-Analysis. *Osteoarthritis and Cartilage,* 19. (2011), 7. 829–839.

[26] Adam Deacon et al.: Osteoarthritis of the Knee in Retired, Elite Australian Rules Footballers. *Medical Journal of Australia,* 166. (1997), 4. 187–190.

[27] Gerhard Jordaan – Martin P. Schwellnus: The Incidence of Overuse Injuries in Military Recruits during Basic Military Training. *Military Medicine,* 159. (1994), 6. 421–426.

[28] Rögzítő (A szerző véleménye: Ortopédsebészeti, szakmai szemlélet alapján egy egészséges ízület rögzítésének szükségessége megosztja a szakma képviselőit. Ennek kifejtése külön kutatás keretén belül érdekes eredménnyel kecsegtet.)

[29] Adam G. Culvenor et al.: Is Patellofemoral Pain Preventable? A Systematic Review and Meta-Analysis of Randomised Controlled Trials. *British Jorunal of Sports Medicine,* 55. (2021), 7. 378–384.

[30] Henri Taanila et al.: Musculoskeletal Disorders in Physically Active Conscripts: A One-Year Follow-Up Study in the Finnish Defence Forces. *BMC Musculoskeletal Disorders,* 10. (2009), 1. 1–11.

[31] Chadwick C. Prodromos et al.: A Meta-Analysis of the Incidence of Anterior Cruciate Ligament Tears as a Function of Gender, Sport, and a Knee Injury-Reduction Regimen. *Arthroscopy,* 23. (2007), 12. 1320–1325.

[32] Michael P. Reiman – Lori A. Bolgla – Daniel Lorenz: Hip Functions Influence on Knee Dysfunction: A Proximal Link to a Distal Problem. *Journal of Sport Rehabilitation,* 18. (2009), 1. 33–46.

fordulás *(rotatio)* valósul meg. A flexio mértéke 0-2 fok az adductio és a befelé rotatio 10-15 fok.[33] Ha nő az aktivitás mértéke – például futás esetén, vagy emelkedőn történő járáskor –, akkor a nemek közti összehasonlító vizsgálatokban szignifikáns eltéréseket találhatunk: a nőknél fokozódnak ezen értékek. Nagyobb mértékű csípő adductio, befelé rotatio a térd középpontját a lábhoz viszonyítva medializálja, azaz valgisalódik a térd. Ezen irányú hatás a szalagokra és a patellofemoralis ízületre ró nagyobb terhelést, ami kialakító tényezője lehet az elülső keresztszalag szakadásnak[34] és patellofemoralis fájdalomnak.[35] Hollman és munkatársai vizsgálatukban szintén azt igazolták, hogy a csípőízület túlzott mértékű addukciója az érintett oldali térd dinamikus valgisalódásához vezethet.[36]

Ha másik anatómiai síkból *(sagittalis)*[37] vizsgáljuk az eredő erők alakulását, akkor azt látjuk, hogy ezek az erők a csípőízület előtt és a térdízület mögött hatnak, így mindkét ízületben flexiós hatást indukálnak. Ha ugrás során, a földet érés pillanatában törzsünk előre hajlított állapotban van, akkor a csípő feszítő izmaira *(extensorokra)* hat nagyobb megterhelés, ha egyenes helyzetben van törzsünk, akkor pedig a térd extensorokra.[38] Ebből könnyen látható, hogy a négyosztatú combizomban *(musculus quadriceps femoris)* húzódás, a patella ínban ínrendellenesség *(tendinopathia)* alakulhat ki és jelenhet meg panasz formájában.

Járáskor, futáskor az eredő erők úgy alakulnak, hogy a térd medialis kompartmentjére nagyobb erő esik, mint a lateralisra, ezáltal pedig az ott lévő porc terhelése fokozódik.[39] Mozgás során törzsünk helyzete, valamint a medence stabilitása fontos az alsó végtagi terhelés szempontjából. Egyes betegségekben vagy állapotokban a csípőtávolító izmok *(abductorok)* izomereje csökkent, ezért a támaszkodási fázisban az ellenoldali csípőt nem képesek megtartani, így az lebillen *(Trendelenburg-jel)*. Ennek következménye, hogy a törzs súlypontja – a középponthoz viszonyítva – átkerül a lengő végtag felé, ez pedig a támaszkodó végtag kifelé hajló *(varus)* irányú eltérését fokozza, ami a belső *(medialis)* ízületi résben túlterhelést okoz. Elmondható tehát, hogy a megfelelő mértékű csípő abductor izomerő csökkenti az ellenoldali csípő arthrosisának kialakulási valószínűségét.[40] A fenti esetben – de más okból kifolyólag is – az emberek törzsüket a támaszkodó oldal felé billentik ellensúlyozásképpen (kompenzatorikusan),

[33] G. Simoneau: Kinesiology of Walking. In Donald A. Neumann (szerk.): *Kinesiology of the Musculoskeletal System.* St Louis, MO, Mosby Inc., 2002. 523–569.

[34] Timothy E.Hewett et al.: Biomechanical measures of neuromuscular control and valgus loading of the Knee Predict Anterior Cruciate Ligament Injury Risk in Female Athletes: A Prospective Study. *American Journal of Sports Medicine,* 33. (2005), 4. 492–501.

[35] Christopher M. Powers: The Influence of Altered Lowerextremity Kinematics on Patellofemoral Joint Dysfunction: A Theoretical Perspective. *Journal of Orthopaedic & Sports Physical Therapy,* 33. (2003), 11. 639–646.

[36] John H. Hollman et al.: Relationships between Knee Valgus, Hip-Muscle Strength, and Hip-Muscle Recruitment during a Single-Limb Step-Down. *Journal of Sport Rehabilitation,* 18. (2009), 1. 104–117.

[37] Nyílirányú.

[38] E. B. Simonsen et al.: Mechanisms Contributing to Different Joint Moments Observed during Human Walking. *Scandinavian Journal of Medicine & Science in Sports,* 7. (1997), 1. 1–13; J. Troy Blackburn – Darin A. Padua: Sagittal-Plane Trunk Position, Landing Forces, and Quadriceps Electromyographic Activity. *Journal of Athletic Training,* 44. (2009), 2. 174–179.

[39] C. R. Winby et al.: Muscle and External Load Contribution to Knee Joint Contact Loads during Normal Gait. *Journal of Biomechanics,* 42. (2009), 14. 2294–2300.

[40] Alison Chang et al.: Hip Abduction Moment and Protection against Medial Tibiofemoral Osteoarthritis Progression. *Arthritis & Rheumatism,* 52. (2005), 11. 3515–3519.

ami szintén negatív következményekkel jár az érintett oldali térdben. Ilyenkor a térd valgisatiója fokozódik, visszahatásképpen pedig mindez a csípő abductorok erejének további csökkenését eredményezi.[41]

Látható, hogy a vizsgálatok egy része a nemek közti anatómiai, biomechanikai sajátosságokat kutatja. Az ilyen irányú kutatások eredményei azt támasztják alá, hogy a nemek közt különbséget nem tevő, egységesített edzésprotokoll megnövekedett kockázatot jelent a térd panaszainak és a sérülések kialakulását illetően. Célszerű olyan programok bevezetése, amelyek ezt az egyenlőtlen terhelést csökkentik és megadják a lehetőséget ezen kockázat mérséklésére. Kraemer és munkatársai vizsgálatából kiderül, hogy a nők esetén bevezetett fizikaierőnlét-növelő edzésprogram javította a hölgyek eredményeit a kiképzés során, így jobb teljesítményt értek el, mint a program nélküli esetekben.[42]

Showery és munkatársai az aktív szolgálatot teljesítő katonák esetén vizsgálta az elsődleges és másodlagos térdízületi arthrosis (térdízületi kopás) kialakulásának incidenciáját. Vizsgálatukból kiderült, hogy a magasabb katonai rang és életkor, a fekete rassz, valamint a légierőnél, illetve tengerészgyalogságnál történő szolgálat szignifikánsan növeli a térdkopás kialakulásának valószínűségét. Írásukban hangsúlyozták a megfelelő preventív eljárás kialakítását és bevezetését, a következményes térd osteoarthritis kialakulási valószínűségének csökkentése céljából.[43]

Murtha és munkatársai azt találták, hogy az ismétlődő térdtraumák okán kialakuló térdízületi kopás gyakori indikációja az 50. életkor alatti totál térdprotézis (TEP) beültetésének. Az elülsőkeresztszalag-sérülés, porckárosodás, meniscussérülés gyakran vezet korai porckopáshoz, amelynek súlyos, a karriert és a mindennapi életet is érintő következményei lehetnek. Az általuk vizsgált, TEP-beültetésen átesett esetek 74%-ánál volt valamilyen, a térdet érintő sérülés. A leggyakoribb sérülés az elülsőkeresztszalag-sérülés volt, amely, ha meniscusszakadással is társult, jelentősen felgyorsította a TEP-beültetés szükségességét. A térdben kialakult károsodás, majd az azt követő TEP-beültetés, a katonai szolgálatot teljesítőknél nagy százalékban (55%) jelentette a további szolgálatra alkalmatlannak történő nyilvánítását.[44]

Jiang és munkatársai tanulmánya szerint önmagában az elhízás, a megnövekedett BMI is fokozott kockázatot jelent a térdízületi kopás kialakulásában.[45]

Az elülsőkeresztszalag-sérülések vonatkozásában Magnussen és munkatársai is azt találták, hogy akik átestek keresztszalagpótláson, azoknál az átlag idő, amíg térdízületi TEP-implantációra került sor 25,7 év, az átlagéletkor pedig 58,1 év volt.[46]

[41] Ronald K. Lawrence et al.: Influences of Hip External Rotation Strength on Knee Mechanics during Single-Leg Drop Landings in Females. *Clinical Biomechanics,* 23. (2008), 6. 806–813.

[42] William J. Kraemer et al.: Effect of Resistance Training on Women's Strength/Power and Occupational Performances. *Medicine and Science in Sports Exercise,* 33. (2001), 6. 1011–1025.

[43] James E. Showery et al.: The Rising Incidence of Degenerative and Posttraumatic Osteoarthritis of the Knee in the United States Military. *The Journal of Arthroplasty,* 31. (2016), 10. 2108–2114.

[44] Andrew S. Murtha et al.: Total Knee Arthroplasty for Posttraumatic Osteoarthritis in Military Personnel Under Age 50. *Journal of Orthopaedic Research,* 35. (2016), 3. 677–681.

[45] Liying Jiang et al.: Body Mass Index and Susceptibility to Knee Osteoarthritis: A Systematic Review and Meta-Analysis. *Joint Bone Spine,* 79. (2012), 3. 291–297.

[46] R A. Magnussen et al.: Total Knee Arthroplasty for Secondary Osteoarthritis Following ACL Reconstruction: A Matched-Pair Comparative Study of Intra-Operative and Early Post-Operative Complications. *Knee,* 19. (2012), 4. 275–278.

Az elülsőkeresztszalag-sérülések, valamint az egyéb sporttal kapcsolatos sérülések a katonák esetén, a civil lakossághoz viszonyítva, tízszer gyakoribb előfordulást mutattak.[47]

Ahn és munkatársai munkájában olvashatjuk, hogy a katonai szolgálat idején elszenvedett elülsőkeresztszalag-sérülések az esetek 76,2%-ában a katonai tevékenységhez, edzéshez, kiképzéshez voltak köthetők, 23,8%-ban pedig egyéb napi elfoglaltság, például labdarúgás szerepelt kiváltó okként. Vizsgálatukból az is kiderül, hogy az adott tevékenység kezdetét követő 30 és 60 perc közti időablakban történtek a sérülések.[48]

Kaplan és munkatársai anatómiai és biomechanikai paraméterek (lábszár hossztengely, a lábszárcsont belső és külső ízfelszínének lejtése, a térd belső ízületi részének mélysége) vizsgálatával próbálták igazolni, hogy különböző nehézségű felszereléssel történő talajra érkezés során a térd elülsőkeresztszalag-rendszerére ható erők csökkenthetők-e azáltal, ha a talajfogás pillanatában az egyének növelik a térd behajlításának mértékét. Azt találták, hogy a flexio növelése jó stratégia lehet az elülsőkeresztszalag-sérülés kockázatának mérséklésére. Munkájukban klinikai relevanciát is megfogalmaztak. Véleményük szerint is fenti anatómiai, biomechanikai paraméterek szűrésével azonosíthatók lesznek azok a személyek, akik kiegészítő gyakorlatok bevezetésével csökkenteni tudják az alsó végtagi sérülések kockázatát.[49]

Természetesen katonák esetén a túlterhelés mellett a kiképzés során, illetve a harctéren szerzett sérülések is okozhatnak térdízületi problémákat. Rivera és munkatársai a civil lakossággal összehasonlítva vizsgálták a térdízületi kopás prevalenciáját térdtáji sérüléseket elszenvedett katonák esetén. Rámutattak, hogy a katonai szolgálat idején bekövetkezett, térdsérülések kapcsán kialakult térdarthrosis prevalenciája magasabb ebben a populációban.[50]

Stannard és munkatársa közleményéből kiderül, hogy a Különleges Műveleti Erőknél szolgálók közt a leggyakoribb sérüléseknek a boka, térd és deréktájéki gerinc bántalmai bizonyultak. Vizsgálatuk szerint a sérülések 68%-a kiképzés alatt alakul ki, amely során a fizikai tréning közben elszenvedett sérülések fordultak elő legnagyobb számban.[51]

A genetikai faktorok vizsgálata is azt mutatta, hogy bizonyos genetikai tulajdonságokkal rendelkező egyének nagyobb valószínűséggel válnak érintetté a térd degeneratív megbetegedéseinek vonatkozásában.[52] Ezzel is magyarázható a nem fehér rasszoknál kialakult nagyobb kockázat ténye, amelyet részben genetikai okokkal, részben pedig az eltérő BMI-vel és csontsűrűség-eltéréssel magyaráznak.[53]

---

47 Brett D. Owens et al.: Incidence of Anterior Cruciate Ligament Injury among Active Duty U.S. Military Servicemen and Servicewomen. *Military Medicine,* 172. (2007), 1. 90–91.

48 J. Ahn et al.: The Mechanism and Cause of Anterior Cruciate Ligament Tear in the Korean Military Environment. *Knee Surgery & Related Research,* 31. (2019), 13.

49 Jonathan T. Kaplan et al.: Association Between Knee Anatomic Metrics and Biomechanics for Male Soldiers Landing with Load. *American Journal of Sports Medicine,* 48. (2020), 6. 1389–1397.

50 Jessica C. Rivera et al.: Posttraumatic Osteoarthritis Caused by Battlefield Injuries: The Primary Source of Disability in Warriors. *Journal of the American Academy of Orthopaedic Surgeons,* 20. (2012), Suppl 1. S64-69.

51 Joanne Stannard – L. Fortington: Musculosceletal Injury in Military Special Operatiopns Forces: A Systematic Review. *BMJ Military Health,* 167. (2021), 4. 255–265.

52 Marc C. Hochberg et al.: Genetic Epidemiology of Osteoarthritis: Recent Developments and Future Directions. *Current Opinion in Rheumatology,* 25. (2013), 2. 192–197.

53 Ana M. Valdes – Tim D. Spector: Genetic Epidemiology of Hip and Knee Osteoarthritis. *Nature Reviews Rheumatology,* 7. (2011), 1. 23–32; Kay Chapman – Ana M. Valdes: Genetic Factors in OA Pathogenesis. *Bone,* 51. (2012), 2. 258–264.

A genetikai eltérések, testsúly, BMI, életkor figyelembevétele, az egyénre jellemző mozgásszervi anatómiai és biomechanikai jellemzők felmérése csökkentheti a kockázatot a későbbi térdpanaszok kialakulását tekintve. Ennek pozitív hatását célzó vizsgálatból (Dijksma és munkatársai) kiderül, hogy a mozgásszervi sérülések ellátása jelentős pénzügyi terhet jelent a költségvetésnek,[54] ami megítélésem szerint sem elhanyagolható tényező. Dijksma és munkatársai egy másik kutatása alapján kijelenthető, hogy lényeges és fontos annak a szemléletnek a kialakítása, amely – prevenció szempontjából – kedvezőbb kiképzési stratégiát követ.[55] Glaviano és munkatársai is arra a következtetésre jutottak, hogy az elülső térdfájdalom kialakulási kockázatának csökkentése érdekében a kutatások középpontjába kerülhetnek az intervenciós programok kidolgozását és a képzési követelmények felülvizsgálatát célzó vizsgálatok.[56] Az időben elkezdett kezelések fontosságát szintén nem e cikk keretén belül szeretném kifejteni, de a megelőzéssel párhuzamosan szükséges lehet egy korai kezelési protokoll felállítása is. Young és munkatársai közleményükben azt vizsgálták, hogy az elülső térdfájdalmak esetén a korai mozgásterápia csökkenti e fájdalmak kialakulásának valószínűségét. Tanulmányukban ugyanakkor leírják, hogy a katonák ilyen panaszokkal az esetek 62,3%-ában nem vettek igénybe kezelést, ami az időben elkezdett kezelés fontosságáról szóló felvilágosítás hatékonyságának növelését teszi szükségessé.[57] Véleményem szerint az aktív katonai szolgálat megkezdése előtt szélesebb körben kellene meghatározni és szűrni azokat a tényezőket, amelyek kockázatként szerepelhetnek a térdízületi problémák kialakulásában, mert a térdízület védelme fontos és meghatározó lehet nemcsak a panaszok megjelenése, hanem annak komplettálódása és az egyén későbbi élete, karrierje szempontjából is.

Felhasznált irodalom

Ahmed, A. M. – D. L. Burke – A. Yu: In-Vitro Measurement of Static Pressure Distribution in Synovial Joints. Part II: Retropatellar Surface. *Journal of Biomechanical Engineering,* 105. (1983), 3. 226–236. Online: https://doi.org/10.1115/1.3138410

Ahn, Joosuk – Byungseop Choi – Yong Seuk Lee – Ki Woung Lee – Jung Woo Lee – Beom Koo Lee: The Mechanism and Cause of Anterior Cruciate Ligament Tear in the Korean Military Environment. *Knee Surgery & Related Research,* 31. (2019), 13. Online: https://kneesurgrelatres.biomedcentral.com/articles/10.1186/s43019-019-0015-1

Allison, Katelyn F. – Karen A. Keenan – Timothy C. Sell – John P. Abt – Takashi Nagai – Jennifer Deluzio – Mark McGrail – Scott M. Lephart: Musculoskeletal, Biomechanical, and Physiological Gender Differences in the US Military. *US*

[54] Iris Dijksma et al.: Epidemiology and Financial Burden of Musculosceletal Injuries as the Leading Health Problem in the Military. *Military Medicine,* 185. (2020), 3–4. e480–e486.

[55] Iris Dijksma et al.: Exercise Programs to Reduce the Risk of Musculuskeletal Injuries in Military Personnel: A Systematic Review and Meta-Analysis. *PM&R,* 12. (2020), 10. 1028–1037.

[56] Neal R. Glaviano – Michelle C. Boling – John J. Fraser: Anterior Knee Pain Risk Differs Between Sex and Occupation in Military Tactical Athletes. *Journal of Athletic Training,* (2021), március 31.

[57] Jodi L. Young et al.: Usual Medical Care for Patellofemoral Pain Does Not Usually Involve Much Care: 2-Year Follow-up in the Military Health System. *Journal of Orthopaedic & Sports Physical Therapy,* 51. (2021), 6. 305–313.

Army Medical Department Journal, (2015), 22–32. Online: https://pubmed.ncbi.nlm.nih.gov/26101903/

Blackburn, J. Troy – Darin A. Padua: Sagittal-Plane Trunk Position, Landing Forces, and Quadriceps Electromyographic Activity. *Journal of Athletic Training,* 44. (2009), 2. 174–179. Online: https://doi.org/10.4085/1062-6050-44.2.174

Brinckmann, Paul – W. Frobin – Gunnar Leivseth: *Musculoskeletal Biomechanics.* Stuttgart – New York, Thieme, 2002.

Chang, Alison – Karen Hayes – Dorothy Dunlop – Jing Song – Debra Hurwitz – September Cahue – Leena Sharma: Hip Abduction Moment and Protection against Medial Tibiofemoral Osteoarthritis Progression. *Arthritis & Rheumatism,* 52. (2005), 11. 3515–3519. Online: https://doi.org/10.1002/art.21406

Chapman, Kay – Ana M. Valdes: Genetic Factors in OA Pathogenesis. *Bone,* 51. (2012), 2. 258–264. Online: https://doi.org/10.1016/j.bone.2011.11.026

Charnley J.: The Lubrication of Animal Joints in Relation to Surgical Reconstruction by Artrhroplasty. *Annals of Rheumatic Diseases,* 19. (1960), 1. 10–19. Online: https://doi.org/10.1136/ard.19.1.10

Culvenor, Adam – G. Marienke van Middelkoop – Erin M. Macri – Kay M. Crossley: Is Patellofemoral Pain Preventable? A Systematic Review and Meta-Analysis of Randomised Controlled Trials. *British Journal of Sports Medicine,* 55. (2021), 7. 378–384. Online: https://doi.org/10.1136/bjsports-2020-102973

Deacon, Adam – Kay Crossley – Peter Brukner – Kim Bennell – Zoltan S. Kiss: Osteoarthritis of the Knee in Retired, elite Australian Rules Footballers. *Medical Journal of Australia,* 166. (1997), 4. 187–190. Online: https://doi.org/10.5694/j.1326-5377.1997.tb140072.x

Dijksma, Iris – Marga Bekkers – Bea Spek – Cees Lucas – Martijn Stuiver: Epidemiology and Financial Burden of Musculosceletal Injuries as the Leading Health Problem in the Military. *Military Medicine,* 185. (2020), 3–4. 1–5. e480–e486. Online: https://doi.org/10.1093/milmed/usz328

Dijksma, Iris – Ilgin G. Arslan – Faridi S. Etten–Jamaludin – Roy G. Elbers – Cees Lucas – Martijn M. Stuiver: Exercise Programs to Reduce the Risk of Musculuskeletal Injuries in Military Personnel: A Systematic Review and Meta-Analysis. *PM&R,* 12. (2020), 10. 1028–1037. Online: https://doi.org/10.1002/pmrj.12360

Fuss, Franz K.: Anatomy of the Cruciate Ligaments and Their Function in Extension and Flexion of the Human Knee Joint. *American Journal of Anatomy,* 184. (1989), 2. 165–176. Online: https://doi.org/10.1002/aja.1001840208

Glaviano, Neal R. – Michelle C. Boling – John J. Fraser: Anterior Knee Pain Risk Differs Between Sex and Occupation in Military Tactical Athletes. *Journal of Athletic Training,* (2021), március 31. Online: https://doi.org/10.4085/1062-6050-0578.20

Hehne Hj. et al.: Eine neue Methode zur Ermittlung lastabhangiger Druck- und Kontaktverlaufe an Grenzflachen. *Morphol Med.,* 1. (1981), 95–106.

Hehne Hj. et al.: Analoge Druck- und Kontaktflachenmessung des Femoropatellargelenkes mit optisch sensibler Druckmessfolie. *Z Orthop,* 120. (1982), 513.

Hewett, Timothy E. – Gregory D. Myer – Kevin R. Ford – Robert S. Heidt – Angelo J. Colosimo – Scott G. McLean – Antonie J. van den Bogert – Mark V. Paterno – Paul Succop: Biomechanical Measures of Neuromuscular Control and Valgus Loading

of the Knee Predict Anterior Cruciate Ligament Injury Risk in Female Athletes: A Prospective Study. *American Journal of Sports Medicine,* 33. (2005), 4. 492–501. Online: https://doi.org/10.1177/0363546504269591

Hochberg, Mark C. – Laura Yerges-Armstrong – Michelle Yau – Braxton D. Mitchell: Genetic Epidemiology of Osteoarthritis: Recent Developments and Future Directions. *Current Opinion in Rheumatology,* 25. (2013), 2. 192–197. Online: https://doi.org/10.1097/BOR.0b013e32835cfb8e

Hollman, John H. – Barbara E. Ginos – Jakub Kozuchowski – Amanda S. Vaughn – David A. Krause – James W. Youdas: Relationships between Knee Valgus, Hip-Muscle Strength, and Hip-Muscle Recruitment during a Single-Limb Step-Down. *Journal of Sport Rehabilitation,* 18. (2009), 1. 104–117. Online: https://doi.org/10.1123/jsr.18.1.104

Jiang, Liying – Wenjing Tian – Yingchen Wang – Jiesheng Rong – Chundan Bao – Yupeng Liu – Yashuang Zhao – Chaoxu Wang: Body Mass Index and Susceptibility to Knee Osteoarthritis: A Systematic Review and Meta-Analysis. *Joint Bone Spine,* 79. (2012), 3. 291–297. Online: https://doi.org/10.1016/j.jbspin.2011.05.015

Jordaan, Gerhard – Martin P. Schwellnus: The Incidence of Overuse Injuries in Military Recruits during Basic Military Training. *Military Medicine,* 159. (1994), 6. 421–426. Online: https://doi.org/10.1093/milmed/159.6.421

Kaplan, Jonathan T. – John W. Ramsay – Sarah E. Cameron – Kayla D. Seymore – Michael Brehler – Gaurav K. Thawait – Wojciech B. Zbijewski – Jeffrey H. Siewerdsen – Tyler N. Brown: Association Between Knee Anatomic Metrics and Biomechanics for Male Soldiers Landing with Load. *American Journal of Sports Medicine,* 48. (2020), 6. 1389–1397. Online: https://doi.org/10.1177/0363546520911608

Kraemer, William J. – Scott A. Mazzetti – Bradley C. Nindl – Lincoln A. Gotshalk – Jeff S. Volek – Jill A. Bush – Jim O. Marx – Kei Dohi – Ana L. Gómez – Mary Miles – Steven J. Fleck – Robert U. Newton – Keijo Häkkinen: Effect of Resistance Training on Women's Strength/Power and Occupational Performances. *Medicine and Science in Sports and Exercise,* 33. (2001), 6. 1011–1025. Online: https://doi.org/10.1097/00005768-200106000-00022

Lawrence, Ronald K. – Thomas W. Kernozek – Emily J. Miller – Michael R. Torry – Paul Reuteman: Influences of Hip External Rotation Strength on Knee Mechanics during Single-Leg Drop Landings in Females. *Clinical Biomechanics,* 23. (2008), 6. 806–813. Online: https://doi.org/10.1016/j.clinbiomech.2008.02.009

Magnussen, Robert A. – Guillaume Demey – Sébastien Lustig – Elvire Servien – Philippe Neyret: Total Knee Arthroplasty for Secondary Osteoarthritis Following ACL Reconstruction: A Matched-Pair Comparative Study of Intra-Operative and Early Post-Operative Complications. *Knee,* 19. (2012), 4. 275–278. Online: https://doi.org/10.1016/j.knee.2011.05.001

McWilliams, D. F. – B. F. Leeb – S. G. Muthuri – M. Doherty – W. Zhang: Occupational Risk Factors for Osteoarthritis of the Knee: A Meta-Analysis. *Osteoarthritis and Cartilage,* 19. (2011), 7. 829–839. Online: https://doi.org/10.1016/j.joca.2011.02.016

Menschik, Alfred: Mechanik des Kniegelenks. Teil 1. *Z. Orthop.,* 112. (1974), 448–495.

Military Environment. *Knee Surgery & Related Research,* 31. (2019), 13. Online: https://doi.org/10.1186/s43019-019-0015-1

Murtha, Andrew S. – Anthony E. Johnson – Joseph A. Buckwalter – Jessica C. Rivera: Total Knee Arthroplasty for Posttraumatic Osteoarthritis in Military Personnel Under Age 50. *Journal Of Orthopaedic Research,* 35. (2016), 3. 677–681. Online: https://doi.org/10.1002/jor.23290

Müller-Gerbl, M. et al.: Die Darstellung der subchondralen Dichtemuster mittels der CT-Osteoabsortiometrie (CT-OAM) zur Beurteilung der individuellen Gelenkbeanspruchung am Lebenden. *Z Orthop.,* 128. (1990), 128–133. Online: https://doi.org/10.1055/s-2008-1039487

Owens, Brett D. – Sally B. Mountcastle – Warren R. Dunn – Thomas M. DeBerardino – Dean C. Taylor: Incidence of Anterior Cruciate Ligament Injury among Active Duty U.S. Military Servicemen and Servicewomen. *Military Medicine,* 172. (2007), 1. 90–91. Online: https://doi.org/10.7205/MILMED.172.1.90

Piazza, Stephen J. – Peter R. Cavanagh: Measurement of the screw-home motion of the knee is sensitive to errors in axis alignement. *Journal of Biomechanics,* 33. (2000), 8. 1029–1034. Online: https://doi.org/10.1016/S0021-9290(00)00056-7

Powers, C. M.: The Influence of Altered Lowerextremity Kinematics on Patellofemoral Joint Dysfunction: A Theoretical Perspective. *Journal of Orthopaedic & Sports Physical Therapy,* 33. (2003), 11. 639–646. Online: https://doi.org/10.2519/jospt.2003.33.11.639

Prodromos, Chadwick C. – Yung Han – Julie Rogowski – Brian Joyce – Kelvin Shi: A Meta-Analysis of the Incidence of Anterior Cruciate Ligament Tears as a Function of Gender, Sport, and a Knee Injury-Reduction Regimen. *Arthroscopy,* 23. (2007), 12. 1320–1325. Online: https://doi.org/10.1016/j.arthro.2007.07.003

Reiman, Michael P. – Lori A. Bolgla – Daniel Lorenz: Hip Functions Influence on Knee Dysfunction: A Proximal Link to a Distal Problem. *Journal of Sport Rehabilitation,* 18. (2009), 1. 33–46. Online: https://doi.org/10.1123/jsr.18.1.33

Rivera, Jessica C. – Joseph C. Wenke – Joseph A. Buckwalter – James R. Ficke – Anthony E. Johnson: Posttraumatic Osteoarthritis Caused by Battlefield Injuries: The Primary Source of Disability in Warriors. *Journal of the American Academy of Orthopedic Surgeons,* 20. (2012), Suppl 1. S64–69. Online: https://doi.org/10.5435/JAAOS-20-08-S64

Smidt, Gary L.: Biomechanical Analysis of Knee Flexion and Extension. *J. Biomechanics,* 6. (1973), 1. 79–92. Online: https://doi.org/10.1016/0021-9290(73)90040-7

Seedholm, B. B. – T. Takeda – M. Tsubuku – V. Wright: Mechanical Factors and Patellofemoral Osteoarthrosis. *Annals of the Rheumatic Diseases,* 38. (1979), 4. 307–316. Online: https://doi.org/10.1136/ard.38.4.307

Showery, James E. – Nicholas A. Kusnezov – John C. Dunn – Julia O. Bader – Philip J. Belmont Jr – Brian R. Waterman: The Rising Incidence of Degenerative and Posttraumatic Osteoarthritis of the Knee in the United States Military. *The Journal of Arthroplasty,* 31. (2016), 10. 2108–2114. Online: https://doi.org/10.1016/j.arth.2016.03.026

Simoneau, G.: Kinesiology of Walking. In Donald A. Neumann (szerk.): *Kinesiology of the Musculoskeletal System.* St Louis, MO, Mosby Inc., 2002. 523–569.

Simonsen, E. B. – P. Dyhre-Poulsen – M. Voigt – P. Aagaard – N. Fallentins: Mechanisms Contributing to Different Joint Moments Observed During Human Walking. *Scandinavian Journal of Medicine & Science in Sports,* 7. (1997), 1. 1–13. Online: https://doi.org/10.1111/j.1600-0838.1997.tb00110.x

Stannard, Joanne – L. Fortington: Musculosceletal Injury in Military Special Operations Forces: A Systematic Review. *BMJ Military Health,* 167. (2021), 4. 255–265. Online: https://doi.org/10.1136/bmjmilitary-2020-001692

Szendrői Miklós (szerk.): *Ortopédia.* Budapest, Semmelweis, 2005.

Taanila, Henri – Jaana Suni – Harri Pihlajamäki – Ville M. Mattila – Olli Ohrankämmen – Petteri Vuorinen –Jari Parkkari: Musculoskeletal Disorders in Physically Active Conscripts: A One-Year Follow-Up Study in the Finnish Defence Forces. *BMC Musculoskeletal Disorders,* 10. (2009), 1. 1–11. Online: https://doi.org/10.1186/1471-2474-10-89

Valdes, A. M. – Tim D. Spector: Genetic Epidemiology of Hip and Knee Osteoarthritis. *Nature Reviews Rheumatology,* 7. (2011), 1. 23–32. Online: https://doi.org/10.1038/nrrheum.2010.191

Wikstrom, Erik A. – Mark D. Tillman – Kai J Kline – Paul A Borsa: Gender and Limb Differences in Dynamic Postural Stability during Landing. *Clinical Journal of Sports Medicine,* 16. (2006), 4. 311–315. Online: https://doi.org/10.1097/00042752-200607000-00005

Winby, C. R. – D. G. Lloyd – T. F. Besier – T. B. Kirk: Muscle and External Load Contribution to Knee Joint Contact Loads during Normal Gait. *Journal of Biomechanics,* 42. (2009), 14. 2294–2300. Online: https://doi.org/10.1016/j.jbiomech.2009.06.019

Witvrouw, Erik – Johan Bellemans – Roeland Lysens – Lieven Daneels – Dirk Cambier: Intrinsic Risk Factors for the Development of Patellar Tendinitis in an Athletic Population. A Two-Year Prospective Study. *The American Journal of Sports Medicine,* 29. (2001), 2. 190–195. Online: https://doi.org/10.1177/03635465010290021201

Witvrouw, Erik – Lieven Danneels – Peter Asselman – Thomas D'Have – Dirk Cambier: Muscle Flexibility as a Risk Factor for Developing Muscle Injuries in Male Professional Soccer Players. A Prospective Study. *The American Journal of Sports Medicine,* 31. (2003), 1. 41–46. Online: https://doi.org/10.1177/03635465030310011801

Witvrouw, Erik – Roeland Lysens – Johan Bellemans – Dirk Cambier – Guy Vanderstraeten: Intrinsic Risk Factors for the Development of Anterior Knee Pain in an Athletic Population. A Two-Year Prospective Study. *The American Journal of Sports Medicine,* 28. (2000), 4. 480–489. Online: https://doi.org/10.1177/03635465000280040701

Woo, Savio L. – J. Marcus Hollis – Douglas J. Adams – Roger M. Lyon – Shinro Takai: Tensile Properties of the Human Femur-Anterior Cruciate Ligament-Tibia Complex: The Effects of Specimen Age and Orientation. *The American Journal of Sports Medicine,* 19. (1991), 3. 217–225. Online: https://doi.org/10.1177/036354659101900303

Young, Jodi L. – Suzanne J. Snodgrass – Joshua A. Cleland – Daniel I. Rhon: Usual Medical Care for Patellofemoral Pain Does Not Usually Involve Much Care: 2-Year Follow-up in the Military Health System. *Journal of Orthopaedic & Sports Physical Therapy,* 51. (2021), 6. 305–313. Online: https://doi.org/10.2519/jospt.2021.10076

Tartalom