ISSN 2676-9042

Vol 3, No 4, 2021.

2021, III. évf. 4. szám

Safety and Security Sciences Review

international, peer-reviewed, professional and scientific journal of safety and security sciences

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

https://biztonsagtudomanyi.szemle.uni-obuda.hu

On the cover can be seen | A borítón
ÉZSIÁS István
sculptor/szobrászművész
Plate relief | **Lemez-relief**
statue | című szobra látható

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

COLUMNS	ROVATOK
Material Safety	Anyagbiztonság
Philosophy and History of the Safety and Security	Biztonságfilozófia és -történet
Security Policy	Biztonságpolitika
Security Systems	Biztonságtechnika
Security Awareness	Biztonságtudatosság
Domotics	Domotika
Health Security	Egészségbiztonság
Food Safety	Élelmiszerbiztonság
Economic Security	Gazdasági biztonság
War Security and Law Enforcement	Hadbiztonság és rendvédelem
Information Security	Információbiztonság
Industrial and Operational Safety	Ipar- és üzembiztonság
Legal and Social Security	Jog- és társadalombiztonság
Book Review	Könyvismertetés
Security of Environment	Környezetbiztonság
Traffic Safety	Közlekedésbiztonság
Facility Security	Létesítménybiztonság
Private Security	Magánbiztonság
Artificial Intelligence	Mesterséges intelligencia
Safety and Security in General	Munkabiztonság
Technical Security	Műszaki biztonság

The aim of the journal is to publish studies, research reports, articles, book reviews of the broad discipline of security science for professionals working in or related fields of security science, thereby developing security awareness and security culture.

Published quarterly, typically in Hungarian, occasionally in a foreign language. Special and/or thematic issues related to conferences and topics are occasionally published in Hungarian or in foreign languages.

Only those papers will be published which reviewed by two independent reviewers and recommended suitable for publication in the Safety and Security Sciences Review. The submitted manuscripts must meet the requirements both of the form and the content which can be found in the journal's website. Please note: we will not return unapproved manuscripts.

Articles in the Safety and Security Sciences Review are archived in the Digital Archives of Óbuda University (ÓDA). The studies of the staff and students of Óbuda University, published in the Journal, are recorded by the staff of the University Library at the Hungarian Scientific Works Library (MTMT).

A **folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek és a téma iránt érdeklődők számára a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése.

Megjelenés negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.

A Biztonságtudományi Szemle folyóiratban csak két független lektor által lektorált és megjelentetésre alkalmasnak tartott tanulmányok jelenhetnek meg. A beküldött kéziratoknak formai és tartalmi szempontból egyaránt meg kell felelnie a Folyóirat weboldalán közölt elvárásoknak. El nem fogadott kéziratokat nem áll módunkban visszaküldeni.

A Biztonságtudományi Szemle folyóiratban megjelenő cikkek az Óbudai Egyetem Digitális Archívumában (ÓDA) archiválásra kerülnek. Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

ISSN 2676-9042
https://biztonsagtudomanyi.szemle.uni-obuda.hu

Editorial office | Szerkesztőség
Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi Doktori Iskola
1081 Budapest, Népszínház utca 8.

Publisher | Kiadó
Óbudai Egyetem, 1034 Budapest, Bécsi út 96/B.

Responsible for publishing | A kiadásért felel
Prof. Dr. KOVÁCS Levente
Rector of the Óbuda University | az Óbudai Egyetem rektora

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 3, No 4, 2021. | **2021. III. évf. 4. szám**

Authors of this issue | **E számunk szerzői**

BÁLINT Márton

balint.marton@phd.uni-obuda.hu

My name is Marton BALINT. I joined the PHD School of Obudai University at 40 years, following my studies of economics at the Foreign School of Economics in Budapest and at University of Montreal. At present I am working with the building of electrical networks. During my work I was involved in several cases when the security of a secure, reliable, and continuous electrical supply was at stake, and the level of danger that a breach is these securities needed to be assessed for the population, the institutions and our everyday life. At this point I felt the need to further study the question of security and to know its widespread details, and the Obudai University, along with the guidance of Mr. Dr. Endre Szucs offers great opportunities in this field. Drones are the basis of my studies, the use of which are far more exceeding the hobby type of application and can be source of real danger in our lives.

BÁLINT Márton vagyok, 40 évesen iratkoztam be az Óbudai Egyetem Doktori Iskolába. Ezt megelőzően tanulmányaimat először a Külkereskedelmi Főiskola Közgazdasági karán, majd a Montreali Közgazdasági Egyetemen folytattam. Jelenleg villamos hálózatok építésével foglalkozom. Ennek során találkoztam számos olyan esettel, melyek során a biztonságos, megbízható és folyamatos áramellátás biztosításának a veszélyét kellett megoldani, illetve átgondolni, hogy ezen veszélyek milyen kockázatokat jelentenek a lakosságra, intézmények működésére és a megszokott mindennapjainkra. Ekkor fogalmazódott bennem meg az igény arra, hogy mélyebben tanulmányozzam a biztonság kérdését, megismerni annak rendkívül sokrétű részleteit. Az Óbudai Egyetem doktori iskoláján, Dr. Szűcs Endre úr irányításával alkalmam nyílik mélyebb tudást szerezni ezen a téren. Munkám fókuszába a drónokat állítottam, melyek hobbi felhasználáson felül sokkal komolyabb szerepet is tudnak kapni, és ezáltal veszélyt jelenteni a mindennapjaink biztonságára is.

BESENYŐ János

besenyo.janos@uni-obuda.hu

Colonel (ret.) Dr. habil János BESENYŐ had 31 years of experience in the Hungarian Defence Forces. In his last assignment he led the General Staff, Scientific Research Centre more than 4 years. He is an assistant professor of University of Obuda Doctoral School on Safety and Security Sciences and teaching African conflicts, European Security and Defence Policy, and conflict management. He is a lecturer in National Public Service University, Budapest (Doctoral School of Military Sciences), Eötvös Loránd University, Budapest (Doctoral School of History) and Eszterházy Károly University of Applied Sciences, Eger about African History, African conflicts, Hungarian participation in African peace operations, Western Sahara, terrorism, Christian-Muslim relations, Hungarian-African relations.

Dr. habil BESENYŐ János 31 éves tapasztalattal rendelkezik a Magyar Honvédségnél. Legutolsó megbízatásában 4 évig vezette a Honvéd Vezérkar Tudományos Kutatóhelyet. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának adjunktusa, ahol afrikai konfliktusokat, európai biztonság- és védelempolitikát, valamint konfliktuskezelést oktat. A budapesti Nemzeti Közszolgálati Egyetem (Hadtudományi Doktori Iskola), a budapesti ELTE (Történelemtudományi Doktori Iskola) és az egri Eszterházy Károly Egyetem oktatója afrikai történelem, afrikai konfliktusok, magyar részvétel az afrikai békeműveletekben, Nyugat-Szahara, terrorizmus, kereszténység-muszlim kapcsolatok és magyar-afrikai kapcsolatok témakörökben.

DOLNEGÓ Bálint

dolnego.balint@tf.hu

Bálint DOLNEGÓ is a sports manager, sports organizer and sports facility operator in terms of education. He completed the Complex Education Language and Intercultural Immersion for Junior Faculty training programme in the United States, at the University of New Mexico. He is a coach in sports shooting, as well as a referee in football and handball. He has been active in football as a member of the 2nd division refereeing panel. Assistant lecturer at the Department of Sports Management of the University of Physical Education and the Head of the Chancellor's Office. In 2019, he was awarded the Lecturer of the Year award by the University's Student Union. He is a doctoral candidate at the Doctoral School of the University of Physical Education, and his research topic is refereeing.

DOLNEGÓ Bálint végzettségét tekintve okleveles sportmenedzser, sportszervező és sportlétesítményüzemeltető. Az Egyesült államokban a Univerity of New Mexico Complex Education Language and Intercultural Immersion for Junior Faculty képzését végzete el. Sportedző sportlövészet, valamint játékvezető labdarúgás és kézilabda sportágakban. A labdarúgásban 2005 óta játékvezető, jelenleg az NB2-es keret tagja. A Testnevelési Egyetem Sportmenedzsment Tanszékén egyetemi tanársegéd, valamint Kancellári titkárságvezető. 2019-ben az egyetem Hallgatói Önkormányzata Az év oktatója díjban részesítette. A Testnevelési Egyetem Doktori iskolájában doktorjelölt, kutatási témája a játékvezetés.

FÁBIÁN Péter

fabianpeter@topcopgroup.com

The author is a police officer, lawyer, criminologist, national security analyst. For many years he worked as a criminal intelligence officer at various police departments. He has been working as a leader in the private security sector for more than 20 years. Private forensic security expert, security consultant for several large multinational corporations. Expert of the PTE Center for Defense Research. He is a doctoral candidate of the Doctoral School of Security Sciences of the University of Óbuda. His research topic is private security.

A szerző rendőrtiszt, jogász, kriminológus, nemzetbiztonsági elemző. Sok évig bűnügyi hírszerzőként dolgozott a Rendőrség különböző szerveinél. Több, mint 20 éve a magánbiztonsági szektorban dolgozik vezetőként. Igazságügyi magánbiztonsági szakértő, több multinacionális nagyvállalat biztonsági tanácsadója. A PTE Védelmi Kutatások Központ szakértője. Az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorjelöltje. Kutatási témája a magánbiztonság.

FARAGÓ Ferenc

farago.ferenc@uni-obuda.hu

My name is Ferenc FARAGÓ, I am a certified environmental engineer, occupational safety engineer, facility energy specialist, commercial pilot, environmental and occupational safety manager. My profession is safety: I have been working as an environmental expert for more than 20 years and I have occupational safety expert qualifications as well. I have worked as a consultant for Hungarian and European companies, and as a manager for large companies, I have also gained global experience in the field of company management, production, environmental and occupational safety. I have worked primarily on developing corporate sustainability strategies for companies in Europe, the United States and the Far

FARAGÓ Ferenc vagyok, végzettségemet tekintve okleveles környezetvédelmi mérnök, munkavédelmi szakmérnök, létesítmény energetikus szakember, kereskedelmi pilóta, környezetvédelmi és munkavédelmi vezető. Hivatásom a biztonság: több, mint 20 éve dolgozom környezetvédelmi szakértőként és munkavédelmi szakértői jogosultságokkal is rendelkezem. Tanácsadóként magyarországi és európai vállalatoknál dolgoztam, vezetőként pedig nagyvállalatoknál, amelyeknél globális tapasztalatot is szereztem a vállalatvezetés, a termelés, illetve a környezet- és munkavédelem terén. Főként vállalati fenntarthatósági stratégiák kialakításán dolgoztam európai, egyesült államokbeli és távol-keleti vállalatok-

East. I am currently working in the management of a multinational manufacturing company as an EHS manager. I am trying to expand my knowledge at the Doctoral School of Security Sciences of the University of Óbuda. My main field of research is safety management, occupational safety performance measurement and forecasting the increase in accident risks, but I am also interested in the study of the use of drones for occupational safety purposes. I am proud to be able to participate in the educational activities of the university, in the training of occupational safety professionals as an instructor, and as a consultant to dissertation students. In addition to higher education, I try to help students with security issues as well as employees and employers. The main topic of my 2BSafe podcast is occupational safety and health. The ever-increasing audience indicates that there is interest in the topic.

nál. Jelenleg egy multinacionális gyártó vállalat menedzsmentjében dolgozom, mint környezetvédelmi és munkavédelmi vezető. Tudásomat az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában igyekszem bővíteni. Fő kutatási területem a biztonság menedzselése, a munkavédelmi teljesítménymérés és a baleseti kockázatok növekedésének előrejelzése, de foglalkoztat a drónok munkavédelmi célú felhasználási lehetőségeinek vizsgálata is. Büszke vagyok rá, hogy részt vehetek az egyetem oktatási tevékenységében, a munkavédelmi szakemberek képzésében oktatóként, illetve a szakdolgozó hallgatók konzulenseként. A biztonsággal kapcsolatos kérdésekben a felsőoktatáson kívül is igyekszem segíteni a hallgatókat, valamint a munkavállalókat és a munkáltatókat is. A 2BSafe című podcastom fő témája a munkavédelem és a munkahelyi biztonság. A folyamatosan növekvő hallgatottság azt jelzi, hogy van érdeklődő a téma iránt.

FÜRTÖS János

furtosjanos@onvedelemoktatas.hu

FÜRTÖS János (1968) self-defence expert. He has been engaged in martial arts and self-defence for more than forty years. He has thirty years of teaching and coaching experience, that he successfully uses to run their self-defence training center. Beside teaching civilians, he also assists to train personnel of the armed forces, police and their special units. He has contributed to the preparation and publication of several books and publications on martial arts. In the field of self-defence and individual security he follows a complex approach to promote the ultimate aim of his followers. He never stops developing his knowledge in his specialization and researches authentic theoretical and practical sources on martial arts and self-defence. He does not teach a style of martial art as self-defense, but he teaches self-defense as martial art.

FÜRTÖS János (1968) önvédelmi szakértő. Több mint negyven éve foglalkozik harcművészetekkel és önvédelemmel. Harminc éves oktatói, edzői tapasztalattal rendelkezik, amelyet sikeresen alkalmaz önvédelmi oktatóközpontjuk vezetésében. Tevékenysége során a civileken kívül segíti a fegyveres erők, testületek és speciális egységeik kiképzését. Több könyv és harcművészeti kiadvány elkészítésében és megjelenésében működött közre. Az önvédelem és az egyéni biztonság témáját komplex módon közelíti meg. Folyamatosan fejleszti tudását és kutatja a harcművészetekkel és önvédelemmel kapcsolatos elméleti, és gyakorlati forrásanyagokat. Nem egy harcművészeti stílust oktat önvédelemként, hanem az önvédelmet oktatja harcművészetként.

GÉCZI Gábor

gabor@tf.hu

Gábor GÉCZI started his career in 1978 as the hockey goalkeeper of the Dózsa Újpesti Budapest. Until the age of 23, he was a member of the Hungarian hockey team 44 times and won the Hungarian First League Championship three times and the Hungarian Cup once. During his sporting career, he earned a degree in physical education and later, in 2004, a BSc in ice hockey coaching and public administration. He started his executive carrier as facility manager (tennis courts, ice rinks), from 2005 to 2007 he was the

GÉCZI Gábor 1978-ban kezdte pályafutását a Dózsa Újpesti Budapest jégkorongkapusaként. 23 éves koráig 44 alkalommal volt tagja a magyar jégkorong válogatottnak, és háromszor nyerte meg a magyar bajnokságot és egyszer magyar Kupát. Sportpályafutása során testnevelő diplomát, majd 2004-ben jégkorong szakedzői és államigazgatási BSc-t végzett. Vezetői pályafutását létesítményvezetőként kezdte (teniszpályák, jégpályák), 2005-től 2007-ig a legnagyobb magyar sport létesítményüzemeltető társaság

CEO of the largest Hungarian sports FM Company (National Sport Centers). Since 2009 he has been a lecturer at the Semmelweis University, Faculty of Physical Education and Sports Science, since 2014 at the University of Physical Education. In 2003, he reformed the entire structure of the hockey coaching program and began running the Heracles Youth Program. He is currently the strategic program leader of the Hungarian Ice Hockey Federation, the director of the Institute of Economics and Social Sciences of the Budapest University of Physical Education, and the head of the Department of Sports Management.

(Nemzeti Sportközpontok) vezérigazgatója volt. 2009-től a Semmelweis Egyetem Testnevelés- és Sporttudományi Karának, 2014-től a Testnevelési Egyetem oktatója. 2003-ban megreformálta a jégkorong edzőképzési program teljes szerkezetét, és megkezdte a Héraklész Bajnok és Csillag Program működtetését. Jelenleg a Magyar Jégkorong Szövetség stratégiai programvezetője, a Testnevelési Egyetem Gazdaság és Társadalomtudományi Intézetének igazgatója, valamint a Sportmenedzsment Tanszékének vezetője.

KONDÁS Katalin

kondaskatalin@gmail.com

Katalin KONDÁS engineer-IT specialist, technical teacher and security engieer. Her area of research is exploring the possibilities of biometric identification in Hungarian prisons. She is currently expanding her knowledge at the Doctoral School of Security Sciences at Óbuda University.

KONDÁS Katalin mérnök-informatikus, mérnöktanár, biztonságtechnikai mérnök. Kutatási területe a biometriai azonosítás lehetőségeinek vizsgálata a magyar börtönökben. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit.

MÉSZÁROS Alexandra Ágnes

meszaros.alexandra@uni-obuda.hu

Alexandra Ágnes MÉSZÁROS, PhD student at Óbuda University Doctoral School on Safety and Security Sciences. She earned her Commerce and Marketing BSc diploma in 2018, then Business Development MSc diploma in 2020 both at Óbuda University. Her primary research field is international military business processes from the view of security sciences. Her work involves organizing and executing international military technology sales and purchase processes. She participated in projects where she followed the development of the products from the blueprint to the series production and market introduction. She has experience in international business contracts and military technology import-export authorization processes.

MÉSZÁROS Alexandra Ágnes, PhD hallgató az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában. 2018-ban diplomát szerzett az Óbudai Egyetemen Kereskedelem és Marketing BSc szakon, majd 2020-ban vállalkozásfejlesztés MSc szakon. Főbb kutatási területi a nemzetközi haditechnikai üzleti folyamatok biztonságtudományi szempontból vizsgálva. Munkája során nemzetközi haditechnikai értékesítési folyamatokat szervez és bonyolít le. Részt vett projektekben, ahol a termék útját a tervrajzoktól a sorozatgyártásig, majd értékesítésig végig kísérte. Tapasztalattal rendelkezik a nemzetközi ügyletekre vonatkozó szerződések területén és a haditechnikai termékek import-export engedélyeztetési folyamataiban.

NYÁRI Norbert

nyari.norbert@uni-obuda.hu

So far, I have studied mainly in the field of informatics, I have degrees in engineering, teaching and computer science. I have been working as a software developer for more than 10 years at a budgetary institution of the Hungarian public administration. Due to my studies and professional experience, I have extensive knowledge in the fields of application development, information security, and psychology. The aim of my doctoral research is to find tools, methods

Eddigi tanulmányaimat alapvetően informatikai területen végeztem, rendelkezem mérnöki, tanári, programtervezői diplomákkal. Több mint 10 éve dolgozom szoftverfejlesztőként a magyar közigazgatás egyik költségvetési szervénél. Tanulmányaimnál és szakmai tapasztalatomnál fogva széleskörű ismeretekkel rendelkezem az alkalmazásfejlesztés, az információbiztonság, valamint a pszichológia területén. Doktori kutatásom célja a magyar közigazgatás

and solutions for strengthening the information security of the Hungarian public administration.

információbiztonságának erősítését szolgáló eszközök, módszerek, megoldások felkutatása.

SZAKALI Miklós

mszakali@hotmail.com

SZAKALI Miklós (1963) lieutenant colonel, currently he is serving at the Hungarian Ministry of Defence, as a senior defence planner. His responsibility is the harmonisation of the national and the NATO's capability developments. He is a doctoral candidate of the Óbuda University Doctoral School on Safety and Security Science in Budapest. His field of research is the study of areas and interactions between security and defence planning. It includes new, complex forms of current security challenges and ways and possibilities to prevent and manage them. He also explores the applicability of NATO's defense planning system (and defense planning systems in general) to address the new types of challenges of our time.

SZAKALI Miklós (1963) alezredes, hivatásos katona, jelenleg a Honvédelmi Minisztérium Védelempolitikai Főosztályon teljesít szolgálatot, mint védelmi tervező főtiszt. Felelősségi területe a nemzeti és a NATO képességfejlesztési tevékenységek harmonizálása. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit, mint doktorandusz hallgató. Kutatási területe a biztonság és a védelmi tervezés területeinek és kölcsönhatásainak vizsgálata. A napjainkban megjelenő biztonsági kihívások új, komplex formáit és azok megelőzésének és kezelésének lehetőségeit vizsgálja. Kutatja a NATO védelmi tervezési rendszerének (és általában a védelmi tervezési rendszerek) alkalmazhatósági lehetőségeit korunk új típusú kihívásainak kezelésére.

SZALÁNCZI-ORBÁN Virág

szalancziorban.virag@uni-obuda.hu

SZALÁNCZI-ORBÁN Virág logistics manager, economist. Currently a PhD student at the Doctoral School of Security Sciences of the University of Óbuda. Research interests: logistics, network science, information security, logistics systems, supply chain. Title of the research topic: Increasing the role of logistics in Hungary with the participation of systems logistics, security sciences and other interdisciplinary disciplines.

SZALÁNCZI-ORBÁN Virág Logisztikai menedzser, közgazdász. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában PhD hallgató. Kutatási terület: logisztika, hálózattudomány, információbiztonság, logisztikai rendszerek, ellátási lánc. Kutatási téma címe: Rendszerlogisztikai, biztonságtudományi és más interdiszciplináris tudományágak közreműködésével Magyarország logisztikai szerepének növelése.

TICK Andrea

tick.andrea@uni-obuda.hu

Andrea TICK PhD is an associate professor at Óbuda University Keleti Faculty of Business and Management. Her research interests include internet security, cyber security, user behavior regarding digital learning, cyber security awareness and the human factor in cyber security. She has a BSc in Economics, an MA in Mathematics, Computer Science and English language. Her PhD and Dr. habil research areas are digital teaching and learning with special cyber security awareness.

TICK Andrea PhD az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi docense. Kutatási területei közé tartozik az internetbiztonság, a kiberbiztonság, a digitális tanulással kapcsolatos felhasználói magatartás, a kiberbiztonsági tudatosság és a kiberbiztonság emberi tényezője. Mesterdiplomát szerzett angol irodalom és nyelvészet, matematika és számítástechnika szakon, valamint közgazdász bachelor diplomával rendelkezik. PhD és Dr. habil kutatási területei a digitális tanítás és tanulás speciális kiberbiztonsági és biztonságtudatossági aspektusai.

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 3, No 4, 2021. | **2021. III. évf. 4. szám**

CONTENT | TARTALOM

BIOMETRICS IN PRISON | BIOMETRIA A BÖRTÖNBEN

KONDÁS Katalin[1]

Abstract

My research area is a biometric identification application in prisons where currently – mostly – object based identification works. Biometric identification is important when the prisoners are placed in the Institute, the identification is done with a fingerprint reader. Generally speaking, the use of a biometric identification reader is simple, does not have to keep any passwords, code and object to ourselves. As all people have unique features, so biometric identification can mean the most accurate identification mode. But which one is the better method in prisons? My publication aims to research this.

Keywords

biometrics, identification, fingerprint, palm vein, prison

Absztrakt

Kutatási területem a biometrikus azonosítás alkalmazás a börtönökben, ahol jelenleg – többnyire – tárgyi alapú azonosítás működik. A biometrikus azonosításnak a fogvatartottak intézetbe vonulásakor van jelentősége, a személyazonosítás ujjnyomat olvasó segítségével valósul meg. Általánosságban elmondható, hogy a biometrikus azonosító olvasó használata egyszerű, nem kell semmilyen jelszót, kódot észben tartani. Mivel az emberek mindegyike egyedi adottságokkal rendelkezik, így a biometrikus azonosítás jelentheti a legpontosabb azonosítási módot. De melyik a jobb módszer a büntetésvégrehajtásban? Publikációm célja ennek kutatása.

Kulcsszavak

biometria, azonosítás, tenyérvéna, ujjnyomat, börtön

[1] kondaskatalin@gmail.com | ORCID: 0000-0002-3775-4653 | IT buyer, National Tax and Customs Administration of Hungary | IT beszerzés , Nemzeti Adó- és Vámhivatal

BEVEZETÉS

A biometrikus azonosítások olyan azonosítások, amelyek az emberi szervezet egyedi jellemzőinek felismerésén alapulnak. Sok ismert azonosítási technológia létezik már, ilyen az arc-, hang-, írisz- retina-, véna-, DNS-, tenyér- és ujj(le)nyomat azonosítás. A köztudatban kevésbé ismert, de mégis létező, az egyénre jellemző pontos azonosító lehet, ahogyan mozgunk, vagy esetleg egy eszközt: a billentyűzetet, a mobiltelefont, vagy az egeret használjuk. A biometrikus azonosítási módszerek folyamatosan fejlődnek, és még inkább életünk részévé válik.

A biometrikus azonosítás egyre inkább előtérbe helyezése nagyon érzékeny téma, hiszen tele van személyes adattal, mégpedig olyan adatokkal, amelyekből könnyen egyéb információ is kiderülhet az adott személyről, így a kor, az egészségi állapot, a bőrszín, vagy akár a nemi orientáció is. A GDPR[2]-szabályok értelmében is, a biometrikus azonosítás témakörében különösen fontos az adatok felhasználásának célhoz kötöttsége. Ennek értelmében meg kell határozni, hogy ki és hogyan vehet fel mintákat, hogyan lehet azt tárolni, harmadik félnek átadni.

Kutatásom központi kérdése, annak vizsgálata, hogy a magyar büntetés-végrehajtásban, van-e lehetőség a fogvatartotti állomány körében, a jelenleg használt tárgyú alapú azonosítás kiváltására biometrikus azonosító rendszerrel.

A magyar törvények szerint a biometrikus azonosítást a büntetés-végrehajtásban jelenleg a fogvatartottak intézetbe vonulásakor, azaz a befogadás során alkalmazzák. Egy korábbi cikkemben bemutattam a törvényi hátteret, melyek közül a Bv. törv[3]ényre is kitértem. A befogadást végző büntetés-végrehajtási intézet köteles az elítélt személyazonosságát, a bűnügyi nyilvántartási rendszer adatait ellenőrzi, illetve az iratokban szereplő adatokat is megnézni. Az ujj- és tenyérnyomat vételt, valamint a DNS-mintavételt a büntetés-végrehajtási (a továbbiakban: bv.) intézet erre kijelölt tagja végzi. A bv. intézet az elítélt azonosítása érdekében rögzíti az elítélt ujjnyomatát és kezdeményezi a szakértői nyilvántartó szervnél a Bnytv.[4] 82. § (5) bekezdés b) pontja szerinti összehasonlítást. Véleményem szerint a befogadáson megjelenő személy adatai ellenőrzésével egyidejűleg célszerű lenne a szakértői nyilvántartó szervtől megkérni a fogvatartott ujj- és tenyérnyomatát, illetve a DNS-mintáját is. Azonban, ha a nyilvántartásban nem szerepel, akkor a bv. személyi állományi tag elvégzi a nyomatok, illetve minták vételét és a szakértői nyilvántartásba vétel céljából megküldi azokat. [1, pp. 15-21.]

Kutatásom során a tenyérvéna alapú és az ujjnyomat alapú azonosítási módszereket hasonlítom össze, a börtönök, fegyházak, fogházak használhatósága szempontjából. A bv. intézet különös környezet a biomerikus azonosítás szempontjából, hiszen fogvatartottak azonosítása a cél. A bv.-ben az általánostól eltérő alkalmazási lehetőségeket szükséges figyelembe venni, ezért is esett a választásom erre a két azonosítási módszerre, melyet a későbbiekben bővebben kifejtek.

[2] General Data Protection Regulation (általános adatvédelmi rendelet)

[3] 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról

[4] 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról

A FOGVATARTOTTAK AZONOSÍTÁSA

Ezt a fejezetet 12 éves tapasztalatomra alapozom, amelyet a büntetés-végrehajtási szervezetnél, informatikai szakterületen töltöttem. Ebben az időszakban folyamatosan kutattam a fogvatartottak biometriai jellemzőivel történő azonosításának lehetőségeit. A fogvatartotti azonosításának fejlődéséről összefoglaló dokumentáció jelenleg nem áll rendelkezésre. Célom, hogy munkám során a magyar börtönökben használt azonosítási rendszerekről és fejlődéséről átfogó képet adjak, illetve az, hogy a fogvatartottak személyazonosításának jövőjét vetítsem előre a magyar börtönökben. Fontos megjegyeznem, hogy a fogvatartottak nyilvántartása sokrétű, azonban a büntetés-végrehajtási szervezet bűnügyi nyilvántartása nem azonos az igazságszolgáltatási szervek által elérhető adatokkal.

2004-ig a börtönökben a fogvatartottak azonosítására nem állt rendelkezése automatikus azonosítási rendszer. A telefonálásra a körletekre helyezett telefonkészülékekkel volt lehetőségük az elítélteknek. A telefonálási igényének regisztrálása ekkor még papír alapon történt. A telefonálás telefonkártya használatával, a személyi állomány részvételével történt. A hívásokat is csak papír alapon adminisztrálták, ahogyan az intézet boltjában megvalósított vásárlásokat is.

A 2005-ben bevezetésre került vonalkódos fogvatartotti azonosítás. Logikája jól átgondolt, kiépítése meghozta a várt elképzelést, könnyebben lehetett kezelni az elítéltek pénzügyi tranzakcióit. A vásárlási, telefonálási műveletek időbeli végrehajtása is jelentősen csökkent.

2013-ban a fogvatartottak nyilvántartási rendszere teljesen új alapokat kapott, melynek során a cél a fogvatartottak azonosításának megújítása is volt, a vonalkódot elkezdte kiváltani a QR-kód.

2019-ben az NFC alapú azonosítás már nemcsak a személyazonosítás lehetőségén változtatott, hanem a mindennapi rutin feladatokat is leegyszerűsítette. A fogvatartotti adatnyilvántartás, és azonosítás jelentősen megújult.

A fejlődés során új koncepciók alakultak ki, a tárgyi alapú azonosítás azonban maradt. A fogvatartottak azonosítására alkalmazott informatikai háttér jól kidolgozott, a rendelkezésre álló rendszer alkalmas újabb – akár biometrikus azonosításon alapuló – azonosítási módszer kialakításához is. [3, pp. 118-124.]

SZEMÉLYAZONOSÍTÁS FONTOS SZEREPE A BÜNTETÉS-VÉGREHAJTÁSBAN

A büntetés-végrehajtásban a személyazonosság megállapításának, azaz az egyén azonosságának jelentős szerepe van. A minden napi rutinfeladatok során többször is szükséges végrehajtani a személyek azonosítását, melyek a fogvatartottak mozgatásával járnak. Ezek közül a legjelentősebbek:

- a befogadás,
- a hozzátartozó látogatás fogadása,
- az elítélt munkába állítása,
- munkába kísérés, munkából visszakísérés,
- a börtön boltjában vásárlás,
- a börtönben kihelyezett fali telefonkészülékkel telefonálás (ez a feladat már lassan megszűnik. a készülékek kivonásra kerülnek az intézetekből),

- az egészségügyi ellátás,
- egyéb mozgatásoknál, pl.: szabadlevegőn tartózkodás megvalósítása, illetve
- a jogérvényesítés tevékenységek során fontos.

Kutatásom során a büntetés-végrehajtás jelenleg használatban lévő oktatási jegyzetében megtaláltam a fogvatartottak azonosításáról szóló összefoglaló leírást. Ez alapján a fogvatartottak azonosítását a zárkából történő kivétel után végre kell hajtania a személyi állománynak, mely a fényképes nyilvántartás alapján valósítanak meg, és az egyeztetés kiterjed a fogvatartás, valamint a fogvatartott legfontosabb személyes adataira is. Tehát a személyi állomány azonosítja a fogvatartottat. A fogvatartott részlegen történő átadását megelőzően a körletfelügyelő a feladatot végző felügyelő részére tájékoztatást ad a körszállításban részt vevő fogvatartottak aktuális magatartásáról, hangulatáról, viselkedéséről, egyéb lényeges információkról. A körlet-főfelügyelőtől a mutatókartonokat átveszi a felügyelő, a jóváhagyott szállítási lista alapján az összes karton meglétét, valamint azokon a célintézet megjelölésének meglétét ellenőrizni szükséges. A célintézetek mutatókartonra történő felvezetése az éjszakás körlet-főfelügyelő feladata. A szállítás során kiemelt figyelmet érdemlő fogvatartottakról készült feljegyzéseket a mutatókartonhoz kell csatolni. Fentiek alapján megállapítom, hogy a jegyzetben megfogalmazott leírás alapján a büntetés-végrehajtásban a fogvatartottak azonosításánál jelentős szerepe van a személyi állománynak. [4, pp. 245-246.]

A BIOMETRIKUS AZONOSÍTÁSI MÓDSZEREK KONCEPCIÓI

A biometrikus azonosításban korábban az ujjnyomatot és a DNS-t használták azonosításra, ma már szélesedik ez a skála, például a retina- és íriszazonosítást, a kézgeometriai vizsgálatot, a hanganalízist, véna azonosítást, vagy éppen az arcfelismerést is alkalmazzák. Ezeket az azonosítási lehetőségeket a tudomány és a technológia fejlődése teszi lehetővé, a módszerek folyamatosan fejlődnek. Legnagyobb előnye, hogy az azonosítást az ellenőrzést végző személytől függetlenül lehet végrehajtani. Korábban szükség volt az ember szakértelmére, aki az összehasonlítást elvégezte, ma már elegendő az azonosításhoz az informatikai-, technikai háttér, és az összehasonlító szoftver. Az azonosítást végző személy részéről a biometrikus adatok vonatkozásában különösebb szakértelemre nincs szükség, azonban mégis fontos, hogy alapvető ismeretekkel rendelkezzen a használatával kapcsolatban. [5, pp. 4-19.]

Tenyérvéna alapú azonosítás

A Fujitsu megalkotta a tenyérvéna alapú azonosítás technológiáját, amelyet PalmSecure-nak nevezett el. Az azonosítás a vénamintázat felismerésével történik. Az egyénre jellemző vénamintázat rögzítéséhez a PalmSecure infravörös-közeli sugarakat bocsát ki, amelyeket az ember tenyerének ereiben áramló vérben található oxigénmentes hemoglobin elnyel, ezáltal a tenyér képe vénamintázatként rögzíthető, és az azonosított korábban rögzített mintájával összehasonlítható. A vénaszkennerben található szenzor jóval több pontot olvas le az emberről, mint más biometrikus azonosító berendezés, maximum 5 000 000 referenciaponton méri a tenyér felszíne alatt található vénastruktúrát személyazonosítás céljából. A módszer érintkezésmentes beolvasást alkalmaz, ami higiénikus módszer. A nyitott tenyér (ujjak nélkül) komplex vénamintázatának leolvasása 4-6 cm-ről történik, tehát a technológia non-invazív. Mivel az erek a testen belül találhatók, a személyazonos-

ság hamisítása rendkívül nehéz, így garantált a nagyfokú biztonság, nem másolható, nem reprodukálható és nem tulajdonítható el, továbbá titkos adatgyűjtésre sem alkalmas.

Fontos tény, hogy az azonosítás csak élő szervezet esetében lehetséges, hiszen a szervezetből nyert információhoz aktív vérkeringésre van szükség. Az egyedi mintázat 5-6 éves korra kialakul, és az életkor előrehaladtával már nem változik. Elmondható, hogy az azonosítás folyamata kényelmesebb, mint pl. az írisz vagy a retina alapú azonosítás alkalmazása esetén. Az innováció műszaki alapja egy kisméretű (35x35x27 mm) és kis súlyú (50 g) egység, ami integrálható multimodális – más funkciókat is ellátó – eszközökbe. Ezáltal azonosítás céljából a beléptető rendszerekben is kiváló alkalmazási lehetőség.

A Fujitsu tájékoztatása szerint egy szkenner eszköz nagyságrendileg 140 000 Ft-ba kerül, azonban a rendszer kialakítása ennél nagyobb költséget von maga után. A kiépítéshez szükséges a megfelelő szoftver, illetve licencek beszerzése, az infrastruktúra kialakítása szintén elengedhetetlen. Tehát önmagában az eszköz megvásárlása nem elég a módszer használatához, ehhez tartozik még a háttérben futó informatikai rendszer is, melynek költségét, annak bonyolultsága határozza meg.

Ha csak számítógépes azonosításhoz, fizetéshez szükséges a vénaleolvasás, akkor elég egy vénaszkennelésre alkalmas egér vagy egy USB-csatlakozós céleszköz, melyek offline állapotban is működnek. Kutatásom tárgya azonban bonyolultabb rendszer kialakítását vonja maga után. [6, pp. 225-234.]

Ujjnyomat alapú azonosítás

Jelenleg a biometrikus eszközök közül a legnagyobb számban az ujjnyomat vizsgáló eszközöket alkalmazzák. Az ujjnyomat azonosításnak többféle megközelítés van. Egyes eljárások a minucia[5] azonosítás hagyományos rendőri módszerét használják (ujjnyomat olvasás), mások egyszerű alakzatazonosító eszközök, ismét mások határtartományokat és ultrahangos letapogatást használnak. Nem mindegyik ujjnyomat olvasó szenzora érzékeli, hogy élő az ujj.

Az ujjnyomat leolvasóknak 3 fő típusa van:

- optikai: a legrégebbi technológia, mely során egyszerűen egy, vagy több kép készül az ujjról, majd olvasás során ezt próbálják meg összehasonlítani az eltárolt képekkel.
- kapacitív: a jelenleg legelterjedtebb módszer, szinte minden mobilban ez található. A módszer során az olvasó alatt rengeteg érzékelő található, melyek a lehető legpontosabban megjegyzi az ujjak domborzatát.
- ultrahangos: a legújabbnak számító technika, ahol már nem kell az ujjal közvetlenül érintkeznie az olvasónak. Működési elve hasonló a kapacitív olvasóéhoz, ugyanis az ujjak felületét szkenneli, de nem kontakt során, hanem ultrahanghullámok segítségével.

Hátránya lehet egyes típusának, hogy a gép nem fogadja el a frissen mosott kezet, ujjat, mivel azok túlságosan természetellenesek, illetve a nedves bőrrel történő azonosítás is hibára futhat. Előfordulhat, hogy a szenzor válik piszkossá, hiszen nagy igénybevételnek van kitéve. A kéz és a szenzor tisztasága ugyanolyan jelentőséggel bír. [7]

[5] A kéz és az ujjak belső oldalán látható elágazások, szigetek, villák, pontszerű képződmények, megszakadások, jellegzetes kezdő és végpontok, átmenő fodorszálak.

Az ujjnyomat-azonosítás előnye, hogy alacsony a FAR[6], és inkább használatból hibákkal lehet találkozni alkalmazása során. A technikai megoldások felhasználóbarátok, egyszerűen telepíthetők, kis méretekkel rendelkeznek, és üzemeltetésük viszonylag egyszerű. Hátránya, hogy a nyomat eredménye függ a nyomás nagyságától, az ujjak nedvességétől, a személy munkájától (a sokat gépelő emberek ujjain a mintázat megkophat), az ujjak szennyezettségétől.

Módszerspecifikus alkalmazás szempontrendszere alapján a személyazonosítás:

- részben mindenkinél alkalmazható,
- részben eltérő helyszíneken és ellenőrzési körülmények között is felhasználható,
- az ellenőrzés folyamatába építhető,
- nem belső biometrikus azonosítón alapul,
- az esetek többségében, jelenleg még nem kontaktmentes a kapcsolat,
- nem eredményezi az ellenőrzési idő jelentős növekedését,
- azonnali eredményt biztosít. [8, pp. 131-134.]

AZONOSÍTÁSI MÓDOK ÖSSZEVETÉSE

A kiválasztott azonosítási módszernek, az alapvető igényeknek szükséges megfelelni. Az elvárás az, hogy legyen egyszerű, gyors, megbízható, biztonságos és lényeges a készülék ár/érték aránya is. Ahhoz, hogy a megfelelő eszköz kiválasztásra kerüljön, meg kell ismerni az azonosítási módszereit és felhasználhatóságát.

Mindkét azonosítási módszernél az azonosítandó személy kezére van szükség, mely higiéniai szempontból előnyös lehet az intézetekben, hiszen a tisztántartását egy kézmosással meg lehet valósítani, ha esetleg az azonosítást a kosz befolyásolná.

Az előző fejezetben elemzett azonosítási módok jellemzőit, a büntetés-végrehajtási intézetek igényeinek megfelelően, összefoglalom az alábbi 1. Táblázatban:

Tulajdonság	Tenyérvéna	Ujjnyomat
leolvasás távolsága	érintkezésmentes, 4-6 cm	közvetlen érintkezés/ érintkezésmentes
pont olvasás	5 000 000	kb. 30-60
élő azonosítás	igen	igen/ nem
olvasó egységár	140 000 Ft	60 000 Ft
sebesség	1 másodperc	1 másodperc
téves elutasítás okai	sérülés	kosz, sérülés

1. Táblázat: Tenyérvéna-, ujjnyomat azonosítás összehasonlítása, saját szerkesztés

A börtönökre jellemző, hogy egyszerre több, - munkába felvonulás során, akár 200 - fő is együtt mozog. Az azonosításnak ennek értelmében gyorsan kell megvalósulni. A módszer kiválasztása során fontos figyelembe venni a környezetet, sok különböző ember tartózkodik egy térben, a higiénikus körülmények nem mindig megfelelőek. A fogvatartottak körében könnyen előfordul, hogy a munkájuk során sérüléseket szereznek a ke-

[6] False Accepting Rate – téves elfogadási arány: hibás elfogadás mértéke, ami megadja, hogy az eszköz milyen arányban ismert fel jogosulatlan felhasználót jogosultként.

zükre. Ez azért lehetséges, mert fizikai munkát végeznek: takarítanak, mezőgazdaságban tevékenykednek, építőipari munkákat végeznek, sok esetben különböző szerszámokat használnak. Ez azért lényeges, mert a vizsgált azonosítási módokhoz a személyek kézére van szükség. Figyelembe véve az esetleges sérüléseket az ujjnyomat azonosítás előnyt élvez ebben az esetben, a tenyérvéna alapú azonosítással szemben. A tenyér nagyobb felületű, mint az ujj, így a sérülés esélye is nagyobb. Az ujjnyomatolvasó használatánál lehetőség van arra, hogy egy fogvatartott több ujjnyomatát is tároljuk azonosítás céljából, így növelhetjük még a biztos azonosítás lehetőségét.

Az azonosításra várók sok esetben türelmetlenek, nem megfelelően hajtják végre a kapott utasításokat, melynek következtében a használatból eredő azonosítási hibák száma is növekedhet. Jelentős kitétel az új rendszer kiválasztásánál, hogy a rendszer használata az azonosítottak részére könnyen elsajátítható legyen, az azonosítás gyorsan megvalósuljon. Bár a tenyérvéna alapú azonosító rendszerek kezdenek elterjedni és a visszajelzések alapján megfelelően működik, alkalmazása mégsem rendelkezik sok tapasztalattal. Tekintettel arra, hogy mind a személyi-, mind a fogvatartotti állomány már rendelkezik ujjnyomat olvasó eszköz használatával célszerű az ujjnyomat alapú azonosítást bevezetni a büntetés-végrehajtásnál. A vizsgált környezetben célszerű már ismert, megfelelően működő rendszer kialakítása. [9]

JAVASLATOK

A GDPR kiindulópontja az, hogy a személyes adatok különleges kategóriáinak és az ebbe a körbe tartozó biometrikus adatoknak a kezelése tilos, tekintettel arra, az alapvető jogok és szabadságok szempontjából a természetüknél fogva különösen érzékeny személyes adatok egyedi védelmet igényelnek, mivel az érintettek jogaira nézve a kezelésük körülményei jelentős kockázatot hordozhatnak.

A biometrikus adatok fokozott védelmének indoka az, hogy a biometrikus adatok közvetlenül kapcsolódnak az érintetthez, csak rájuk jellemzőek és állandók, ezért nem, vagy csak nehezen változtathatók meg, nem tagadhatók le, ezért visszavonhatatlanok. Éppen ezért a biometrikus adatokkal kapcsolatos bármely jogsértés veszélyezteti a biometrikus adat további felhasználását és felhasználhatóságát, amelyekre vonatkozóan nincs lehetőség a jogsértés következményeinek enyhítésére. [10, pp. 9-21.]

Jelenleg a fogvatartottak azonosítása tárgyi alapú, a részükre elkészített – az egyedi nyilvántartási számot is tartalmazó – kártyával valósul meg. Ennek hátránya, hogy a kártyát elveszítheti a fogvatartott, vagy eltulajdonítják tőle társai. Megtalálása érdekében nyomozást szükséges indítani, amely sok időveszteséggel és munkaerő lefoglalással jár.

Véleményem szerint fontos a biometrikus jellemzőt alkalmazó fogvatartotti azonosító rendszer kiépítése a magyar büntetés-végrehajtásban. Javaslatom, hogy a tárgyi alapú azonosítás kiváltása egyelőre ujjnyomattal valósuljon meg, tekintettel arra, hogy az intézeti befogadások során az ujjnyomat rendelkezésre állhat. Az új azonosítási rendszer kialakítása során azonban fontos kiemelni, hogy a szervezet jogszabályi háttérét szükséges módosítani a biometrikus azonosítás bevezetése előtt. A törvényi szabályozás nem teszi lehetővé jelenleg, hogy az ujjnyomatot a büntetés-végrehajtás tárolja, illetve felhasználja más célokra.

Tapasztalataim alapján elmondható, hogy a háttér informatikai rendszer már rendelkezésre áll. A biometrikus azonosításnak az egyik legfontosabb előnye a börtönökben,

hogy a fogvatartottnak semmilyen azonosításra alkalmas tárgyat nem kell maguknál tartani.

A bv. intézeteiben sok ember él együtt. Ezt szem előtt tartva célszerű egy olyan eszközt kiválasztani, amely kevésbé koszolódik. A higiénia megtartása fontos ebben a környezetben, illetve működése stabil, az eszköz karc és ütésálló legyen. A napi feladatok során sokszor kell azonosítani a fogvatartottat, ebből adódóan célszerű egy olyan eszközt kiválasztani, amely kiértékelési ideje minimális. [11, pp. 45-46.]

Első lépésként célként határoznám meg, hogy az újonnan bevezetett biometrikus azonosítás segítségével tudjanak vásárolni. Az ujjnyomat rendelkezésére állásával már egyéb használatára is szert lehet tenni, melyek a napi feladatokat gyorsítanák és könnyítenék meg. Megoldható lenne ennek segítségével pl. a fogházas körleten a mozgások szabályozása is.

Az ujjnyomat olvasó azonosítási technológia kiépítését a büntetés-végrehajtás szervezetén belül pilot rendszerben célszerű megvalósítani. A szervezetnek ebben már jelentős tapasztalata van, és jól működik. Ha az igényekhez mérten sikerül beágyazni a teszt intézetnél, a jelenlegi rendszerbe a biometrikus azonosítást, akkor történhet meg az országos szintű kiterjesztése. Ehhez azonban szükséges megvizsgálni a biometrikus azonosítás bevezetésének megvalósítása érdekében az informatikai rendszert.

Egyelőre a biometrikus azonosítás bevezetése kizárólag, szigorúan csak önkéntes alapon, az eddigi kártyás azonosítással párhuzamosan történne. Ennek bevezetésénél a fogvatartott egy nyilatkozat aláírásával igazolja beleegyezését, az új rendszer tesztelésében való részvételét. Aki ezt nem teszi meg, annak természetesen nem származik semmilyen hátránya, ugyanúgy használja a rendszert, mint eddig.

Ha az ujjnyomat olvasó használata eléri a kívánt biztonsági működést a teszt intézeteknél, akkor az elkövetkezendő időszakban az egész országra ki lehet terjeszteni ennek bevezetését. Azonban kötelező használatához törvényi változásokra van szükség. Az újonnan megálmodott rendszerek bevezetése meghatározott ütemezés szerint kell, hogy megtörténjen. Jelentős feladat, hogy a bv. számára legoptimálisabb lehetőséget feltárjam, és hosszú elemzések soraként egy konkrét terv álljon össze.

ÖSSZEGEZÉS, KUTATÁSI EREDMÉNYEK

Munkám során a büntetés-végrehajtás fogvatartotti állomány azonosításának megújítását vettem előtérbe. Témaválasztásom aktualitását a rohamosan fejlődő azonosítási lehetőségek indokolják.

Elemeztem a tenyérvéna-, és az ujjnyomat alapú azonosítási technológiákat, kiválasztottam azt az azonosítási lehetőséget, amely jelenleg a közelebb áll a büntetés-végrehajtási intézetekben megvalósíthatóságát illetően. Hangsúlyt fektettem a jelenlegi azonosítási technika kialakulására, illetve kitértem az azonosítások alkalmazásának fontosságára a börtönökön belül. Javaslatot tettem a kiválasztott biometrikus azonosító rendszer bevezetésének hátterére és koncepciójára a szervezetnél.

Összefoglalva – véleményem szerint – publikációm jól hasznosítható támpontként a biometrikus azonosító rendszer, büntetés-végrehajtási szervezetnél szükséges bevezetése során.

Kutatásom folytatásaként felmerül a kérdés, hogy a büntetés-végrehajtásban jelenleg alkalmazott tárgyi alapú és biometrikus azonosítások figyelmen kívül hagyásának

következtében, valóban az ujjnyomat alapú azonosítás lenne-e a legmegfelelőbb módszer a fogvatartottak azonosítására.

IRODALOMJEGYZÉK

[1] KONDÁS, Katalin – SZŰCS, Endre: A személyazonosításra vonatkozó speciális szabályok a büntetés-végrehajtásban, Biztonságtudományi Szemle, Évf. 2. szám 2., 2020., pp. 15-21., https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/52/49 (letöltve: 2021.10.20.)
[2] KONDÁS, Katalin: Identification of convicts in Hungarian prisons, Revista Academiei Fortelor Terestre NR. 2 DOI: 10.2478/raft-2021-0017 (102)/2021., pp. 118-124., https://www.armyacademy.ro/reviste/rev2_2021/Art_Kondas.pdf (letöltve: 2021.11.01.)
[3] KOCSIS, Zsolt: Büntetés-végrehajtási Biztonsági Ismeretek, Közép- és felsőfokú szaktanfolyami képzés jegyzet, 2021., pp. 245-246., 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 (letöltve: 2021.10.10.)
[4] BALLA, József: A rendészeti célú személyazonosítás biometriája, Határrendészeti tanulmányok, XIII. évfolyam 3. szám, 2016., pp. 4-19., https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/2016-3_-szam.original.pdf (letöltve: 2021.10.05.)
[5] PRISZNYÁK, Szabolcs: A tenyérvéna alapú azonosítás egyes alkalmazási lehetőségei. Pécsi Határőr Tudományos Közlemények, XV., 2014., pp. 225-234., http://www.pecshor.hu/periodika/XV/prisznyak.pdf (letöltve: 2021.10.07.)
[6] KOVÁCS, Tibor – MILÁK, István – OTTI, Csaba: A biztonságtudomány biometriai aspektusai, Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról, XIII. kötet, 2012, http://www.pecshor.hu/periodika/XIII/kovacsti.pdf (letöltve: 2021.10.01.)
[7] BALLA, József: A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására, Dialóg Campus Kiadó Budapest, 2019., pp. 131-134., https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Balla_Jozsef_biometrikus_adatok-okmany.pdf, (letöltve: 2021.10.12.)
[8] http://www.biosecgroup.com/hu/technologia, letöltve: 2021.10.20.
[9] KOVÁCS, Tibor – MIKLÓS, Gellért: A biometrikus rendszerek adatvédelmi szempontú elemzése Biztonságtudományi Szemle, 2021. III. évf. 3. szám, pp. 9-21., https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/151/139 (letöltve: 2021.10.18.)
[10] KONDÁS, Katalin: Fogvatartotti azonosítás a büntetés-végrehajtásban, Diplomamunka, 2013., pp. 45-46.

JOGSZABÁLYOK

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról
2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról

ENHANCING PERSONAL SECURITY THROUGH ADAPTATION OF STRATEGIC MODELS

AZ EGYÉN BIZTONSÁGÁNAK FOKOZÁSA A STRATÉGIAI MODELLEK ADAPTÁLÁSÁVAL

FÜRTÖS János[1] – SZAKALI Miklós[2]

Abstract

In this article we would like to draw attention to the importance of personal security, taking into consideration that the state is unable to provide full protection to its citizens against the current and possible future complex security challenges. We emphasize the need for a change of approach in the personal security, and for the fact that personal security must also be interpreted and managed in a complex way in line with the challenges. We believe that in this rapidly changing security environment, the individual must also play a much more active role in strengthening their own security. As a first step in the change of approach, we would like to promote a forward-looking and security-aware way of thinking with the methods and examples described in this article. In our view, proven strategic models applied in security policy can greatly contribute to develop a structured, security-aware way of thinking. Alongside the structure of the models, individuals can develop their own concept and activities to increase their personal security based on the current and the foreseeable future challenges and their own capabilities.

Keywords

individual security, complex approach, security awareness, foresight, strategic models

Absztrakt

A cikkben az egyén biztonságának előtérbe kerülésére hívjuk fel a figyelmet, tekintve, hogy korunk komplex biztonsági kihívásainak negatív hatásaival szemben az állam nem képes teljes védelmet nyújtani a polgárainak. Fontosnak tartjuk kiemelni a szemléletváltás szükségességét az egyén biztonságának megközelítésében. A kihívásoknak megfelelően az egyén biztonságát is komplex módon kell értelmezni és kezelni. Úgy gondoljuk, hogy ebben a gyorsan változó biztonsági környezetben sokkal aktívabb szerepet kell vállalnia az egyénnek is saját biztonsága erősítése érdekében. A szemléletváltás első lépéseként szeretnénk elősegíteni az előrelátó, biztonságtudatos gondolkodást a cikkben leírt módszerekkel és példákkal. Úgy gondoljuk, hogy a biztonságpolitikában bevált stratégiai modellek nagymértékben segíthetik az egyén strukturált biztonságtudatos gondolkodásának a fejlődését. A modellek felépítése mentén az egyén saját biztonsági helyzete és lehetőségei alapján kialakíthatja saját stratégiáját és megtervezheti a szükséges lépéseket biztonsága növelése érdekében.

Kulcsszavak

egyéni biztonság, komplex megközelítés, biztonságtudatosság, előrelátás, stratégiai modellek

[1] furtosjanos@onvedelemoktatas.hu | ORCID: 0000-0003-3699-1101| self defence expert | önvédelmi szakértő
[2] mszakali@hotmail.com | ORCID: 0000-0002-8983-3855|doctoral candidate, Óbuda University Doctoral School on Safety and Security Science | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

AZ EGYÉN BIZTONSÁGÁNAK KIALAKULÁSA

A biztonság, mint alapkövetelmény az emberiség kialakulásával egyidős. Végigkísérte az emberiség és az emberi társadalmak fejlődését napjainkig, illetve a jövőben is alapvető fontosságú marad. A biztonság megléte, illetve a biztonságra való mind nagyobb mértékben való törekvés alapvető feltétele volt az emberi faj életben maradásának és fejlődésének. A biztonság szavatolása érdekében már a kezdetektől fogva nem csak az időjárás, az elemek, a növény-, és állatvilág kihívásaival kellett megküzdeni az embernek a túlélésért, hanem a fajtársakkal is. A közösségek kialakulásának kezdeti szakaszában szinte kizárólag a fizikai erő és ügyesség döntött az életben maradásról, és a jobb életfeltételek biztosításáról. Mindezek alapján megállapíthatjuk, hogy kezdetektől fogva az egyén biztonságát és ezzel az életét is az egyén tágabb értelemben vett önvédelemi képességei határozták meg.

A háború és a fegyveres harc nem csak az egyén biztonságát befolyásolta, hanem az adott hadsereg, és ezzel együtt az állam megsemmisüléséhez is vezethetett, amely együtt járt a nemzet szuverenitásának elvesztésével, lakosságának kifosztásával és rabszolgasorba taszításával vagy kipusztításával. Mint tudjuk, számtalan olyan nép és birodalom (gótok, longobárdok, Római Birodalom, Asszír Birodalom, stb) tűnt el a történelem süllyesztőjében, melyek létezéséről ma már csak történelemkönyvekben olvashatunk. Ezért a biztonság súlypontja már ekkor áttevődött az egyéni biztonság fontosságáról a társadalmi biztonság elsődlegességére, és ennek a felismerésnek a kapcsán meghatározóvá vált a haderő helyzetének és fejlesztésének, valamint a háború, a fegyveres harc elméleti kérdéseinek fontossága. Ez a folyamat azonban nem állt meg az ókorban, tovább folytatódott a középkoron keresztül egészen napjainkig. Cikkünknek nem célja részletesen bemutatni, hogyan változtak a biztonsági felfogások/stratégiák a történelem folyamán, és azok milyen lényegi változásokat okoztak a nemzetek és az egyének biztonsága területén. Napjaink biztonságát még mindig befolyásolja a II. világháborút követően kialakult biztonsági szemlélet, amely lényegében a hidegháború végéig tartotta magát és a biztonságot a háború és béke kérdésének tekintette. Ezért a katonai erő fejlesztésének és alkalmazásának meghatározó szerepe volt a biztonság szavatolásában, ugyanakkor minden egyéb tevékenységet csak ezzel összefüggésben, ennek támogatására értelmezett. Ez a biztonsági szemlélet megmutatkozott a nemzetközi biztonsági struktúrák és intézmények kiépítésében is. Ebben az időszakban alakultak meg azok a nemzetközi szervezetek, amelyeknek alaprendeltetése a nemzetközi béke és biztonság megőrzése volt, főleg politikai és katonai eszközökkel. [1] Mindez alátámasztja azt a megállapítást, hogy az egyén biztonsága szigorúan alárendelt viszonyba került a társadalom, az állam biztonságához képest, valamint teret nyert a biztonság regionális és globális fontossága.

AZ EGYÉNI BIZTONSÁG VIZSGÁLATÁNAK MEGKÖZELÍTÉSEI

Az egyén biztonságának kérdése önmagában is és a biztonság egészére nézve is meghatározó fontosságú, ezért több tudományág is vizsgálta és jelenleg is vizsgálja törvényszerűségeiket és összefüggéseiket. Az első fontos lépés a pszichológia területén történt, amely az egyén motivációjára, a motivációs szintek hierarchiájára koncentrált. [2] Az egyén biztonságának fontosságát és helyét is Abraham Maslow amerikai pszichológus határozta meg a motivációs hierarchiában. A kutatás az egyén szükségleteire fókuszált, azonban fontos információt jelentett a társadalom működésének és összefüggéseinek megértéséhez is.

Maslow kutatási eredményeit először 1943. július 1-én publikálta „A Theory of Human Motivation/Az emberi motívumok elmélete" című tanulmányában. Kezdeti elképzeléseit tovább fejlesztette, és a "Motivation and Personality/Motiváltság és személyiség" című könyvében mutatta be részletesebben 1954-ben.

A Maslow-piramist 5-lépcsősként jellemezzük, amely így néz ki:

1. Ábra: Maslow piramis (forrás: https://hu.wikipedia.org/wiki/Maslow-piramis)

Az emberi motivációk és szükségletek egy szétágazó és egyénenként eltérő rendszert mutatnak be. Ez a rendszer a végrehajtás szempontjából is teljesen különböző. A motívumkutatások szerint az emberek először a legfontosabb és legsürgősebb szükségleteiket elégítik ki. Mint látjuk az ábrán, a biztonság az ember életének nélkülözhetetlen eleme, és ezért került a második helyre, közvetlenül a létfenntartást követően. A biztonság fogalma ugyanakkor idővel változott. Régen sokkal inkább fizikai jellegű volt. Kellett egy menedék, ami véd az időjárás viszontagságaitól, fegyver, amivel meg tudja védeni magát, és családját az egyén, vagy tűz, amely meleget ad. Ma már nem ugyanaz a jelentése. Sokkal komplexebb szükséglet lett, hiszen a "menedék" mellett jelentheti az egészségi és akár az anyagi biztonságunkat is. Abraham Maslow szerint az emberi szükségletek hierarchikus megközelítéssel leképezhetők egy piramismodellel, melynek az alapja jelenti a nélkülözhetetlen és ezért legfontosabb követelményeket. Ezek alapján:

- A piramis alján az alapszükségletek, a létfenntartáshoz kapcsolódó szükségletek helyezkednek el.
- A létfenntartás megteremtése magával hozza a biztonsági szükségletek kialakulását: ez az élet, a család és a megszerzett javak megóvását, védelmét jelenti.
- A szociális szükségletek az ember társas lény mivoltából fakadnak. A szociális szükséglet kapcsolatteremtési, összetartozási szükséglet. Ennek kielégítése érdekében törekszik az egyén jó családi, érdeklődésének, gondolkodásmódjának megfelelő baráti, munkahelyi kapcsolatokra.
- Az ember igyekszik megtalálni helyét a többiek, a társai között, ebből fakad az elismerés iránti szükséglete: igyekszik elfogadtatni magát, elismertetni egyéniségét, képességét, rátermettségét.
- A piramis csúcsán az önmegvalósítás szükséglete áll. Az emberek egy része erős késztetést érez arra, hogy képességét, tehetségét maximálisan kihasználja.

A piramis alapjának alsó két szintje jelenti a piramis (az egyén életének) stabilitását, amely nélkülözhetetlen a további szintek építéséhez és az egyén életének kiteljesedéséhez.

A biztonság-, állam- és hadtudományok folyamatosan fejlődtek és a nemzetek, régiók, illetve a globális biztonság kutatására fókuszálták erőkifejtéseiket, nem pedig az egyén biztonságára. Az egyén biztonságának szavatolását az állam feladatának tartották és azt az állam által biztosított keretek között megoldottnak tekintették. Ezt az álláspontot igazolni látszott az a tény, hogy a törvényalkotás és törvénykezés, valamint az erőszakszervezetek (rendőrség, haderő, büntetésvégrehajtás) létrehozása, fenntartása és alkalmazása az állam monopóliumát képezték. Mindezek együttes rendelkezésre állása esetén garantáltnak vették az államrend, a közrend fenntartását és egyben az egyén biztonságát is.

Később, jellemzően a hidegháborút követően, a biztonságtudományok túlléptek a katonai biztonság kizárólagosságán és tágították a biztonsági horizontot. Azonosították a biztonság különböző szintjeit, amelyek önállóan is értelmezhetőek és kölcsönhatásaikban is meghatározóak. Mindezek alapján a biztonság négy szintjét különböztetjük meg, az egyénit, a nemzetit, a nemzetközit (regionálist) és a globálist. [3] Ekkor nyert teret a biztonság egyéni szinten és kölcsönhatásaiban történő vizsgálata.

A humán biztonság kérdése is ekkor került a figyelem előterébe. Ez az elmélet a klasszikus, államokra alapozott biztonság elsődlegességét kérdőjelezi meg, azt állítva, hogy az állam helyett az egyént kellene a biztonsági koncepciók középpontjába állítani. Ez ugyanis mind nemzeti, mind regionális és globális szinten kevesebb konfliktust, és nagyobb stabilitást eredményezne. Egyrészt tehát a kiindulási alap eltér a klasszikus realista biztonságfelfogásétól: a hangsúly áthelyeződik az államról az egyénre. Másrészt a hatókör is változik: a klasszikus biztonságfelfogás külső agresszióval szemben védi az államot, míg a humán biztonságban ez a koncepció kiegészül olyan szélesebb körű fenyegetésekkel, mint a környezetszennyezés, a klímaváltozás vagy a járványok. Ugyanakkor azt is figyelembe kell venni, hogy a humán biztonság elmélete nem vált széleskörű gyakorlattá, állami szinten csak néhány állam kezdett fókuszáltan foglalkozni a gyakorlati megvalósításával. Ezek az államok (Kanada és Japán) is a humán biztonság egy-egy aspektusára helyezték a hangsúlyt, és nem egy komplex megközelítést követtek. [4] Ezzel ugyan tágult az egyén biztonságának megteremtésében résztvevő szereplők száma, azonban így is az egyén biztonságának első számú felelőse az állam marad.

Jelentős állomás a biztonságtudományok fejlődésében az új típusú biztonsági stratégiák megjelenése, amelyek már szélesebb megközelítésben értelmezték a biztonságot. További fontos lépés volt a stratégiaalkotás kereteinek, lépéseinek és tartalmi elemeinek kidolgozása és ezek modellezése. [5] Ugyanakkor mindez csak keretet és megközelítési lehetőségeket biztosít egy ország biztonsági stratégiájának megalkotásához és tanulmányozásához, egyik modellt sem lehet teljes egészében alkalmazni minden probléma megoldására. Az előforduló hasonlóságok ellenére minden országnak és régiónak megvannak a speciális, csak az adott térségre jellemző biztonsági kihívásai, illetve a nemzetek eltérő érdekekkel, erőforrásokkal, politikai és jogi szabályozókkal rendelkeznek biztonságuk szavatolására és érdekeik védelmére.

A stratégiaalkotást és a stratégiai modelleket a biztonsági kategóriák nemzeti és a regionális szintjein alkalmazzák általában. A globális biztonság szintjére szinte lehetetlen stratégiát kidolgozni a szereplők és az ellentétes érdekek nagy száma miatt. Ugyancsak nem

alkalmazzák a stratégiai kereteket és modelleket az egyéni biztonság vizsgálatára, kidolgozására sem.

Napjainkban a megtapasztalt biztonsági kihívások (járványhelyzet, migráció, klímaváltozás stb.) következtében ismét egyre jobban előtérbe kerül az egyén biztonságának kérdése. Egyre tisztábban látszik, hogy a biztonsági kihívások megoldásában nem lehet a nemzetközi szervezetekre támaszkodni, mivel sem a hatáskörük, sem pedig a rendelkezésre álló forrásaik nem teszik lehetővé a kihívások átfogó megoldását. Az államok ugyan igyekeznek megtenni minden lehetségest, de sok esetben korlátozottak a képességeik és a lehetőségeik. Ezért fontosnak tartjuk kiemelni az egyén szerepét a saját biztonsága szavatolásában. Egyre inkább szükség lesz a biztonságtudatosság fokozására, arra, hogy az egyén felelősen és tudatosan közelítse meg a biztonság kérdését. A mai biztonsági kihívások komplexitása [6] nem teszi lehetővé, hogy az állam minden veszélyeztetett területen (közbiztonság, gazdaság, egészségügy stb.) egyformán és időben segítő kezet nyújtson minden polgárának, éppen ezért szükség van az egyén öngondoskodására.

Az egyéni biztonság elválaszthatatlan az önvédelem kérdéskörétől, ugyanakkor az idők folyamán önvédelem szóval egyfajta negatív értelmezés párosult. Az önvédelem szó egyik összetevője a „védelem", amely feltételezi, hogy támadás – általában fizikai - alatt állunk és azt akarjuk kivédeni. Ezért az önvédelmet egyfajta fizikai védekező tevékenységgel azonosítják, amely feltételezi az eszköz nélküli vagy eszközzel vívott közelharcot és a harcnak megfelelő mentális és pszichés hozzáállást. Ezen az általános értelmezésen szeretnénk változtatni, szeretnénk az önvédelmet is tágabb értelemben, komplexen megközelíteni. Véleményünk szerint az önvédelem értelmezésének is a biztonsághoz hasonlóan paradigmaváltáson kell keresztülmennie és alkalmazkodnia kell a gyorsan váltakozó és egyre komplexebb biztonsági kihívásokhoz.

Az önvédelem nem egyenlő a verekedéssel, mint ahogy egy nemzet biztonsága sem egyenlő a háborúskodással. Már az önvédelem kifejezés is valamelyest beszűkíti az amúgy nagyon is széles, sok összetevős témakört. A jog nyelve nem véletlenül inkább a „jogos védelem" kifejezést használja, ezzel is megteremtve annak a lehetőségét, hogy az „önvédelmet" ne csak magunk, hanem szükség esetén más személyek, anyagi javak, vagy társadalmi érdekek védelmére is kiterjesztve alkalmazzuk. Éppen ezért az alaptörvény V. cikke alapján az állam fel is ruházza az egyént a védekezés jogával.

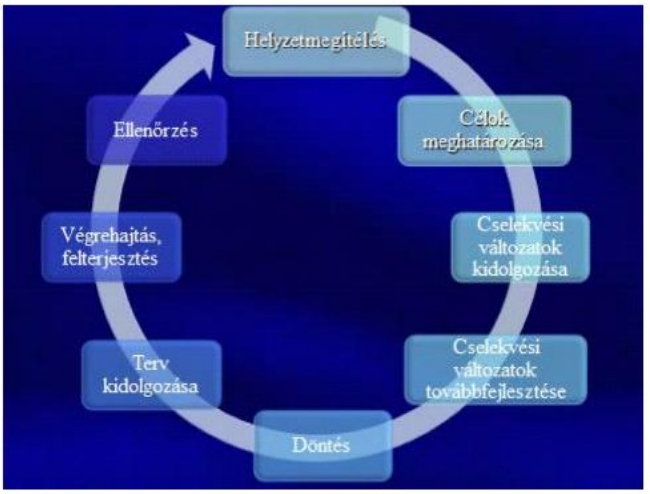
„Mindenkinek joga van törvényben meghatározottak szerint a személye, illetve a tulajdona ellen intézett vagy az ezeket közvetlenül fenyegető jogtalan támadás elhárításához." [7]

Amikor a téma átfogó megközelítéséről beszélünk, akkor az egyén biztonsága szempontjából a fizikai önvédelem csak egy pont a sok közül, és talán nem is a legelső. Fontosabbnak tartjuk az előrelátó gondolkodást, a megfontolt, magabiztos viselkedést, a jó helyzetfelismerést, a jó kommunikációt, a gyors döntéshozatalt, valamint a céltudatos cselekvést. Természetesen előnyt jelent a hatékony önvédelmi technikák magabiztos ismerete, amely önmagában is egy komplex tudomány, mert számos elméleti és gyakorlati tudásanyagot ötvöz egy működőképes egésszé. A technikák hatékony alkalmazásához szükség van pszichológiai, anatómiai, ismeretekre, végrehajtásukhoz pedig némi fizikai erőre, ügyességre, gyorsaságra és taktikai érzékre.

Az önvédelem komplex megközelítése és az előrelátó gondolkodás erősítése érdekében hasznosnak tartjuk az egyéni biztonsági stratégia kialakítását, és egy egyéni biztonsági terv átgondolását és elkészítését. Úgy gondoljuk, hogy az egyén biztonságtudatosságának kialakításához és elmélyítéséhez jó alapot biztosíthat a stratégiai modellek adaptálása az egyén biztonságának tanulmányozására és biztonsági stratégiájának kidolgozására. Megítélésünk szerint a stratégiai modellek elemei nem csak államokra, vagy szervezetekre értelmezhetőek, hanem az egyénre nézve is. A stratégiaalkotás során használt kifejezésrendszer, mint nemzeti érdekek és célkitűzések, ebben a kontextusban az egyén biztonsági érdekeit és célkitűzéseit jelentik. A veszélyeztetettség, helyzetelemzés-, és értékelés, valamint az erőforrások rendelkezésre állása nyilván más tartalmat takarnak az egyének szintjén, de teljes mértékben értelmezhető az egyén biztonsága tekintetében is. Természetesen az egyén esetében a stratégiai elemek tartalma lényegesen más lesz, mint egy állam esetében. A stratégiaalkotás logikája és eljárásrendje pedig olyan módszert jelenthet, amely fejleszti az egyén strukturált biztonságtudatos gondolkodását és lehetővé teszi a biztonságának sokoldalú és árnyalt megközelítését.

A STRATÉGIAI MODELLEK ALKALMAZÁSA AZ EGYÉNI BIZTONSÁG TERVEZÉSÉHEZ

Stratégiai tervezési folyamat modell



2. Ábra: Stratégiai tervezési folyamat (Stratégiaalkotás, stratégiai módszerek, 21.o.) [5]

A modell a tapasztalatok felhasználásával került kialakításra, és egy általános eljárásrendet javasol a tervezés végrehajtására. Az általános megközelítés lehetőséget biztosít a modell többcélú felhasználására, így lehetővé teszi nemzeti stratégiák (politikai, gazdasági, biztonsági, stb.) megalkotásához, de felhasználható az ágazati stratégiák kidolgozásához is. Természetesen a stratégiák céljától függően a stratégiaalkotás lépései különböző tartalommal rendelkeznek. Nemzeti stratégia esetén a nemzetre vonatkozó kihívások és kockázatok, valamint a nemzet erőforrásai, politikai, gazdasági, diplomáciai és katonai lehetőségei kerülnek mérlegelésre, illetve a szintnek megfelelő célok, cselekvési változatok és döntések születnek. Egy ágazati, vagy vállalati stratégia esetén az eljárásrend nem változik,

azonban a lépések tartalma az adott szintnek megfelelő lesz, az adott ágazat vagy vállalat szintjéhez igazodik.

Véleményünk szerint a modell éppen az általánossága miatt alkalmazható az egyén biztonsági stratégiájának kidolgozására is. A tervezési kör lépései adaptálhatók az egyén jelenlegi és előrelátható biztonsági helyzetének, erőforrásainak és lehetőségeinek értékelésére és az eredménynek megfelelő célkitűzések és cselekvési változatok kidolgozására. Mindezek figyelembevételével megalapozott döntés hozható az egyén biztonságának növelése érdekében. A modell alkalmas az egyén komplex biztonságának vizsgálatára (több biztonsági elem együttes figyelembevételére), valamint a biztonsági elemek önálló feldolgozására is. Javasoljuk az alábbi biztonsági elemek figyelembevételét és egyenkénti elemzését-értékelését:

- személy és családbiztonság;
- egészség védelme
- objektum és vagyonbiztonság;
- adat- és információbiztonság,
- gazdasági és egzisztenciális biztonság;
- egyéb biztonsági elemek az egyén helyzetéből adódóan.

Egy példán keresztül szeretnénk érzékeltetni a modell alkalmazhatóságát biztonság egyes területeire. A példa csak a jobb megértést szolgálja, minden esetben az egyén specifikus helyzetéhez és lehetőségeihez kell igazítani. Példának a személy és családbiztonság témakörét vettük, amely szerint [8]:

Helyzetmegítélés

Lehetséges tartalma a saját és a családtagjaink biztonságára vonatkozó alapvető kérdések megfogalmazása:

- Biztonságban vagyok a lakóhelyemen, a munkahelyemen és az általam gyakran látogatott helyeken (útvonal és terület a lakóhely és a munkahely között, vásárlás, edzés, fodrász, orvos, üzemanyagtöltő, stb.)?
- Minden lehetséges helyet és útvonalat elemezni és értékelni kell biztonsági kockázat szempontjából.
    - a lakás és a lakókörnyezet biztonsági elemzése (bűnözés helyzete, leggyakoribb bűncselekmények, erőszakos jellegű cselekmények, egyéni vagy csoportos elkövetés dominál, stb.)
    - a munkahely és környezetének biztonsági elemzése (a kollégák, ügyfelek viselkedése, jellemző-e az agresszivitás, előfordult-e fizikai erőszak, a munkahely biztonsági környezete, valószínű kockázatok stb.)
    - a lakás és a munkahely közötti útvonal biztonsági elemzése (a legbiztonságosabb útvonal nappal/éjjel, alternatív útvonalak, lehetséges közlekedési eszközök, legbiztonságosabb közlekedési mód és eszköz nappal/éjjel, valószínű biztonsági kockázatok, segítségkérési lehetőségek stb.)
    - lakás/munkahely - bevásárlás/edzés közötti útvonal és közlekedési eszközök biztonsági elemzése (a fentiek alapján)
- Saját erőforrások és lehetőségek

- a lakás és lakókörnyezet biztonsága érdekében (biztonságosabb környékre költözöm, erősítem a technikai védelmet, nem sétálok sötétedés után, lehetőleg nem egyedül közlekedek, tanulok önvédelmet, stb.)
- munkahelyen (fejlesztem a kommunikációs és konfliktuskezelési képességeimet, tartok magamnál önvédelemre is használható eszközt, segítséget kérek a biztonsági őrtől, rendőrségtől, tanulok önvédelmet),
- esti, éjszakai tömegközlekedési eszközön (körültekintően közlekedek, gyorshívón beállítom a rendőrségi segélyhívó számát, távol helyezkedek az ittas csoportoktól, a vezetőhöz közel tartózkodom, csatlakozom a hasonló irányba tartó csoporthoz, önvédelemre is használható tárgyat-eszközt tartok magamnál, szerződtetek két fő kísérőt, tanulok önvédelmet, folyamatosan edzem magam, stb.)
- a gyaloglóshoz (kerülöm a sűrű bokros, vagy elhagyatott területeket, telefonon beállítom a rendőrségi segélyhívó számát, nem viselek ékszert, feltűnő tárgyat, úgy öltözöm, hogy a ruházatom ne korlátozzon a szabad mozgásban, viszek magammal önvédelemre is használható eszközt, csatlakozom egy arra haladó csoporthoz, tanulok önvédelmet és kommunikációt, stb.)

A célok meghatározása

Fontos, hogy olyan célt tűzzek magam elé, amelyet erőforrásaim és lehetőségeim megengednek, ugyanakkor a cél elérésével növeljem a biztonságomat. Erőforrásaink figyelembevételével meghatározhatunk rövid és hosszútávú célkitűzéseket egyaránt. Például:

- Növelem a lakásom biztonságát, riasztórendszert szereltetek be. (rövid távú cél)
- Fejlesztem az önvédelmi képességeimet (fizikai, mentális, kommunikációs, stb.) (hosszabb távú cél)

Cselekvési változatok kidolgozása

Lehetőség szerint több alternatívát dolgozunk ki arra, hogy milyen módon tudom megvalósítani a célkitűzéseimet a legkönnyebben. Például:

- A riasztórendszerek tanulmányozása, szolgáltató keresése, ár-érték arány összevetése, időpont meghatározása, stb.
- Veszek egy kutyát és kiképeztetem őrzés-védelemre.
- Csak gépkocsival közlekedek, és az XX útvonalat használom a lakás és a munkahely között.
- Keresek olyan tanfolyamot, edzést, amely megfelel célkitűzéseimnek, meggyőződök a szolgáltatás színvonaláról, időrendjéről, költségéről, stb.

Döntés

- Eldöntöm, hogy milyen típusú riasztórendszert építtetek be, illetve melyik szolgáltatót választom és mennyit fordítok rá.
- Eldöntöm, hogy melyik tanfolyamot, edzést fogom látogatni és bejelentkezem.

Terv kidolgozása

Célszerű egy nagybani tervet kidolgozni, amely tartalmazza a döntések végrehajtásának időrendjét, költségeit és a végrehajtás főbb mérföldköveit. Például:

- 2021 végéig felszereltetem a riasztórendszert YY költséggel, majd üzemeltetem havi ZZ ráfordítással.
- Rendszeresen látogatom az önvédelmi edzéseket legalább egy évig, aztán konzultálok az edzővel a fejlődésről és a további lehetőségekről. Fél év elteltével lehetőség szerint plusz órákat veszek.

Ellenőrzés:

- Időszakosan szakemberrel ellenőriztetem a riasztórendszert, és konzultálok a további technikai fejlesztés lehetőségeiről.
- Negyedévente megbeszélem az edzővel az elért eredményeimet és javaslatot kérek a következő időszakra.

Bartlett modell

3. Ábra: Bartlett modell (forrás: Stratégiaalkotás, stratégiai módszerek 23.o.) [5]

Ez a modell egyszerűbbnek tűnik, mint az általános modell és kevesebb lépést tartalmaz, azonban a lényege ugyanaz, az erőforrások és a veszélyek összevetéséből határozza meg a biztonsági célkitűzéseket, amelyeket a stratégia által tervez megvalósítani.

Míg az előző modell esetében a helyzetmegítélés magában foglalta a veszélyek és a rendelkezésre álló erőforrások összevetését, addig itt két külön lépésként került feltüntetésre. Ez a kiemelés mutatja, hogy a modell kidolgozói ezt a két tényezőt és ezek részletes elemzését tartották kulcskérdésnek a megalapozott célkitűzések és a stratégia kidolgozásához.

A biztonság elérését az erők, eszközök és a veszélyek egyensúlyi helyzetének tekintették, egyszerűbben megfogalmazva, amíg van erőforrásunk a veszélyhelyzetek kezelésére addig biztonságban vagyunk. A modellben a két kívülről ható tényező (erőforrások korlátjai, biztonsági környezet) jelenti az egyensúlyi helyzet ellen ható „erőket", amelyek hatásait ki kell egyensúlyozni. A biztonsági környezet változásai megbontják az egyensúlyt, amelyet csak az erőforrások változtatásával (több erőforrás bevonásával) lehet kiegyenlíteni. Ugyanakkor a szükséges erőforrásokban beálló csökkenés következményeként a veszélyek növekednek és kezelhetetlenné válnak, amely szintén megbontja az egyensúlyi

helyzetet és ezzel a biztonságot is. Hátránynak tekinthető, hogy ez a modell inkább reagáló jellegű, mint előre tekintő, ezért nem biztosítja a biztonsági kihívások kialakulásának megelőzését, megakadályozását.

A szakirodalom ezt a tervezési módot a kevesebb erőforrással rendelkező országok stratégiai modelljének tekinti, de köztudottan az országok döntő többsége esetében az erőforrások nem állnak rendelkezésre korlátlan mértékben, ezért a biztonsági igényeket szinte sohasem lehet teljes mértékben kielégíteni. Ezért szükség van a prioritások felállítására és a kiegyensúlyozó tevékenységre.

Véleményünk szerint ez a modell is jól használható az egyén biztonsági stratégiájának kidolgozására, mivel általánosnak tekinthető az erőforrások korlátozott rendelkezésre állása és a folyamatos egyensúly keresése a fenyegetettség és a ráfordítások között. Javaslatunk szerint a biztonsági környezet elemzésének és a célkitűzések előremutató jellegének erősítésével, valamint a szükséges források biztosításával elérhető a biztonság preventív módon való fenntartása.

Saját erők, eszközök

A rendelkezésre álló erőforrások (erők, eszközök) meghatározása esetében az általános modell (2. ábra) tárgyalásánál már említett biztonsági elemeket célszerű figyelembe venni és elvégezni az alábbi főbb szempontok alapján az elemzést.

- pénzügyi,
- technikai,
- kapcsolati, együttműködési,
- egyéni képességek, tudás, tapasztalat,
- fizikai, önvédelmi,
- hivatalos és informális lehetőségek,
- stb.

Veszélyek

A veszélyek elemzése a másik alapvető feladat a biztonságunk megítélése érdekében, amelyeket szintén minden biztonsági elemre nézve végre kell hajtani az alábbi kérdések mentén:

- Mi veszélyeztetheti a biztonságomat otthon és a lakókörnyezetben?
- Milyen veszélynek vagyok kitéve a munkahelyemen és az általam gyakran látogatott helyeken (munkahely és környezete, vásárlás, edzés, fodrász, orvos, üzemanyagtöltő, stb.)?
- Milyen veszélynek vagyok kitéve a közlekedés alatt?
- (útvonalak, közlekedési eszközök a lakóhely-munkahely-gyakran látogatott helyek között)

Célkitűzések

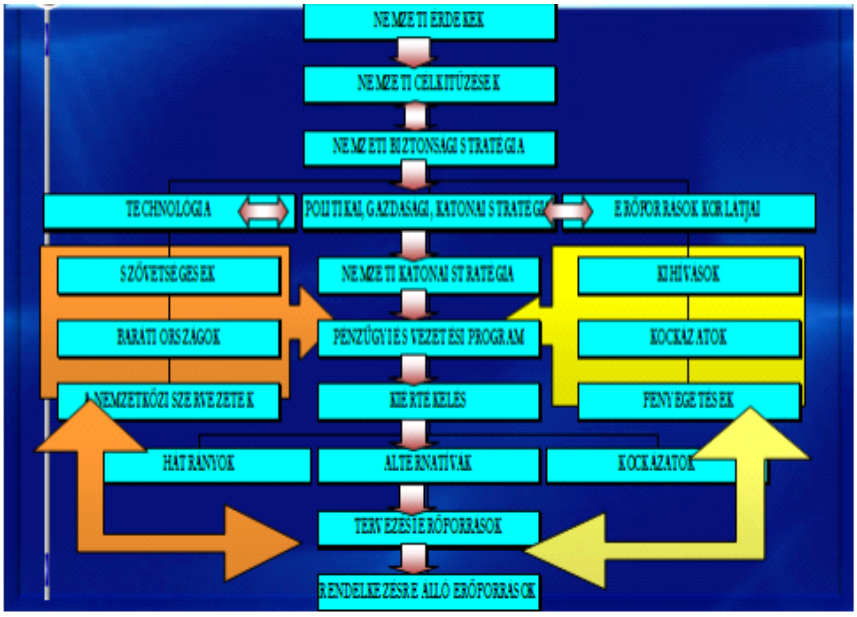
- Ebben a lépésben vetjük össze a veszélyek és a rendelkezésre álló erők, eszközök elemzésének eredményeit és kialakítjuk az erőforrásokkal alátámasztható, reális célkitűzéseinket.

Stratégia

- A stratégia megalkotásánál a célkitűzések megvalósításáról döntünk az erőforrások hozzárendelésével, valamint meghatározzuk a végrehajtás időrendjét és főbb lépéseit és az ellenőrzés, visszacsatolás rendjét.

Lloyd's modell

Az egyik legtöbb részstratégiát és befolyásoló elemet figyelembe vevő rendszer a Lloyd's modell. A modell mutatja a biztonsági stratégia kapcsolódását a nemzeti érdekek által meghatározott nemzeti célkitűzésekhez, valamint a biztonsági stratégia kidolgozásának lépéseit és mindazokat az elemeket, amelyeket figyelembe vesz a stratégia kidolgozásában. Mint minden modellnél, itt is meghatározó a veszélyek és lehetőségek elemzése, kiértékelése és alternatívák (cselekvési változatok) kidolgozása. A modell különlegessége, hogy részletesen több szintre bontva (kihívások, kockázatok, fenyegetések) elemzi a veszélyeket. Ugyancsak egyedi elem a külső lehetőségek szintekre bontott (szövetségesek, baráti országok, nemzetközi szervezetek) elemzése és figyelembe vétele a biztonsági alternatívák kidolgozásában. Természetesen itt is nagy szerepe van a rendelkezésre álló erőforrásoknak és az erőforrás korlátoknak. Tekintettel korunk technológiai fejlődésére, meghatározó szerepet kapott a technológiák elemzése és figyelembevétele a stratégiák kidolgozásánál.



4. Ábra: Lloyd's modell (forrás: Stratégiaalkotás, stratégiai módszerek 26.o.)[5]

Véleményünk szerint a veszélyek és a külső lehetőségek szintekre bontott részletes elemzése miatt ez a modell nyújthatja a legmegalapozottabb elemzést és értékelést. Ezért nem csak egyéni biztonsági stratégiák kidolgozásához javasoljuk, hanem cégeknek is célszerű lehet a módszer használata. Felépítése és részletessége miatt a modellt célszerű szakember segítségével adaptálni az egyén, vagy cég biztonsági szükségleteire. Nem véletlenül

a modell is tartalmazza a tervezési erőforrásokat, vagyis a személyi és szakmai követelményeket.

Az alábbi példában kiemeljük a modell specifikumait a szintekre bontott veszélyek és külső lehetőségek meghatározását.

Veszélyek

- Kihívások: azok a veszélyhelyzetek, amelyeknek bekövetkezése kevésbé valószínű, illetve hatásuk kevésbé súlyos a biztonságra nézve. Pl. lakásbetörés egy technikai eszközökkel biztosított lakóparkban.
- Kockázatok: azok a veszélyhelyzetek, amelyek bekövetkezése valószínű vagy jelentős hatással van a biztonságra nézve. Pl. nagy összegű készpénzt nyilvános helyen elővenni és számolni.
- Fenyegetések: azok a veszélyhelyzetek, amelyek bekövetkezésének nagy a valószínűsége és súlyosan veszélyezteti biztonságunkat. Pl. éjszaka sétát tenni egy bandaháborúkról ismert városrészben.

Külső lehetőségek

- Szövetségesek: akiket érdekazonosság miatt meg lehet nyerni akár egy, a biztonságot erősítő közös fellépéshez, akcióhoz. Pl. a ház lakóit a 7/7, 24/24 portaszolgálat bevezetésére.
- Baráti országok: rokonok, barátok, kollégák vagy sporttársak, akiknek számíthatunk a rendszeres segítségükre, együttműködésükre. Pl. a kollégám rendszeresen hazavisz kocsival az elhúzódó túlórák után.
- Nemzetközi szervezetek: egyéni stratégia esetén nem feltétlenül nemzetközi szervezetekre gondolunk, inkább hazai hivatalos és nem hivatalos szervezetekre. Pl. rendőrség, polgárőrség, magán biztonsági szolgálatok, stb.

Alternatívák (cselekvési változatok kidolgozása)

- A veszélyek és a külső lehetőségek összevetését követően kerülnek kidolgozásra az alternatívák. Alternatívák elemzése során meghatározzák a lehetséges kockázatokat és hátrányokat és ezek kapcsán módosítják vagy elvetik az alternatívákat. Prioritási sorrend kialakítása az erőforráskorlátok figyelembevételével.

Rendelkezésre álló erőforrások

- A megmaradt alternatívák összevetése történik a rendelkezésre álló erőforrásokkal a prioritási lista figyelembevételével. És ezzel gyakorlatilag megtörténik a cselekvési vázlatokhoz történő forrásallokáció, valamint kialakul a végrehajtás időrendje.

A bemutatott stratégiai modellekkel csak egy új területen történő alkalmazás lehetőségére szerettük volna felhívni a figyelmet a fenti példák alapján. Tudni kell, hogy a bemutatottakon kívül több modell is az érdeklődők rendelkezésére áll a biztonságuk tanulmányozására és növelésére. Természetesen lehetőség van a modellek kombinálására is az egyéni igényeknek és körülményeknek megfelelően. Ugyanakkor a modellek csak útmutatásul szolgálnak a biztonságtudatos gondolkodásunk kialakításához és biztonságunk fokozásához, azonban egy modellt sem lehet felhasználni minden biztonsági kérdés megoldá-

sára. Azonban bízunk abban, hogy cikkünk hozzájárul az olvasó előrelátó, komplex, biztonságtudatos szemléletének kialakulásához, egyéni biztonsági stratégiájának megalkotásához.

ÖSSZEFOGLALÁS

A biztonsági környezetünkben jelenleg lezajló folyamatok, a COVID-19 járvány, a klímaváltozás és a tömeges migráció komplex hatást gyakorolnak az államra, a társadalomra és az egyénre egyaránt. Ezt a komplex hatást az állam a legjobb akarata mellett sem tudja maradéktalanul kezelni, és minden polgárát megóvni a negatív következményektől. Ezért saját biztonsága érdekében egyre nagyobb szükség van az egyén szerepvállalására. Tudomásul kell venni, hogy az egyén is felelős saját biztonságáért, nem várhatja el, hogy a társadalom és az állam teljes körűen garantálja a biztonságát. Ennek érdekében fontosnak tartjuk az egyén biztonságtudatos gondolkodásának fejlesztését és erősítését, mint első lépést az egyén biztonsága felé vezető úton. Ha az egyén átgondolja a biztonságára jelenleg és a jövőben potenciálisan hatást gyakorló biztonsági kockázatokat és veszélyeket, valamint számba veszi a saját erőforrásai alapján lehetséges megoldásokat, már akkor sokat tett a biztonsága érdekében. Az előrelátó biztonságtudatos gondolkodás által az egyén elkerülheti a biztonsági kihívások bekövetkezését, vagy bekövetkezésük esetén felkészülten tud reagálni a veszélyhelyzet elhárítására vagy a következmények hatásainak (személyi veszteségek és anyagi károk) csökkentésére.

Fontosnak tartjuk, hogy ne csak a kihívásokat, hanem az egyén biztonságát is komplexen értelmezzük, túllépve ezzel az eddig berögződött fizikai biztonság kérdését. Le kell szögeznünk, hogy fontos a fizikai biztonság, de csak egy szeletét jelenti az egyén teljes biztonságának, különösen a mai globális, űrtechnológiát, kiberteret és digitalizációt magában foglaló és egyre inkább használó világunkban. Éppen a biztonság összetettsége miatt célszerű az egyén biztonságának strukturált megközelítése és egy logikus eljárásrend biztosítása, amely mentén a kevesebb tapasztalattal rendelkező egyén is képes átgondolni a biztonságára ható kérdéseket és felépíteni a biztonságát erősítő eszköz és eljárásrendszerét.

Az előrelátó biztonságtudatos gondolkodás fejlesztéséhez a biztonságpolitikában már bevált stratégiai modellek adaptálásával szeretnénk hozzájárulni. Véleményünk szerint a stratégiai modellek jól használhatók az egyén biztonságának strukturált megközelítésére, tanulmányozására és az egyén vagy vállalat biztonsági stratégiájának kidolgozására. Megítélésünk szerint a stratégiai modellek elemei nem csak államokra, vagy szervezetekre értelmezhetőek, hanem az egyénre nézve is. A stratégiaalkotás során használt kifejezésrendszer, mint nemzeti érdekek és célkitűzések ebben a kontextusban az egyén biztonsági érdekeit és célkitűzéseivel azonosíthatóak. A veszélyeztetettség, helyzetelemzés-, és értékelés, valamint az erőforrások rendelkezésre állása más tartalommal bírnak az egyének szintjén, mint az államok és szervezetek szintjén, de teljes mértékben értelmezhető az egyén biztonsága tekintetében is. A stratégiaalkotás logikája és eljárásrendje pedig olyan módszert nyújthat, amely fejleszti az egyén strukturált biztonságtudatos gondolkodását és lehetővé teszi a biztonságának sokoldalú és árnyalt megközelítését. Mindezek alapján széles körben ajánljuk a stratégiai modellek adaptált felhasználását az egyéni biztonság tudatos növelésére.

FELHASZNÁLT IRODALOM

[1] Lenhoffer Péter-Nagy László, „A 2001. szeptember 11-ei terrortámadás hatása az Amerikai Egyesült Államok Nemzetiztonsági rendszerére," *Honvédségi Szemle,* 148. évf. 2020/5 szám, Budapest, 2020.

[2] Wikipédia, „Maslow Piramis", https://hu.wikipedia.org/wiki/Maslow-piramis, [Hozzáférés dátuma: 2021.09.10.].

[3] Dr. Vida Csaba, „A biztonság és a biztonságpolitika katonai elemei," *Nemzetbiztonsági Szemle,* MMXIII/I évf. I szám, 91-92.o., 2009.

[4] Péczeli Anna, „A humán biztonság elmélete és gyakorlata, Kanada és Japán példáján" http://www.grotius.hu/doc/pub/ESLRKT/2011_243_peczeli_anna_a_human-biztonsag_elmelete_es-gyakorlata.pdf, [Hozzáférés dátuma: 2021.09.05.].

[5] Turi Laura Tamara - Dr. Resperger István - Dr. Túri Viktória, Stratégiaalkotás, stratégiai módszerek, Nemzeti Közszolgálati Egyetem, Budapest, 2012, 21-26.o.

[6] Szakali Miklós és Dr. Szűcs Endre, „Lehetőség a komplex biztonsági kihívások kezelésére," *Biztonságtudományi Szemle.,* III. évf. 2. szám (16.o.), Budapest 2021.

[7] *Magyarország Alaptörvénye,* Budapest, 2011., V cikk.

[8] Kovács Ildikó, „Előzd meg a tragédiát - 7+1 tipp a biztonságos futáshoz," https://www.noionvedelem.hu/blog/tippek-a-biztonsagos-futashoz/.[Hozzáférés dátuma: 2021.10.02.]

THE IMPACT OF QUANTUM COMPUTING ON IT SECURITY

A KVANUTMSZÁMÍTÁSTECHNIKA HATÁSA AZ INFORMATIKAI BIZTONSÁGRA

NYÁRI Norbert[1]

Abstract

Cryptography, that is the science of encryption is one of the important sub-areas of IT security, that of logical security in particular. Achieving quantum supremacy, quantum computing becoming mainstream, poses a growing threat overtime to the security of currently prevalent cryptographic algorithms.

This paper discussing quantum computing also examines what quantum dominance means and why this new technology is dangerous to the security of today's electronic information systems.

It then introduces the quantum cryptographic and quantum communication solutions currently available, and presents post-quantum cryptographic efforts around the world, including the latest studies of the US National Institution of Standards and Technology (NIST), the EU-European Union Agency for Cybersecurity (ENISA), and the NATO as well.

Keywords

IT security, cryptography, quantum computing, post quantum cryptography

Absztrakt

Az informatikai biztonság, azon belül is a logikai védelem egyik fontos részterülete a kriptográfia, vagyis a rejtjelezés tudománya. A kvantumfölény elérése, a kvantumszámítástechnika mainstream-mé válása egy olyan veszélyt jelent az aktuálisan elterjedt rejtjelező algoritmusok biztonságára, melynek bekövetkezési valószínűsége az idő előrehaladtával egyre nagyobb.

Jelen cikk a kvantumszámítástechnika tárgyalása során kitér arra is, hogy mit jelent a kvantumfölény, és miért veszélyes ez az új technológia a mai elektronikus információs rendszerek biztonságára.

Ezt követően sorra veszi a jelenleg elérhető kvantumkriptográfiai és kvantum kommunikációs megoldásokat, majd bemutatja a posztkvantum kriptográfiai törekvéseket szerte a világból kitérve az USA National Institution of Standards and Technology (NIST), az EU European Union Agency for Cybersecurity (ENISA), továbbá a NATO legfrissebb tanulmányaira is.

Kulcsszavak

informatikai biztonság, kriptográfia, kvantum számítástechnika, posztkvantum kriptográfia

[1] nyari.norbert@uni-obuda.hu | ORCID: 0000-0003-0229-7584 | doctoral candidate, Óbuda University Doctoral School on Safety and Security Sciences | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

Cybersecurity is a key factor in modern life, because either the bodies of public administration or private firms are highly bound to the electronic information systems. Such systems are considerably exposed to cyberspace threats. Information being a high-valued asset nowadays needs to be adequately protected. The goal of IT security can be summarized in the CIA principle, that is a secure electronic information system guarantees the Confidentiality, Integrity and Accessibility of the managed information. This is done through several layers of security, one of them is logical security.

Cybersecurity often relies on cryptography besides other subfields. Fundamentally cryptography aims to ensure the confidentiality, the integrity of data, the authentication of either entities or data origin, and finally the non-repudiation. So, practically speaking cryptography helps implementing the C and I from the well-known CIA principle. [1]

The term *cryptography* stems from the ancient Greek word kryptós, which means secret or hidden, and graphein meaning "to write". [2] It is the science of information concealing methods, used in secure communication allowing the sender and the original recipient to exchange messages while outsiders being unable to get know of the contents of the messages. The contents of these messages, the information to be communicated is called *plaintext*, the encrypted message is referred with the term *ciphertext*, and we call *cipher* any method of transforming a message to conceal its meaning. The *key* is a parameter of the cipher, it must be kept secret, in some cases it is shared between the parties involved in the communication. There are usually other parameters than the key e.g., initialization vector, salt etc. that are not required to understand the article and are therefore not discussed in detail. [2]

Kerckhoff formulated basic expectations for cryptographic systems in the 19th century, some of which are still valid today. *Kerckhoffs's principles* which state that even fully disclosing everything (except the key of course) about a cryptosystem to the public should not compromise its security. Such systems are considered sufficiently safe even if it is not possible to break them by practical methods, theoretical unbreakability is not a prerequisite according to Kerckhoffs's principles. [2] [1]

Built from well-defined *cryptographic primitives* as basic building blocks a cryptographic system (or *cryptosystem*) is providing information security services. The designer of such systems not necessarily has to be competent in the mathematical and practical considerations involved in cryptographic primitives. [1] Hereinafter I shall examine the algorithms with this level of detail.

Commonly used cryptographic primitives are following Kerckhoffs's principles regarding unbreakability, since they are based on mathematical problems with such computational difficulties that solving them is not feasible with regular computers. Practically speaking breaking them is hard enough not to worth the effort for most of the attackers (they are lacking money, computational capacity etc.). [2] Note Kerckhoffs's principles mentioned above.

There are several primitives, I shall cover the following types in the current article: *symmetric-key cryptography* (SKC), *Public-key cryptography* (PKC), *Cryptographic Hash Functions* (CHF), *Digital Signature* and Cryptographically Secure Pseudorandom Number

Generator (CSPRNG). Other primitives such as Mix Networks, Private Information Retrieval, Commitment Scheme are related to hard-to-trace communications and ensuring anonymity, which goes beyond the scope of this publication. [1]

Regarding to Alfred Menezes cryptosystems can be classified into five main categories regarding security: "Unconditionally security, Complexity-theoretic security, Provable security, Computational security and Ad hoc security". *Unconditionally secure* systems withstand attacks from adversaries even with unlimited computational resources, this is often called Perfect security. [1]

Complexity-theoretic security is based on a gap between efficient algorithms guaranteed for the rightful users and the computational infeasibility of breaking the cryptosystem for an attacker. [3] In this scheme attackers are modeled as having the same, feasible computational resources as rightful users. [1]

A cryptosystem is said to be *computational secure* when breaking it needs a level of computation power which exceeds the resources of an assumed attacker. *Provable security* is a subclass of Computational security, breaking such system is "as difficult as solving a well-known mathematical problem". [1] Provable security systems include the commonly used PKC algorithm RSA (Rivest, Shamir, Adleman), which I shall discuss later on.

Finally, *Ad hoc security* means the cryptosystem is safe against the attack of a known adversary with fixed resources. [1]

One more topic needs to be highlighted before I get into the details: *Quantum technology*, which is a still emerging discipline including essentially everything based on quantum mechanics. Stemming from physics and engineering quantum technology relies on the principles of quantum physics, including quantum entanglement and quantum superposition. It has many subareas including, but not limited to *quantum computing*, *quantum communications* and *quantum cryptography*. [4]

In the following I shall introduce the basic concepts of quantum computing. I then discuss cryptographic primitives considering their quantum computing threats. Finally, I review the recent NIST, ENISA and NATO studies in the topic.

QUANTUM COMPUTING

The basic unit of information in *quantum computing* is called *qubit* (or quantum bit) Qubits are defined as two-level quantum systems. The basic difference to classical computing however is that qubits can also be at any of the infinitely many intermediate levels or states between 0 and 1, unlike classical bits. [4] Theoretical *quantum computers* make it possible to use the quantum properties of qubits in order to perform quantum computations, and run quantum algorithms, allowing to perform certain operations in a completely different, and importantly, much more efficient way. [4]

Quantum supremacy or (*quantum advantage*) is an important concept. Harrow and Montanaro defines it as "when a universal quantum computer performs a computational task that is beyond the capability of any classical computer, an event known as quantum supremacy". [5] Chris Bernhardt states that the existence of a universal quantum computer with at least 72 qubits would mean quantum supremacy. [6]

There is a keyword in both above definitions that can be easily overlooked when it comes to publication of quantum computation related results: "*universal*". Articles about

quantum supremacy so far are demonstrations that a concrete, programmable quantum device is capable of solving a problem with quantum algorithm, a problem which cannot be solved in feasible time with regular computers. However, this says nothing about the usefulness of the problem solved with quantum computers, yet it is important because it generates competition among IT companies that promotes technical development. I shall present examples later.

In my humble opinion a new term should be introduced cases where quantum supremacy is specific for a computational task, or it is achieved on an experimental, computation specific, that is not universal hardware. I would suggest that *quantum supremacy* should stay the way Harrow and Montaro defined it (see above), but *quantum advantage* should not be the synonym for quantum supremacy and should mean cases where the "universal" restriction would not hold.

According to ETSI White Paper No. 8 'Quantum Safe Cryptography and Security' some cryptographic algorithms are "*known to be vulnerable"* to quantum attacks and some others are "*thought to be safe"* from such attacks, that is quantum safe. Should a cryptographic primitive be well examined and proves to be resistant against known types of quantum attacks, it is regarded as quantum safe. [7]

In my understanding quantum computing poses no direct threat to cryptography at the moment because real-life quantum computers lacking the processing power for breaking cryptographic systems. Notwithstanding, cryptographers are working on finding quantum safe ways of cryptography in order to prepare for the so-called quantum apocalypse, the time of the real quantum supremacy. In my humble opinion this preparation is vital, for this new technology will fundamentally change the field of cryptography eventually breaking most of current cryptography techniques used.

SYMMETRIC-KEY CRYPTOGRAPHY

Firstly, *symmetric-key cryptography* (SKC) consists of algorithms that use the *same key* for encrypting and decrypting messages. Using the same key on both ends (encryption and decryption) is a downside, because in some *cases key distribution can be challenging*. there are two large families of algorithms in SKC: stream ciphers and block ciphers. Stream ciphers encrypt handling the message as a stream of bytes or letters (typically bytes), encrypting one byte at a time. Block ciphers take several bits and encrypt them as a single block, the length of the plain text must be a multiple of the block size, so it is padded if necessary. Commonly used SKC algorithms are AES, Twofish, Blowfish, RC4, IDEA etc. [2]

It is vital for optimal security that the used *symmetric key* has been generated using a *statistically good quality random numbers* utilizing real random generator or at least cryptographically safe pseudo random number generator (CSPRNG). [1]

However, it is worth highlighting the *OTP symmetric key algorithm* because it provides *unconditional security*. It has downsides unfortunately. In this case the length of the key must be at least equal to the length of the message. This makes key distribution even harder. [2] Let us consider a message which is 4 GB, in this case the key must be 4 GB as well, and it must be available to both ends while kept secret. There are a few restrictions though, which must be met in order to ensure the security OTP encryption, one that *it is forbidden to reuse the key*. [2]

In my understanding, OTP cannot be attacked any more efficient with quantum computers given that it is utilized properly (no repeating of keys), because *the only way to attack it is through brute force*, that is trying all the possible keys for a ciphertext. Even if the brute forcing process speeded up, the attacker would not be able to choose the original message, because brute forcing an OTP encrypted message of length n will result in the list of all the n-length possible cleartexts.

SKC algorithms can be attacked in many ways including but not limited to known-plaintext attack. The known-plaintext attack (KPA) is a cryptanalytic attack model based on the assumption that the attacker has managed to get hold of a few pairs of plaintext and its associated ciphertext. [1]

I highlight this type of attack, because in 1996 Grover presented a *quantum searching algorithm which gives a quadratic speed up to KPA attacks* against SKC algorithms, notwithstanding AES-256 is still considered quantum-safe. [8] [9]. The SKC is considered quantum secure provided that the key size is large enough, as a rule of thumb the keysize should be doubled. [8]

CRYPTOGRAPHIC HASH FUNCTIONS

Cryptographic Hash Functions are mathematical algorithms maps a *fixed length message digest* or hash to data or message of arbitrary size. There are a few restrictions though. The computation of the message *digest must be relatively quickly done*. The function must be deterministic that is, the same input must result in the same hash value. Generating a message that results in a certain hash value must be infeasible. Finding two different messages with the same message digest (*collision*) should also be *infeasible*. Even a one-bit change in the original message changes the output hash value to such an extent that the new hash value conspicuously does not correlate with the old hash value. [2] [1]

Collision is inevitable though because of the arbitrary length and number of the input and the fixed number of the output values, stemming from the fixed message digest length. [1]

Hash functions can be keyed or unkeyed. Unkeyed functions are mainly used for modification detection (MDCs), see digital signature below and keyed ones are primarily for message authentication (MACs). [1]

In the 2020 article ‘Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories’ authors state that “The first dedicated quantum attack on hash functions was presented at EUROCRYPT 2020 by Hosoyamada and Sasaki” This attack can be performed against a specific hash algorithm AES-MMO. [10] Hosoyamada and Sasaki showed that *classically secure hash functions are potential subjects to attacks from quantum computers*. [11]

In my understanding these proposed *quantum attacks shorten the time needed* to find collisions, so increasing the *length of the message digest will strengthen hash algorithms* against quantum attacks.

PUBLIC-KEY CRYPTOGRAPHY

The third category is *Public-Key Cryptography* (PKC), which is based on the usage of keypairs. A keypair consist of *a private key and a public key*. While the public key can

be securely disclosed to anyone, the private key must be kept secret. [2] Public-key cryptography is there basically many aspects in modern life such as communication between computers on networks, securing payments with credit cards etc. [2]

The PKC can be used for message encryption. In this case, the public key is used to encrypt a message for the holder of the private key. Such message can be decrypted only with the private key. In this scheme, communicating parties exchange their public keys and use them respectively. Unfortunately, *public-key encryption is much slower than symmetric-key encryption*. [2] According to Alfred Menezes "The security of many public-key cryptosystems *relies on* the apparent intractability of *computational problems"*. [1] Invented in 1978, the *RSA* algorithm is a prominent example of PKC relying heavily on either *prime factorization* or the algebraic structure of *elliptic curves*. [1]

Digital signature, the other application of PKC is much more common utilizing the *DSA* algorithm rooted in the *discrete logarithm* problem. [1]. In this scenario the holder of the private key encrypts a hash of a document and attaches the message digest to the document. Anyone who has the public key can verify if the document was signed by the holder of the private key. [2]

PKC algorithms are *computationally secure*, their security is based on the difficulty of mathematical computations like computing the factors of large integer numbers. There is no known algorithm for solving such calculation in feasible time running on regular computers. The calculation grows much more difficult (for regular computers) increasing the size of the prime factors, practically speaking increasing the key size. [2]

Mathematical problems like the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem *cannot be handled with regular computers in feasible time*, but all of them can be *easily solved with Shor's algorithm* running on a large-scale quantum computer. [12] [13]

Shor's algorithm *has been implemented* since its discovery in 1994, with the number 15 being successfully factorized in 2001 by a group at IBM with an experimental 7-qubit quantum computer. [14] In 2012 the number 21 was factorized. [15] [6]

This also shows that quantum computing is *not a direct threat* at the moment but quantum computers *breaking RSA* seems to be *a question of time*. [6]

KEY EXCHANGE AND KEY DISTRIBUTION

Key exchange or Key Establishment methods are designed to solve the previously mentioned key-distribution problem. To establish a secure communication between two parties a few things must be done in advance. They must be *agreed on a cryptographic algorithm* SKC or PKC. Using SKC both parties must have the symmetric key. In case of PKC, they must exchange their public keys. This process is known as the key exchange.

In case of PKC, the key distribution is rather simple, because as it was stated before, public keys can be safely disclosed to anyone, without the risk of compromising the secure communication. The identification of the holder of the keypair is a remaining problem though. [2]

The so-called *Public Key Infrastructure* (PKI) is aimed to solve the problem of the identification of the users utilizing *Certificate Authorities* (CA) and *Regional Authorities* (RA). A certificate is created in "chain of trust" or a "certification path". The chain of trust means that every issued certificate is signed by the level above. The chain basically consists

of the root certificate, the one or more RA certificates below that, and the CA certificates on the lowest level. The root certificate is the exception regarding the signature, because it has no level above it, so it must be a self-signed certificate. [2] Practically speaking the certificate holder's identity is certified by an authority through a digital signature.

A *digital certificate* (or PKI certificate) has many usages, firstly, it is used to identify users, servers or other entities when communicating over public or untrusted networks, furthermore, to sign electronic documents or computer programs and eventually to encrypt data or communication. [2] Practically speaking the certificate proves the ownership of the public key, by storing it together in a PKI with information about the owner. The *certificate is signed digitally by the issuing CA* and the signature is attached in the certificate. [2] The X.509 standard defines the most common format for public key certificates. [2]

Currently PKI is heavily relying on PKC so it will be a main subject to large-scale quantum computer attacks in the future.

Published in 1976 the *Diffie-Hellman Key Exchange* cryptographic protocol enables communicating parties to securely *exchange secret keys* on a *public channel* even if an attacker is monitoring it. The solution of Whitfield Diffie and Martin E. Hellman is one of the first public key systems known. [2] [16] It uses prime numbers raised to determined powers to establish keys. Computing the key for an attacker from the captured network data is mathematically overwhelming, even if everything on the public channel is monitored, that is the algorithm is computationally secure. [2] [17]

Both the Diffie-Hellman Key Exchange and PKC are based on *compute-intensive* mathematical problems *significantly exceeding* the computing power of *today's computers* from an attacker perspective, including the difficulty of factoring large numbers, exponentiation, and modular arithmetic. [2] [17] As stated above these problems are easily solvable with a sufficiently powerful quantum computer. So Diffie-Hellman key exchange is neither quantum safe.

There is however a post-quantum cryptographic algorithm called *Supersingular isogeny Diffie–Hellman key exchange (SIDH)* which can be a replacement for Diffie-Hellman key exchange in the future. [18]

CRYPTOSYSTEMS

As stated, in the Introduction, *cryptosystems* are designed and *constructed using cryptographic primitives*. The overall security depends on the primitives used and the proper usage of them. [1] Needless to say, such systems are exposed to quantum attacks to the extent that their individual components.

A prominent and widely used example of cryptosystems is *Transport Layer Security (TLS)*, formerly Secure Sockets Layer (SSL), it is commonly used on TCP/IP networks to ensure privacy and data integrity in client-server communication. The latest version is TLS 1.3 effective since August 2018, it is described in detail in the RFC8446 standard. [19] The best-known form is HTTPS protocol for access websites on the Internet. [2]

Before the *creating the secure* communication *channel*, the client and server must *agree on using TLS* for the session, they establish a stateful connection by using the so-called handshake procedure utilizing *a public-key algorithm to set up various parameters* for the later used symmetric-key cipher and a *shared secret key* specific for the current

session. After that *all additional network traffic* is encrypted using a *symmetric key algorithm*. Basically RSA, digital certificates and Diffie-Hellman key exchange is used for this handshake, but the standard allows other algorithms as well. [19]

Previously stated that RSA, and Diffie-Hellman are not quantum safe, so should quantum computers with high computational performance appear, there will be a serious issue around the world given that the phenomenon hits the industry unprepared.

POST-QUANTUM CRYPTOGRAPHY AND QUANTUM CRYPTOGRAPHY

The *still emerging* quantum technology holds many opportunities regarding *communication* and *cryptography*. *Post-quantum cryptography* (or quantum-safe) refers to cryptographic algorithms that are "*thought to be secure"* (that is not proven to be vulnerable) against a cryptanalytic attack by a *quantum computer*. [7] I would like to stress that the goal is not necessarily to implement cryptographic algorithms using quantum technology, but to find new ways of concealing information, whether using quantum computing or not, that can withstand even quantum attacks in the future. [6]

As previously stated, post-quantum cryptography means cryptographic primitives which can withstand attacks from large-scale quantum computers. Quantum-safe is often used as a synonym for post-quantum cryptography. Quantum cryptography means cryptographic primitives based on quantum technology. I think that the following nomenclature would describe the situation more precisely: *Post-Quantum Cryptography* should be a generic term, including all solutions that can withstand quantum attacks (quantum based or not), *quantum-safe* (or quantum-proof, quantum-resistant) should not be a synonym for quantum cryptography but mean the regular computing algorithms which can withstand quantum attacks and finally quantum cryptography meaning cryptographic primitives based on quantum technology.

Quantum Key Distribution (QKD) is currently the best known and most widely used application of quantum cryptography. According to Alfred Menezes, *Unconditional security* (provable) can be achieved against attackers based on the laws of quantum physics "provided the parties have access to (aside from the quantum channel) a conventional channel subject to only passive adversaries" [1] [20]

QKD is the process of *a key establishment* using quantum communication, that is creating a *random key* on a quantum communications channel. The channel could be fiber optics or free space. After the key establishment done with quantum communication, the key can be used for SKC algorithms e.g., OTP. There are two QKD protocols BB84 (1984) and E91 (1991). On practical level has a few setbacks though, the range of communication is limited. So far the best result on fiber optics was 12 km in December 2020 by the Indian Defence Research and Development Organization and 300 meters in free space, in March 2021, by the Indian Space Research Organization. [6] [20] [21]

QKD has *commercial implementations* as well, six companies offer QKD systems worldwide, including the Swiss company, *ID Quantique*. In 2004 the first bank transfer was carried out with QKD in Vienna, Austria, in 2007 Swiss ballot results were transmitted to the capital with QKD. [20] [21]

Regarding to the article 'The European Quantum Communication Infrastructure (EuroQCI) Initiative' "Since June 2019 all 27 EU member states signed the European Quantum Communication Infrastructure (*EuroQCI*) Declaration, signalling their commitment to

the EuroQCI initiative". The EuroQCI project aims to create a quantum communication infrastructure based on QKD *across Europe* and to facilitate quantum technology development. In parallel, member states are working on designing and implementing national quantum communication networks. [22] As for Hungary, the Quantum Information National Laboratory Hungary aims to build the Hungarian regional quantum network in order to connect to the European quantum internet. [23]

According to the current state of science, the so-called quantum apocalypse does not seriously affect symmetric cryptographic primitives. Increasing the key sizes (at least double them) however will certainly be necessary in time. [8] [13]

Today's dynamically evolving quantum computers, which still exist as *special-purpose hardware*, do not have the computational capacity yet to break real-life cryptographic algorithms. There are however several *efforts worldwide* that aim to deal with the problem of PKC not being quantum safe.

NIST (US National Institution of Standards and Technology) has a program named *Post-Quantum Cryptography Standardization* aiming to find *replacements* for current public-key algorithms, since they shall be potential subjects to quantum attacks in the not-too-distant future. As a first step, NIST, with the involvement of the cryptographic community, has begun to develop a minimum set of acceptance and evaluation criteria for the potential candidates. The submission period for post-quantum candidate algorithms ended in November 2017. The process has been through two rounds already. [24]

Round 3 candidates for standardization were announced on 22nd July 2020 with 7 finalists and 8 alternatives. According to Dustin Moody, a member of NIST PQC team, *finalists* are the "most promising algorithms we expect to be ready for standardization at the end of the 3rd round" and *alternates* are "candidates for potential standardization, most likely after another (4th) round". [25] The candidates include 4 algorithms for PKC and Key-establishment Algorithms (with 5 alternatives) and 3 algorithms for Digital Signature Algorithms (with 3 alternatives). [26] A *virtual conference* was held June 7th-9th, 2021 where each submission team had the opportunity to give updates on their submitted algorithm. [27] The release of *draft standards* and call for public comments is *expected in 2022-2023*. [25]

ETSI (European Telecommunications Standards Institute) has a working group called "*ETSI Quantum-Safe Cryptography (QSC) working group"* aiming to "assess and make recommendations for quantum-safe cryptographic primitives, protocols, and implementation considerations". In August 2020 ETSI released *TR 103 619* defining *migration strategies and recommendations "*for Quantum-Safe schemes and enhancing cryptography awareness". [28]

In September 2021 ETSI supported the NIST Post-Quantum Cryptography Standardization program with *two technical reports* regarding *quantum-safe PKC*, and *quantum-safe digital signature* (ETSI TR 103 616 V1.1.1 (2021-09) "Quantum-Safe Signatures" and ETSI TR 103 823 V1.1.1 (2021-09) "Quantum-Safe Public Key Encryption and Key Encapsulation"). [29]

ISO/IEC also has a *working group* on quantum computing so as to get demands or requirements for quantum computing and establish a unified understanding of the *terminology and vocabulary* for this emerging technology. [30] [31]

In May 2021 *ENISA* (European Union Agency for Cybersecurity) published a freely available *study on the current situation* on the Post-Quantum Cryptography standardization process. [32] In the Chapter six, *Quantum Mitigation* the study offers *two proposals* that can be implemented against quantum capable adversaries. The first one is a *hybrid approach* of pre- and post-quantum cryptographic schemes, the other one suggests the *use of pre-shared keys* into all key establishment via PKC. [32]

NATO is working on two post-quantum projects under the "Science for Peace and Security (SPS) Programme" in the field of *secure communication*. "NATO partner country Malta aims to establish and implement post-quantum cryptographic solutions and protocols", with experts from the University of Malta and universities of many other partner countries including the USA, Slovakia and Spain. [33]

The aim of the other NATO project is to create an underwater *quantum communication channel* between Italy and Malta utilizing already existing optical fibers, creating the basic infrastructure for *quantum communication* between the two countries with a portable quantum station in both countries. The project also contributes to the protection of *critical infrastructures* in Malta. [33]

As for *quantum supremacy*, in 2019, a group of researchers at Google published a paper stating that they created a quantum processor that carried out a *specific calculation* in 200 seconds. The same calculation would take 10,000 years with even the best regular supercomputer. Also stating "This dramatic increase in speed compared to all known classical algorithms is an experimental realization of *quantum supremacy for this specific computational task*" [34] This is great news, it surely facilitates further research, but it is unfortunately not the quantum supremacy we wait for. In the previously suggested nomenclature, I would call this *quantum advantage*.

In 2020, a Chinese group of researchers *at University of Science and Technology of China (USTC)* also claimed to reach *quantum supremacy*. Their paper states that their quantum computer generated the certain number of samples in 20 seconds, that would take 600 million years for a classical supercomputer. [35] This is *quantum advantage* as well.

Led by the Chinese quantum physicist Pan Jianwei, *USTC* research team designed quantum computing system, called "Zuchongzhi 2.1" in October 2021, the first time for China to reach quantum supremacy in superconducting quantum computing. The *66-qubit* programmable quantum computer is stated to have a "calculation complexity more than 1 million times higher than Google's Sycamore processor". The other quantum computer prototype, "Jiuzhang 2.0", is light-based and it "can implement large-scale Gaussian boson sampling (GBS) 1 septillion times faster than the world's fastest existing supercomputer". [36] This is a great progress as well, but it proves *quantum advantage* (instead of quantum supremacy), because "Jiuzhang 2.0" is a special-purpose hardware.

In October 2021, Amazon Web Services (AWS) opened a new quantum computing facility ("AWS Center for Quantum Computing") in California. The facility, with the aim of developing and building the company's own large-scale superconducting quantum computer, has been built in cooperation with the California Institute of Technology (Caltech). The new center's team shall consist of experts from academic institutions and from Amazon supplemented by Caltech researchers. [37]

SUMMARY

As I wrote earlier, I think *some concepts need to be refined* on the subject, and these clarified terms should be used consequently, like quantum supremacy, post-quantum cryptography etc. The *ISO/IEC AWI 4879* standard on Quantum Computing Terminology and Vocabulary may make this change. [31]

Although quantum computing means *no direct threat to cryptography yet*, I think it is vital to *find post-quantum alternatives* for quantum-endangered cryptographic primitives. All efforts from standardization institutes, research groups are highly welcomed. Unfortunately, it is *not possible to estimate* when we can expect a *breakthrough* in quantum computing, but the world *must be prepared* to replace current PKC solutions when this breakthrough occurs, considering that many systems worldwide depend on digital signatures and public-key cryptography.

RESOURCES USED

[1] A. J. Menezes, Handbook of applied cryptography, CRC Press, 1996.

[2] A. S. Tannenbaum, Computer Networks, New Jersey: Pearson Education, 2003.

[3] S. Neukamm, "Complexity Theoretic Cryptography," 2005.

[4] M. A. López, Quantum Technologies - Digital transformation, social impact, and cross-sector disruption, Inter-American Development Bank (IDB), 2019.

[5] Harrow, Aram W.; Montanaro, Ashley, "Quantum computational supremacy," Nature, vol. 549, no. 7671, pp. 203-209, 2017.

[6] C. Bernhardt, Quantum Computing for Everyone, Cambridge, Massachusetts U.S.A.: MIT Press, 2019.

[7] ETSI, Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges, ETSI, 2015.

[8] D. J. Bernstein, "Grover vs. McEliece," Sendrier N. (eds) Post-Quantum Cryptography. PQCrypto 2010. Lecture Notes in Computer Science, vol. 6061, 2010.

[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on the, Philadelphia, Association for Computer Machinery, 1996, pp. 212-219.

[10] Xiaoyang Dong et al., "Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories," Cryptology ePrint Archive, Report 2020/1030, 2020.

[11] Akinori Hosoyamada and Yu Sasaki, "Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound," Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniquess, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II, pp. 249-279, 2020.

[12] W. P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, 1997.

[13] D. J. Bernstein, "Introduction to post-quantum cryptography," in Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography, Berlin, Springer, 2009.

[14] Vandersypen, Lieven M. K.; Steffen, Matthias; Breyta, Gregory; Yannoni, Costantino S.; Sherwood, Mark H. & Chuang, Isaac L., "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," NATURE, vol. 414, no. 20, pp. 883-887, 2001.

[15] Martín-López, Enrique; Martín-López, Enrique; Laing, Anthony; Lawson, Thomas; Alvarez, Roberto; Zhou, Xiao-Qi; O'Brien, Jeremy L., "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," Nature Photonics, vol. 6, no. 11, pp. 773-776, 2012.

[16] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, p. 644–654., 1976.

[17] A. Anastasios, "How is Diffie-Hellman Key Exchange Different than RSA?," 14 07 2020. [Online]. Available: https://www.venafi.com/blog/how-diffie-hellman-key-exchange-different-rsa. [Accessed 17 10 2021].

[18] Wikipedia, "Supersingular isogeny key exchange," 08 04 2021. [Online]. Available: https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange. [Accessed 24 10 2021].

[19] RFC, "The Transport Layer Security (TLS) Protocol Version 1.3," 08 2018. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8446. [Accessed 20 10 2021].

[20] Wikipedia, "Quantum cryptography," 01 10 2021. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_cryptography#Quantum_cryptography_beyond_key_distribution. [Accessed 24 10 2021].

[21] Wikipedia, "Quantum key distribution," 13 10 2021. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_key_distribution. [Accessed 24 10 2021].

[22] European Comission, "The European Quantum Communication Infrastructure (EuroQCI) Initiative," 21 10 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci. [Accessed 31 10 2021].

[23] Quantum Information National Laboratory Hungary, "Realization of a Quantum Communication Network," [Online]. Available: https://qi.nemzetilabor.hu/research-fields/realization-quantum-communication-network. [Accessed 31 10 2021].

[24] NIST, "Post-Quantum Cryptography Standardization," 03 01 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization. [Accessed 20 10 2021].

[25] D. Moody, "NIST Status Update on the 3rd Round," [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf. [Accessed 24 10 2021].

[26] NIST, "Post-Quantum Cryptography - Round 3 Submissions," 03 01 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions. [Accessed 20 10 2021].

[27] NIST, "Third PQC Standardization Conference," 10 02 2021. [Online]. Available: https://csrc.nist.gov/events/2021/third-pqc-standardization-conference. [Accessed 24 10 2021].

[28] ETSI, "Quantum-Safe Cryptography (QSC)," [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Accessed 24 10 2021].

[29] ETSI, "ETSI RELEASES TWO TECHNICAL REPORTS TO SUPPORT US NIST STANDARDS FOR POST-QUANTUM CRYPTOGRAPHY," 06 10 2021. [Online]. Available: https://www.etsi.org/newsroom/news/1981-2021-10-etsi-releases-two-technical-reports-to-support-us-nist-standards-for-post-quantum-cryptography. [Accessed 24 10 2021].

[30] IEC, "Quantum computing: the latest frontier for international standards," 03 08 2020. [Online]. Available: https://www.iec.ch/blog/quantum-computing-latest-frontier-international-standards. [Accessed 24 10 2021].

[31] ISO/IEC AWI, "ISO/IEC AWI 4879 - Information technology — Quantum computing — Terminology and vocabulary," [Online]. Available: https://www.iso.org/standard/80432.html. [Accessed 24 10 2021].

[32] ENISA, "Post-Quantum Cryptography: Current state and quantum mitigation," 03 05 2021. [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. [Accessed 24 10 2021].

[33] NATO, "NATO works on quantum cryptography with Malta," 16 04 2019. [Online]. Available: https://www.nato.int/cps/en/natohq/news_165733.htm. [Accessed 20 10 2021].

[34] Frank Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, p. 505–510, 2019.

[35] Zhong, Han-Sen; Wang, Hui; Deng, Yu-Hao; Chen, Ming-Cheng; Peng, Li-Chao; Luo, Yi-Han; Qin, Jian; Wu, Dian; Ding, Xing; Hu, Yi; Hu, Peng , "Quantum computational advantage using photons," Science, vol. 370, no. 6523, pp. 1460-1463, 2020.

[36] Global Times, "Chinese researchers achieve quantum advantage in two mainstream routes," 26 10 2021. [Online]. Available: https://www.globaltimes.cn/page/202110/1237312.shtml. [Accessed 31 10 2021].

[37] D. Leprince-Ringuet, "AWS's new quantum computing center aims to build a large-scale superconducting quantum computer," 29 10 2021. [Online]. Available: https://www.zdnet.com/article/awss-new-quantum-computing-center-is-dedicated-to-building-a-large-scale-superconducting-quantum-computer/. [Accessed 31 10 2021].

[38] L. Buttyán and I. Vajda, Kriptográfia és alkalmazásai, Budapest: Typotex, 2005.

[39] Roetteler, Martin; Naehrig, Michael; Svore, Krysta M.; Lauter, Kristin, "Quantum resource estimates for computing elliptic curve discrete logarithms," 2017.

DANGERS AND CHALLENGES OF SMALL POWER PLANTS ON THE ELECTRIC GRID

KISERŐMŰVEK OKOZTA VESZÉLYEK ÉS KIHÍVÁSOK A VILLAMOS HÁLÓZATOKON

BÁLINT Márton[1]

Abstract

Before some time, one was astonished to see in Austria the high wind turbines, and by travelling further in the mountains even in small towns shiny tablets, solar panels appearing on the roofs of the houses. Nowadays in Hungary such sights are more and more widespread, and even if the development of wind turbines has slowed down, thanks to the conscious consumer attitude and incentive application and financial environment the development of small, domestic solar power plants shows an even stronger increase. Such development calls for new challenges to the electrical distribution network, which are crucial for our everyday comfort even if their existence is often unnoticed by most of us. Stable voltage and symmetrical electrical parameters are the main aspects of them. The development of such electric power generation units also means an increase of potential risk of electrocution and electric fire.

Keywords

domestic power plant, distribution network, electrical industry, energy, overload, instability, risks

Absztrakt

Régebben álmélkodva szemléltük a szomszédos Ausztriába érve a hatalmas szélerőműveket, majd tovább haladva a hegyekbe a falvakban is felkerültek csillogó táblák, naperőművek a háztetőkre. Néhány év elteltével ez a látvány hazánkban is egyre gyakoribb, és bár a szélerőművek terjedése megtorpant, a háztartási naperőművek a tudatos fogyasztói hozzáállásnak, valamint az ösztönző pályázati és pénzügyi környezetnek köszönhetően annál nagyobb mértékben nőtt. Ez a növekedés azonban korábban ismeretlen kihívások elé állítja a sokak által kevésbé észlelt, ámde a mindennapjaink komfortjához elengedetlen villamos elosztó hálózatot, különösképpen a stabil feszültség, illetve szimmetrikus működés folyamatos biztosítását. Az elektromos termelő egységek elterjedésével párhuzamosan nőtt az áramütés és az elektromos tűz potenciál kialakulásának veszélye.

Kulcsszavak

háztartási kiserőmű, elosztó hálózat, villamosipar, energia, túlterhelés, ingadozás, veszélyek

[1]balint.marton@phd.uni-obuda.hu | ORCID: 0000-0002-5703-5584 | PhD Student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Egyre növekvő tendenciát mutat Európában és a világon a gazdaság dekarbonizációja, amelyhez jelentős mértékben járulnak hozzá a különböző energiarendszerek. A Párizsi Megállapodás ambiciózus környezeti céljainak elérése érdekében jelentősen meg kell növelni a megújuló energiaforrások részarányát az energiatermelésben.

Az energiaellátó rendszerek folyamatosan fejlődnek a bevezetésük kezdete óta – ez az ipari forradalom kései időszakára datálható. Jelentős előrelépés történt az energiaellátó rendszerek technológiájában a hatékonyság, a minőség, a biztonság és a megbízhatóság terén, az első kereskedelmi erőműtől (NY City, Pearl Street), amely egyenáramú (DC) generátorokat alkalmazott egy New York-i, egy négyzetmérföldes blokk ellátására, egészen a szárazföldet és a tengereket átszelő, egymástól távol lévő erőműveket összekötő villanyvezetékek széles hálózatáig [1]. Ez az evolúció lehetővé tette, hogy az energiaellátó rendszerek egyre nagyobb jelentőséget kapjanak az emberek életében, valamint a világgazdaságban. A megbízható energiaellátó rendszereket a modern társadalmak megkülönböztető jegyévé váltak [2].

Egyetlen műszaki rendszer sem teljes mértékben megbízható. Ennek megfelelően elkerülhetetlen a meghibásodások kockázata az elektromos elosztórendszerek (Electrical Distribution System - EDS) esetén. Ennek legkézzelfoghatóbb eredménye általában a fogyasztói oldalon fellépő kiesés. Ugyan gazdaságilag nem motivált – illetve nem is lehetséges - a maximális megbízhatóság elérése, de fontos a kockázatcsökkentés és a befektetési költségek közötti egyensúly megtalálása. Társadalmunk egyre inkább függ a megbízható villamosenergia-elosztástól, továbbá nőtt a költséghatékonyság iránti igény.

KISERŐMŰVEK ÁTTEKINTÉSE

A villamos energiáról szóló 2007. évi LXXXVI. törvény, valamint a 279/2007. (X.19.) Kormányrendelet 2008-ban bevezette a háztartási méretű kiserőmű fogalmát (HMKE). Az a villamos energiát termelő berendezés minősíthető háztartási méretű kiserőműnek a jelenlegi szabályozás szerint, amely a következő feltételeknek megfelel:

- közcélú kisfeszültségű hálózathoz, illetve kisfeszültségű magán- vagy összekötő vezeték hálózatra csatlakozik,
- erőművi névleges teljesítőképessége nem haladja meg a felhasználó rendelkezésre álló teljesítményének mértékét,
- valamint maximum 50 kVA erőművi névleges teljesítőképességű.

A háztartási méretű kiserőművek hallatán a legtöbb ember fejében a családi házak tetején helyet kapó napelempanelek összessége villanhat fel. Azonban ez a megnevezés, illetve a fentebb felsorolt feltételek további energiatermelő berendezéseket is magukba foglalnak:

- napelemes rendszer,
- szélturbina,
- vízturbina,
- motorhajtású berendezés (dízelmotor, Stirling motor stb.).

Alapvetően minden természetben előforduló energiaforrásunk a napenergiára vezethető vissza. A legtöbb energiát közvetett módon nyerik:

- fotoszintézis, amelyek a növények kémiai energiáját növeli, végül pedig a biomaszsza és a fosszilis tüzelőanyagok belső energiatartalmát határozza meg,
- párolgás, mint a víz és a gőz körforgása, amely a vízenergia potenciális energiáját határozza meg,
- végül pedig a víz és a levegő áramlása, amely megadja az óceáni áramlások és a szél mozgási energiáját, további a hullámok potenciális energiáját [3].

Azoknak az energiatermelő berendezéseknek, amelyek működése kihasználtsága az időjárási körülményektől jelentős mértékben függ (pl. napelemes rendszer, szélturbinás rendszer, vízturbinás rendszer), a hálózatra gyakorolt fő jellemzői a következők lehetnek:

- a hálózati feszültségprofil változása,
- tranziensek megjelenése be- és kikapcsoláskor,
- rövidzárlati áramok növekedése,
- a termelés és fogyasztás függvényében változó veszteségek mértéke,
- az ellátás minőségére és megbízhatóságára gyakorolt hatások,
- a védelem összehangolásának szükségessége [3].

A növekvő igény az ellátásbiztonság és -megbízhatóság iránt új feladatok elé állítja a tervezőket, fejlesztőket. A munkájukat elsősorban befolyásoló tényezők közé sorolhatjuk például a rendelkezésre álló teljesítmény előrejelzésének bizonytalanságát, a kimenő teljesítmények változásainak nagyságát és sebességét is [3].

A következőkben elsősorban a napelemes rendszerek jellemzésére fektetem a hangsúlyt, ezt pedig az 1. táblázatban látható adatok alapján teszem. Könnyen leolvasható és kiszámolható, hogy (a 2017-es adatok alapján) a háztartási méretű kiserőművek beépített összeteljesítményéből a napelemes rendszerek 99 %-t tesznek ki, emellett a többi erőműtípus termelése és darabszáma elhanyagolható.

Megnevezés	**Nap-energia**	**Szél-energia**	**Víz-energia**	**Biogáz**	**Bio-massza**	**Termál-metán**	**Föld-gáz**	**Dízel**	**Egyéb**	**Összesen**
Beépített teljesítőképesség [kW]	239960	619	112	115	20	206	291	11	36	241370
Darabszám [db]	29510	84	14	28	1	26	20	1	1	29685
Hálózatra betáplált villamos energia [MWh]	103626	105	387	32	0	553	258	0	125	105086

1. táblázat: HMKE-k energiaforrás szerinti eloszlása hazánkban 2017-ben [4]

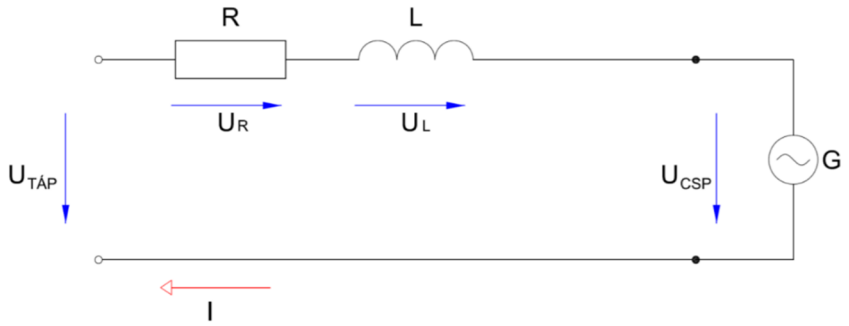
Az 1. táblázatból szintén leolvasható, hogy a szélenergia rendelkezik a második legnagyobb darabszámmal, azonban messze nem hozzá kapcsolódik a második legnagyobb mértékű hálózatra táplált villamosenergia – pedig a beépített teljesítőképesség alapján is a

szélenergia a második helyezett. Szintén látható, hogy 2017-ben több mint 241 MW beépített teljesítménnyel rendelkeztek a HMKE-k, amivel éves szinten több mint 105 GWh energiát sikerült a hálózatra táplálni.

A kiserőművek hálózati számításának alapjai

Először is szeretném bemutatni annak a folyamatnak az eletrotechnikai hátterét, amikor egy napelemes rendszert a középfeszültségű hálózatra csatlakoztatunk.

A középfeszültségű hálózatra csatlakozó HMKE-kről kijelenthető, hogy azok áramgenerátorként működnek, vagyis a pillanatnyi termelt árama állandó lesz. Az erőműnek a csatlakozási ponton feszültségkülönbséget kell létrehoznia, hogy ezt az áramot be tudja táplálni a hálózatba. Napelemes rendszerek inverterét (ami a termelt egyenáramot váltóárammá alakítva) tetszőleges fázishelyzetűre lehet állítani. Mivel az energiatermelő berendezés tulajdonosának érdekében áll, hogy minél nagyobb hatásos villamos energiát tápláljon a hálózatra (az átvételi árat a hatásos rész után kapja), a fázisszöget 1 értékre fogja állítani. Így például egy 10 kVA névleges teljesítményű napelemes rendszer 10 kW hatásos és 0 kVAr meddő teljesítményből fog összeadódni. Ezidáig a magyarországi elosztó engedélyesek nem vizsgálták annak a lehetőségét, ha a HMKE nem 1 értékű fázisszöggel üzemel. Egy hálózatra kapcsolt háztartási méretű kiserőmű elvi kapcsolási vázlata látható az 1. ábrán [5].



1. ábra: Hálózatra kapcsolt HMKE elvi vázlata [5]

Ahogy korábban említettem, a HMKE csatlakozási pontján feszültségemelést kell megvalósítani az erőműnek. Ennek az különbségnek a mértéke pedig a táppont és a csatlakozási pont közötti vezetékek impedanciájától függ, és az alábbi képlettel számítható:

$$\overline{U_{Táp}} = \overline{U_{CSP}} + \overline{U_R} + \overline{U_L} \Rightarrow \overline{U_{CSP}} = \overline{U_{Táp}} - (\overline{U_R} + \overline{U_L}) \quad (1)$$

Ahol:

$\overline{U_{Táp}}$ [kV]: a táppont villamos feszültsége,

$\overline{U_{CSP}}$ [kV]: a csatlapozási pont villamos feszültsége,

$\overline{U_R}$ [kV]: a fázisvezető ellenállásán eső feszültség [5].

$$\overline{U_R} = \bar{I} \cdot \bar{R} \quad (2)$$

Ahol:

$\bar{R}$ [Ω]: az energiaátvitelre szolgáló fázisvezető egyenáramú ellenállása,

$\bar{I}$ [A]: a hálózat egészén átfolyó áram,

$$\overline{U_L} = \bar{I} \cdot \overline{X_L} \tag{3}$$

Ahol:

$\overline{X_L}$ [Ω]: az energiaátvitelre szolgáló fázisvezető induktív reaktanciája.

Amennyiben a HMKE teljesítménytényezője 1, akkor az $\overline{U_R}$ és $\overline{U_L}$ egymással 90-ot zárnak be. A napelemes rendszerekben lévő inverter alkalmas arra is, hogy a megtermelt villamosenergia fázisát szabályozzák. Habár Magyarországon jelenleg nincs előírva a meddőteljesítmény szabályozása, azonban erre külföldön már van példa. Például Németországban a termelők lehetőséget kaptak a teljesítménytényező 5%-os változtatására, mind a két irányba (kapacitív és induktív). Ha a termelést induktív irányba mozgatják, akkor az erőmű feszültségemelése alacsonyabb, ha kapacitív irányba mozgatják, akkor pedig magasabb lesz [5].

ÜZEMZAVAROK

A kiserőművek dinamikus feszültségváltozása

Ha egy HMKE-t szeretnénk a hálózatra csatlakoztatni, akkor alapvetően két tényezőt szükségszerű megvizsgálni:

- a hálózat feszültség a vezeték egyik pontján sem lehet nagyobb az előírtnál
  - 22 kV esetében 24 kV,
  - 11 kV esetében 12 kV [5].
- a vezetéken létrehozható feszültségváltozás maximuma:
  - középfeszültségen 2%,
  - kisfeszültségen 3% [5].

Ezen értékeket országunk elosztói engedélyesei által elkészített és a MEKH által deklarált dokumentum tartalmazza (Elosztói Szabályzat - Háztartási méretű kiserőművek elosztóhálózati csatlakozásának műszaki feltételei). Azonban ezeket a mennyiségeket maga az elosztói engedélyes felülírhatja és engedélyezhet akár magasabb mértékű feszültségváltozást is [5].

Egy erőmű csatlakoztathatóságának pontos számítása igen bonyolult, általában számítógépen futó hálózatszámítási programok iterációs megoldásával lehetséges (load flow analízis). Azonban közelítése analitikus úton is lehetséges, ennek az alapvető egyenleteit fogom a következőkben bemutatni, az egyszerűbbtől haladva, az egyre bonyolultabb felé:

$$k = \frac{S_{Z-CSP}}{\sum S_{Gmax}} \tag{4}$$

Ahol:

k [-]: kiserőmű csatlakoztathatóságára szolgáló arányszám (a korábban bemutatott 2% vagy 3% reciproka),
S_{Z-CSP} [kVA]: a csatlakozási pont zárlati teljesítménye,
$\sum S_{Gmax}$ [kVA]: a csatlakozási ponton lévő HMKE maximális teljesítménye [5].

A tagokból is látható, hogy ez az összefüggés nem veszi figyelembe a hálózat fázistolását, sem pedig a HMKE termelésének fázisszögét.

$$\Delta U_{\%} = \frac{S_{Gmax} \cdot \cos(\Psi+\varphi)}{S_{Z-CSP}} \cdot 100\% \tag{5}$$

Ahol:

Ψ [°]: a vezeték fázisszöge,
φ [°]: az erőmű által termelt villamosenergia fázisszöge [5].

Ez az egyenlet ugyan már egy pontosabb közelítést eredményez, azonban 0 értéket is felvehet (cos90°) esetén, ami nem fordulhat elő a valóságban. Éppen ezért a $\cos(\Psi + \varphi)$ sosem lehet kisebb mint 0,1 [5].

$$\Delta U_{\%} = \frac{S_{Gmax} \cdot (\mathrm{R} \cdot \cos\varphi + X_L \cdot sin\varphi)}{U_v^2} \cdot 100\% \tag{6}$$

A (6) összefüggés segítségével már képesek lehetünk a vezeték ellenállásán és induktivitásán eső feszültség meghatározására [5].

Végezetül a HMKE csatlakoztathatóságát analitikus közelítéssel megadó (7) összefüggés:

$$\Delta U_{\%} = S_{Gmax} \cdot \frac{S_{Z-TP} - S_{Z-CSP}}{S_{Z-TP} \cdot S_{Z-CSP}} \cdot 100\% \tag{7}$$

Ahol:

S_{Z-TP} [kVA]: a táppont zárlati teljesítménye [5].

HMKE hálózati visszahatásai

Feszültségemelkedés és feszültségesés

A hálózati visszahatások sorából a legjelentősebb a hálózati feszültség változására való hatás. Amennyiben a korábban már leírt csomóponti feszültségemelkedés az előírt maximumnál (jelenleg 3%) magasabb, akkor a rendszerben zavarok keletkezhetnek. A másik alapvető eset, amikor a hálózaton nem feszültségemelkedés, hanem feszültségesés következik be. Ez például akkor fordulhat elő, ha a kiserőművet lekapcsolják a hálózatról (pl. egy

védelmi automatika). Természetesen több védelmi automatika kapcsolása esetén, nagyobb, érezhető esés következik be a hálózati feszültségben [6].

Negatív aszimmetria

Az MSZ EN 50160 szabvány (A közcélú elosztóhálózatokon szolgáltatott villamos energia feszültségjellemzői) előírja a maximális negatív sorrendű aszimmetria értékét (háromfázisú fogyasztó esetén kisebbnek kell lennie, mint 2%, egyfázisú fogyasztó esetén pedig 3%-nál). Ez az aszimmetria akár hálózati oldalon, akár fogyasztói oldalról is jelentkezhet [6]:

$$A_x = \frac{X_{negatív}}{X_{pozitív}} \tag{8}$$

Ahol:

A_x [-]: az aszimmetria mértéke,

X_i [V vagy A]: pedig az aktuális mennyiség, feszültség [V] vagy áram [A] alapharmonikus [6]

A HMKE hálózati visszahatásainak lehetséges műszaki megoldásai

Feszültségváltozás csökkentése

A manapság napelemes rendszerekben használatos inverterek impulzusszélesség modulációra képesek. Ugyan jelenleg nem alkalmazzák, de képesek lennének akár induktív, akár kapacitív meddőtermelésre is. Továbbá ehhez egy olyan automatikus szabályozóra is szükség lenne, ami szabályozza a meddőtermelés irányát és mennyiségét (például Németországban már kizárólag ilyeneket alkalmaznak) [6].

Szimmetria biztosítása

Abban az esetben, ha az aszimmetria hálózati, akkor az adott vezető két végpontját szükséges szimmetrizálni. Viszont, ha azt a szimmetriát szeretnénk minimalizálni, amit a terhelés okoz, akkor erre a következő módszerek léteznek:

- szimmetrikusan el kell oszlatni a fogyasztói terhelést,
- adott fogyasztónál szükséges kompenzálni,
- zárlati teljesítményt kell növelni a csatlakozási ponton [6].

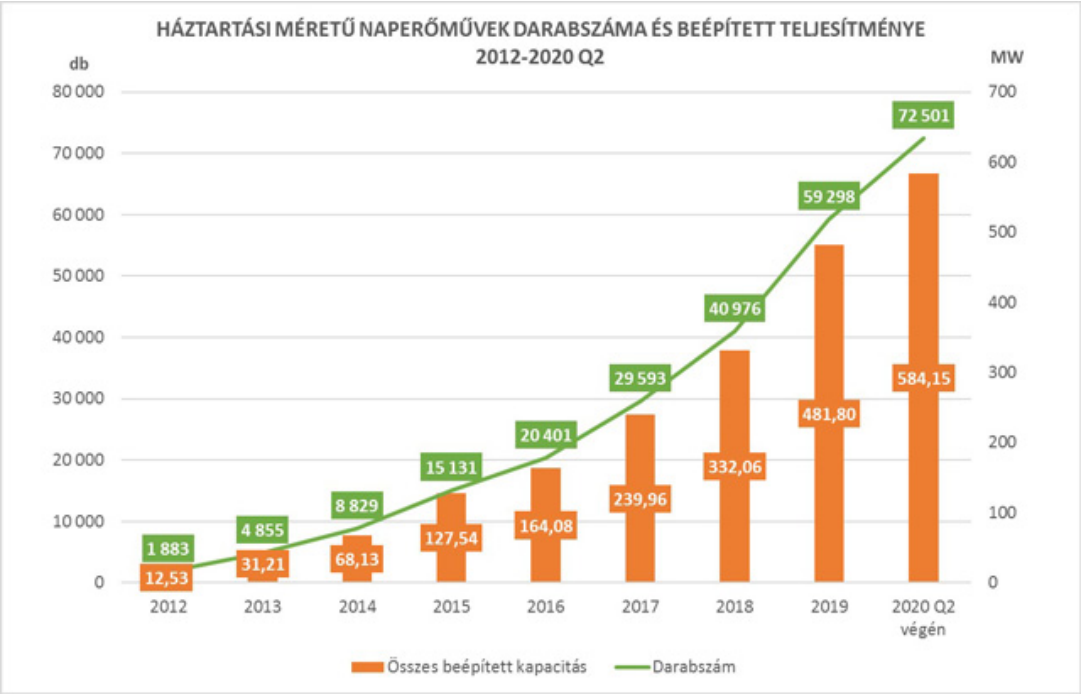
INFRASTRUKTÚRA- ÉS SZEMÉLYVESZÉLYEZTETÉS

A 2. ábrán látható a háztartási méretű napelemes rendszerek rohamos növekedése az elmúlt évtizedben. Vélhetőleg, ha nem is ilyen léptékben, de a tendencia folytatódni fog. ráadásul a szélsőséges időjárási jelenségek a napelemes rendszereket sem kímélik, és ezek terjedésével az energiabiztonság és kármegelőzés kérdése is egyre nagyobb kihívásokat jelentenek, mint ahogy erről Dr Szűcs Endre is ír a „Rendkívüli időjárási viszonyok közötti energiabiztonság megvalósításának lehetőségei családi ház esetében” című dolgozatában. [7].

A napelemes rendszerek esetében két alapvető veszélyforrás említhető meg:

- tűzeset,
- áramütés [8].

Az 1. táblázat 2017-ig tartalmazott adatokat a MEKH közzététele alapján, azonban a 2. ábrán látható, hogy a háztartási méretű napelemek darabszáma és teljesítménye több mint duplájára növekedett.



2. ábra: Háztartási méretű napelemes rendszerek darabszámának és beépített teljesítményének alakulása (Forrás: https://www.mnnsz.hu/toretlen-a-haztartasi-meretu-naperomuvek-terjedese/)

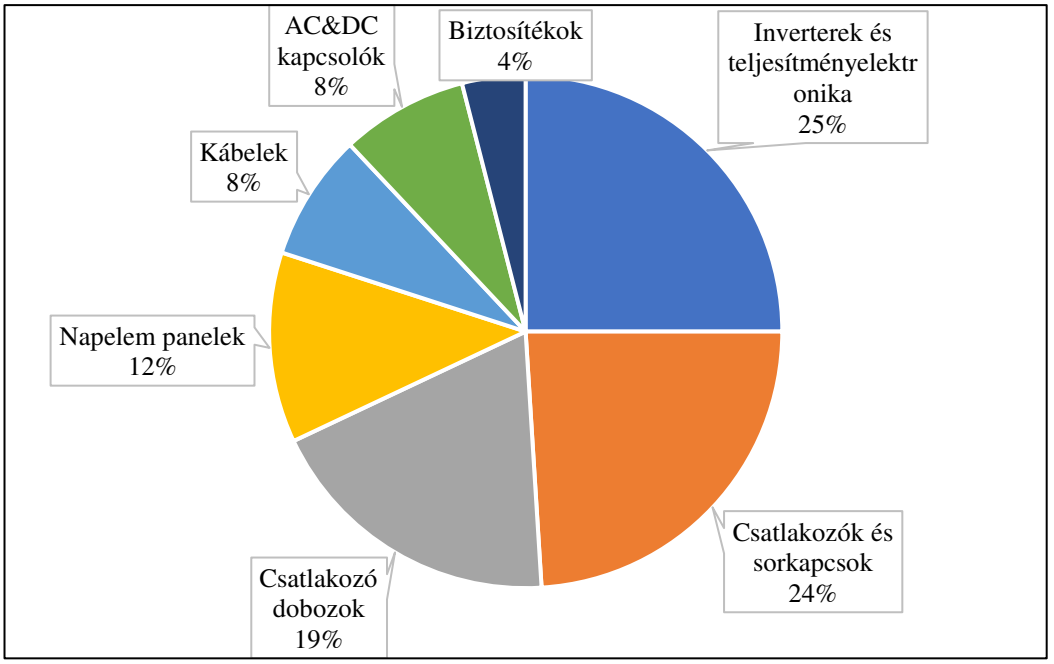
Tűzeset

Magyarországon jelenleg nem található olyan statisztika, amely a napelemes rendszerek tűzeseteit vizsgálná, ezért a nemzetközi esetekből végeztem merítést, ezt prezentálom a továbbiakban (2. táblázat és 3. ábra).

Helyszín idő	**Telepítési jellemzők**	**Károsodás**	**Az oltási műveletek akadályai**
Bakersfield, CA, USA 2009. április	Kereskedelmi bolt tető 380 kW	A tűz nem károsította a fém tetőfedést	Két külön tűz alakult ki, valamint a DC-leválasztók hiánya miatt egy villanyszerelőnek kellett 56 biztosítékot kapcsolnia
Delanco, NJ, USA 2013. szeptember	Raktártető 1,6 MW	A tetőszerkezet 30 000 m^2 része megsemmisült	az áramütés veszélye miatt a tűzoltók nem oltották a tetőt
La Farge, WI, USA 2013. május	Irodaháztető 70 kW	A 4 000 m^2 alapterületű épület egyik szárnya megsemmisült	A tetőszerkezet lefedése akadályozta a szellőzést és felgyorsította a részleges beomlást
Walldorf, Németország 2014. június	Raktártető	Néhány ezer európai kár	A rendszerek rögzítésére szintetikus gyantalemezt használtak. A tűzoltók az épület elérése előtt megfékezték a tüzet.
Norderney, Németország 2013. augusztus	Gyárépület tető	Néhány millió európai kár	A tetőszerkezet összeomlott a napelemekkel együtt.

2. táblázat: Napelemes rendszerekhez köthető tűzesetek médiamegjelenések alapján (Forrás: https://pv-magazine-usa.com/2019/08/22/there-are-solar-power-fires-per-year/)

A 2. táblázatban bemutatott néhány esetből levonható, hogy a napelemes rendszerekhez köthető tűzesetek és az azokból eredő károk mennyisége és milyensége nem függ közvetlenül a napelemes rendszer méretétől.



3. ábra: 1995-2012 közötti németországi napelemrendszerekhez köthető tűzesetek (180 db) kiindulópontjai (Forrás: https://pv-magazine-usa.com/2019/08/22/there-are-solar-power-fires-per-year/)

Átlagos körülmények között egy mai közepes teljesítményű napelem modul kb. 30-40 V egyenfeszültséget jelent, azonban, ha több panelt sorba kötünk, az így adódó feszültség akár az 1000 V egyenfeszültséget is elérheti (a 8-9 A termelt egyenáram mellett). Egyenáram esetén az esetlegesen létrejövő elektromos ívet sokkal nehezebb kioltani, ugyanis nincs nullátmenet. Az előbb leírt mennyiségek mellett akár 10-20 cm-es ív is kialakulhat, ami könnyedén okozhat tüzet – tetőszerkezetre telepített napelemek esetén – a tetőszerkezetben [9].

Az MSZ HD 60364-7-712 szabvány (Épületek villamos berendezéseinek létesítése. 7-712. rész: Különleges berendezésekre vagy helyiségekre vonatkozó követelmények. Napelemes (PV) energiaellátó rendszerek (IEC 60364-7-712:2002)) kijelenti, hogy a fotovoltaikus rendszerek egyenfeszültségű oldalát folyamatosan feszültség alatt állónak kell feltételezni. Ez akkor is fennáll, ha maga az épület áramtalanítva van. Amennyiben tűz üt ki és a vezetékek sérülnek, azok tovább gerjesztik a tüzet, valamint akár a tűz megfékezését végző tűzoltók áramütését is okozhatják. Az OTSZ (Országos Tűzvédelmi Szabályzat) és a TvMI (Tűzvédelmi Műszaki Irányelv) meghatározzák a napelemes rendszerek egyenoldalának lekapcsolását tűzeset idején. Továbbá előírják, hogy az épületen belüli egyenfeszültségű vezeték hosszát minimalizálni szükséges, illetve automata kapcsoló beépítésével szükséges biztosítani az egyenvezetékek bontását feszültségmentesítés esetén. Külön pont foglalkozik azzal, hogy a csatlakozódobozokon jól látható, feliratot kell elhelyezni, ami arra hívja fel a figyelmet, hogy a vezetőket állandóan feszültség alatt állónak kell tekinteni (karbantartáskor megelőzhető a szerelő áramütése). Ez utóbbi célt szolgálja a napelemes rendszer létére figyelmet felhívó felirat is, amelyet az épület bejáratánál vagy a tűzvédelmi főkapcsolónál szükséges elhelyezni (tűzoltók számára is hasznos információ) [9].

4. ábra: Tetőszerkezeten helyet kapó napelemes rendszer tűzeset után
(Forrás: https://www.pv-magazine.com/wp-content/uploads/2020/11/fire-pic.jpg)

Egyenfeszültségű oldalon nem alkalmazhatók az AC hálózatoknál megszokott érintésvédelmi megoldások (TT vagy TN), egyenfeszültség esetén a II. hibavédelmi osztály vagy az ún. kettős szigetelés alkalmazása szükséges. Ezek alapján kijelenthető, hogy az egyenfeszültségű oldalon alkalmazott minden eszköznek meg kell felelnie az 1000 V egyenfeszültségnek, illetve a kettős szigetelésnek is. Ebből kifolyólag nem alkalmazhatók a 400 V váltófeszültségre tervezett berendezések [9].

A napelemmodul hőmérsékletének függvényében változik annak kimeneti feszültsége. A gyártók által megadott értékeket a panel adattábláján a következő bemeneti paraméterek mellett kell érteni: 1000 W/m2 fényintenzitás, 25 °C felületi hőmérséklet és 1,5 AM (légtömörség tényező). A napelem modulok kimeneti feszültsége a hőmérsékletcsökkenése mellett emelkedik. Egy tiszta, napfényes, hideg téli napon mért feszültség akár 100 V-tal is nagyobb lehet, mint egy meleg nyári napon mért modulfeszültség. Minden alkalmazott berendezésnek meg kell felelnie ezeknek a szélsőséges viszonyoknak is (kapcsolók, túlfeszültséglevezetők stb.). Ezen információ felett való eltekintésből a rendszertervezéskor, kivitelezéskor keletkezik a legtöbb napelemes tűzeset. Egy nem megfelelően kiválasztott egyenoldali kapcsoló esetében létrejövő elektromos ív nem fog elaludni, így a kapcsoló hamar túlmelegszik, majd kigyullad és tűz keletkezik. Nem csak a kapcsolókra, hanem a csatlakozódobozok megfelelő kiválasztására is nagyobb hangsúlyt kellene fektetnie a tervezőknek, kivitelezőknek. Nem pedig az egyszerűbb és megfelelő minősítéssel nem rendelkező alkatrészek alkalmazására törekedni a költséghatékonyság jegyében [9].

5. ábra: Fotovoltaikus rendszer kapcsolódoboza tűzesetén után
(Forrás: https://www.villanylap.hu/images/1751-1488969483.jpg)

Kristensen és társai a tűzesetek hatását vizsgálták lapostetős épületre vonatkozólag, amelyen napelempanelek találhatók. Ehhez magát a tüzet gázégővel reprezentálták, nyolc pontban mérték a hőáramot – ugyanabban a síkban, ahol a gázégő teteje helyezkedett el. A gázégőt a napelempanel középpontja alatt helyezték el. Az eredményeket napelempanel nélküli esettel hasonlították össze, amikor a napelem visszaverő hatása nem érvényesül. Jelentős mértékű hőáramnövekményt mértek a paneles esetben, ez azt jelzi, hogy a panelek nagymértékben hozzájárulhatnak a tető károsodásához, elsősorban azért, mert fokozzák a tetőn terjedő tüzet, amelyre fel vannak szerelve. A mért hőáram nagyobb volt a panel legmagasabb része alatt, két fontos, lánggal összefüggő ok miatt:

- lángelhajlás a panel legmagasabb része felé,
- a panel felületének hőmérsékleteloszlása nem homogén az elhajlott láng következtében, ebből következik, hogy a felhevített panel emissziója sem homogén [10].

A tesztek eredményei rendkívül hasonlók voltak egy vadonatúj modul és egy negyedik alkalommal tesztelt panel esetében. Kivéve azt az időtartamot, amíg az új napelem alatt lévő vékony fólia égett [10].

Ju és társai szintén a tűzesetek és a napelempanelek kapcsolatát vizsgálták. Pontosabban szintén azt az eshetőséget, amikor a lapostetőre szerelt napelempanelek hátsó oldala tovább gerjeszti a tüzet. A megdöntött napelemek alatt szintén gázégőt használtak hőforrásként, és a panel dőlésszögét, a tetőtől való távolságát, valamint a hőfelszabadulási sebességet (Heat Release Reat – HRR) vizsgálták. Megmérték a lángkiterjedés geometriáját és a láng reradiációs hőáram-eloszlását. Az eredmények azt mutatták, hogy a lángnyújtás hossza

és függőleges vastagsága (azaz a panel hátsó felületétől a lángprofilig mért távolság) a napelem dőlésszögének és a panel-tető távolságának növekedésével csökken, viszont a tűz hőfelszabadulási sebessége nő. Ezeket a tényezőket egybegyúrva javaslatot tettek egy dimenzionélküli HRR használatára a lángkiterjedés geometriájának egységes számszerűsítésére. Ezenkívül a lángsugárzás és a lánggeometria közötti fizikai összefüggésen alapuló általános egyenletet dolgoztak ki a reradiációs hőáram eloszlásának jellemzésére a tető felületén. Végül javaslatokat fogalmaztak meg a telepítéssel és a tetőfedő anyagok kiválasztásával kapcsolatban, a tetőre telepített napelemes rendszerek alatt kialakulható láng terjedési sebességének csökkentése érdekében [11]

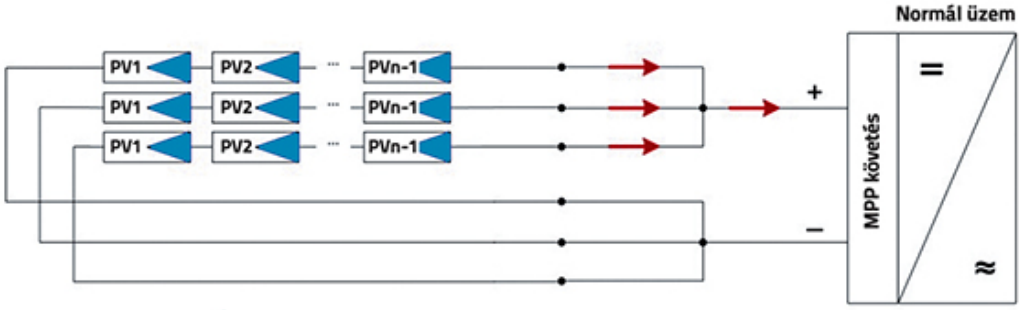
Összefoglalva elmondható, hogy a napelemes rendszerekhez kapcsolódóan két csoportba oszthatók a tűzvédelmi intézkedések:

- megelőző intézkedések, amelyekkel a DC-oldalon létrejövő meghibásodás tűzokozása és a következmények súlyának csökkentése érhető el,
- illetve a mentést segítő intézkedések, amelyekkel az oltásban és mentésben résztvevők áramütése kerülhető el [12].

A megelőző intézkedések általában passzív módon értendők (pl. megfelelő nyomvonal kialakítás, illetve a vezetékek tűzálló anyaggal való körülhatárolása). A mentést segítő intézkedések pedig aktív módon értendők (pl. tűzeseti lekapcsolás) [12].

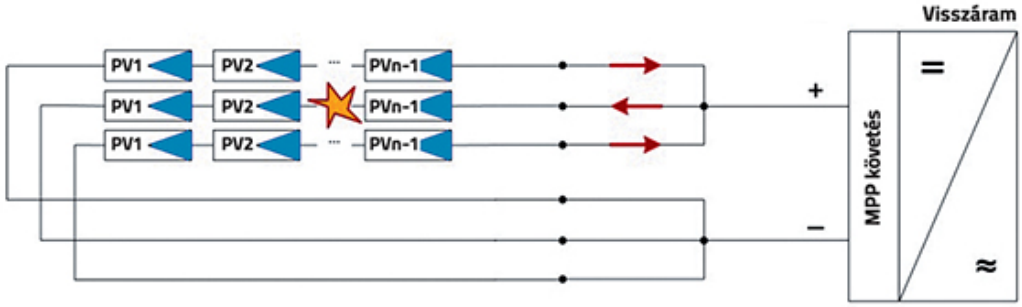
Visszáram

Rövidzár esetén a munkaponti áram mennyiségéhez képest kb. 20%-kal nagyobb a napelem zárlati árama. Napelemes rendszerek esetében a túláramvédelem kialakítása meglehetősen körülményes, erre az igény főleg nagyobb rendszerek esetén értelmezendő (párhuzamosan kötött sztringek esetén). Túláram esetén is végül tűz alakulhat ki, hiszen a modulok felmelegszenek, tönkre mehetnek, egyenáramú ív alakulhat ki, ami tűzhöz vezet [9].



6. ábra: Napelemes rendszer normál működése [9]

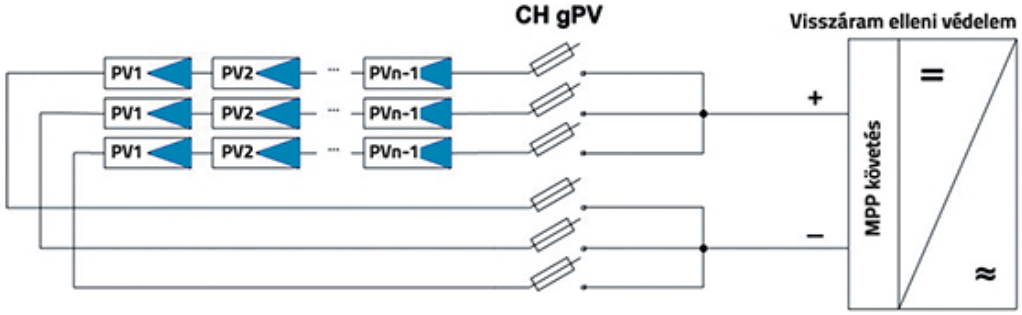
A 6. ábrán látható, hogy a rendszer normális működése során a párhuzamosan kötött sztringek áramai összeadódnak.



7. ábra: Napelemes rendszer egyik sztringjében kialakult zárlat hatása [9].

A 7. ábra az egyik sztringben kialakult zárlat hatását szemlélteti, ekkor a hibapont felé folyik az áram a még jól működő ágakból. Könnyen belátható, hogy a hibapont felé folyó áram nagysága a párhuzamosan kapcsolt sztringek számától függ [9].

A napelemek egyenoldalának túláramvédelme az ún. gPV karakterisztikájú olvadóbetétekkel oldható meg (legalább is, ha megfelelően vannak méretezve). A túl alacsony zárlati áramra választott betét akár intenzív besugárzás esetén is ki tud olvadni, viszont a túl nagy zárlati áramra méretezett betét nem fog kellő védelmet biztosítani. A túláramvédelem méretezésének alapja akár a rendszer földrajzi elhelyezkedése is lehet (északon kisebb áramra, délen nagyobb áramra) [9].



8. ábra: gPV olvadóbetétek elhelyezése a napelemes rendszer egyenoldalán [9]

Az olvadóbetétek szerelése során figyelmet kell arra szentelni, hogy minden sztring mindkét pólusába elhelyezésre kerüljenek (8. ábra). A választott betétek névleges feszültségének nagyobbnak kell lennie, mint a maximálisan előfordulható feszültség. Magyarországon a következő ökölszabály követendő a gPV olvadódbetétek méretezése során: a napelem sztring zárlati áramát 1,2-vel megszorozzuk, majd az eggyel nagyobb biztosítékértékkel rendelkező betétet választjuk. Például egy 8,67 A zárlati árammal rendelkező sztring esetén 12 A értékű biztosítékokat kell mindkét pólusába szerelni. Nagyobb teljesítményű rendszerekhez kapható invertereknél a gyártók már külön foglalatot is kialakítanak ezeknek a betéteknek, sőt akár magától a gyártótól is lehet kérni, hogy beszerelje a sztringbiztosítékokat [9].

Veszélyforrások az inverter váltóoldalán

A hálózatra tápláló inverterek azokkal szinkronban működnek, vagyis hálózati áramszünet esetén az inverternek is szükséges lekapcsolnia (például karbantartás esetén ne fordulhasson elő, hogy a szerelők áramütést szenvednek a hálózatra tápláló HMKE miatt). A hálózati engedélyes a következő védelmi funkciók meglétét írhatja elő a hálózatára csatlakoztatni kívánt inverter esetében:

- rövidzárlat-védelem,
- túlterhelés-védelem,
- feszültségnövekedés-védelem,
- feszültségcsökkenés-védelem,
- frekvenciaeltérés-védelem,
- elosztóhálózati-szigetüzem elleni védelem,
- földzárlatvédelem,
- testzárlatvédelem,
- egyenáramú védelem [9].

Ha összegezni szeretnénk a felsoroltakat, akkor elmondható, hogy a HMKE nem veszélyeztetheti a hálózat biztonságos üzemét, minőségét, szimmetriáját, torzítás- és villogásmentességét. Továbbá hálózati zárlat esetén, arra nem táplálhat rá, illetve a névlegesnél nagyobb áramot sem táplálhat a rendszerbe (max. 10%) [9].

Időjárás okozta veszélyforrások

Mivel a fotovoltaikus rendszereket szabadég alá telepítik (épület tetejére vagy nyílt terepre), és nem csupán néhány évre tervezik élettartamukat, a felhasznált anyagoknak és alkatrészeknek több évtizedig ki kell bírniuk az időjárás viszontagságait. Legnagyobb veszélyt természetesen a villámcsapás jelenti, hiszen a rendszerek nagy mennyiségű fémet tartalmaznak, amelyekből villamos vezetékek indulnak. Ezek a természeti jelenségek villamos zavarokat idéznek elő, nagyméretű túlfeszültség formájában (nem megfelelő vezetékelrendezésből adódó hurkok miatt). Tetőre telepített eszközök esetében akár az épület egyéb készülékeiben is kár keletkezhet (nem csupán a telepített panelekben). Éppen ezért rendkívül fontos a villámvédelem figyelembe vétele a tervezés és a kivitelezés során (pl. megfelelő vezetékezés, túlfeszültség-levezetők alkalmazása) [13].

Tetőszerkezetre telepített rendszer esetén a villámvédelmet mindig az épülettel együtt szükséges kezelni. Figyelembe kell venni az adott épületre jellemző évenkénti villámok számát, azt növelő vagy csökkentő tényezőket, vezetékeket, tetőszerkezet kialakítását, minőségét, anyagát, jellegét, pánikveszélyt. A szakma jelenlegi ismerete alapján a tetőre elhelyezett napelemes rendszerek nem növelik az épület villámcsapási kockázatát, azonban négy kockázat követelménye alapján szükséges meghatározni a villámvédelem szükségességét:

- emberi élet elvesztése (R1),
- közszolgáltatás kiesése (R2),
- kulturális örökség elvesztése (R3),
- gazdasági érték elvesztése (R4) [14].

A földre telepített napelemes rendszerek pénzügyi oldaláról megközelítve szintén szükségesek a villámvédelmi intézkedések, hiszen, ha az üzemelés során káresemények történnek, akkor a rendszer után fizetendő biztosítási díj is emelkedik, amely végül csökkenő megtérülési időt eredményez. Bármilyen objektum közvetlen villámcsapás elleni védelmének kialakításának szükségessége statisztikai alapra vezethető vissza. A földre telepítendő napelemes rendszer felületigénye könnyedén meghatározható a helyszínre érkező napsugárzás mennyiségéből, a rendszer tervezett tájolásából, a panelek dőlésszögéből, valamint az egyes rendszerelemek hatásfokából. Ezután villámsűrűségi térképből meghatározható a telepítendő rendszer helyszínére jellemző évenkénti villámcsapások száma, amelyből megadható, hogy évente hány darab villámcsapásra, vagy hány évente kell közvetlen villámcsapásra számítani a napelemes rendszer teljes területén. A villámvédelmi mechanizmusokkal elsősorban a gazdasági kiesés miatt érdemes kalkulálni. A 9. ábra például egy csehországi földre telepített napelemes rendszer egyik panelsorát mutatja közvetlen villámcsapás után [14].

9. ábra: Csehországi napelemes rendszer közvetlen villámcsapást követően (Forrás: https://www.dehn.hu/sites/default/files/media/files/gyik-09.pdf)

ÖSSZEFOGLALÁS

A háztartási méretű kiserőművek telepítési üteme egyre csak nő, nem csak hazánkban, hanem a nemzetközi szintéren is egyre több döntés születik ezen rendszerek telepítése mellett. A telepített háztartási méretű kiserőművek jelentős hányada napelemes berendezés. Jelen cikkben a háztartási méretű kiserőművekkel kapcsolatos kihívások egy részét mutattam be, elsősorban azokat, amelyek kapcsolatban állnak, állhatnak az elosztói hálózattal.

Először is felvázoltam a háztartási méretű kiserőmű fogalmát, típusait, illetve lehetséges energiaforrásait. Bemutattam, hogy a megújuló energiaforrások szinte mindegyike

visszavezethető a napenergiára. Egyébként a fosszilis energiaforrások (témakörhöz kapcsolódóan pl. dízelmotorral hálózatra termelt villamosenergia) is értelmezhetők megújuló energiaforrásként, csupán a megújulási ciklusuk nem emberi léptékkel felfogható.

Egy rövid áttekintő után, bemutattam a háztartási méretű kiserőművek hálózati számítási alapjait, végezetül pedig rátértem a fő témára, az erőművekkel kapcsolatos üzemzavarokra. Elsőként a hálózatra gyakorolt lehetséges zavarokat soroltam fel és jellemeztem, ide sorolva a dinamikus feszültségváltozást, a feszültségemelkedést, feszültségesést, a negatív aszimmetriát, valamint az ezekre alkalmazható megoldási javaslatokat is bemutattam. Az utolsó fejezetben pedig bemutattam a háztartási méretű kiserőművek esetén szóba jöhető infrastruktúra- és személyveszélyeztetést, megemlítve a lehetséges tűzeseteket, áramütéseket, egyen- és váltóoldali veszélyforrásokat, valamint a szélsőséges időjárási jelenségek okozta veszélyeket és azoknak lehetséges megoldásait.

A cikk írása során világossá vált számomra a téma rendkívüli összetettsége, a rendszerek tervezését és a telepítést végző vállalkozók nagyon nagy felelőssége, hiszen egy-egy alkatrészen (típusán) való spórolás, akár emberéletekbe is kerülhet.

IRODALOMJEGYZÉK

[1] HUGHES, T. P.: *Networks of power: Electrification in Western society, 1880–1930*. London, England: JHU Press, 1993.

[2] SMIL, V.: *World history and energy.* Encyclopedia of Energy, 6, 549–561. 2004

[3] MIKULEC, A. és MIKULIČIĆ, V.: *Influence of Renewable Energy Sources on Distribution Network Availability.* Computer Science, International Journal of Electrical and Computer Engineering, 2011.

[4] MEKH: *Összefoglaló a nem engedélyköteles – ezen belül a háztartási méretű – kiserőművek adatairól (2008–2017).* http://www.mekh.hu/download/7/28/60000/nem_engedelykoteles_es_hmke_beszamolo_2008_2017.pdf Letöltve: 2021.05.08

[5] KOVÁCS, Z.: *A decentralizálódó középfeszültségű hálózatok problémáinak vizsgálata*. Diplomamunka, Miskolci Egyetem, 2018.

[6] SZABÓ, S.: *Háztartási méretű kiserőművek hatása az elosztóhálózat fejlesztésére.* Szakdolgozat, Miskolci Egyetem, 2017

[7] Szűcs, Endre (2010): *Rendkívüli időjárási viszonyok közötti energiabiztonság megvalósításának lehetőségei családi ház esetében* pp. 12-17. Paper: 8. In: Rácz, Pál (szerk.) IESB2010, Budapest, Magyarország: Óbudai Egyetem

[8] DÁN, A. és ORLAY, I.: *Háztartási méretű kiserőművek szerepe a jövő energiaellátásában*. Elektrotechnika, A magyar elektrotechnikai egyesület hivatalos lapja. 101. évfolyam, 2008/10, pp. 5-7.

[9] MVM PARTNER ZRT.: *A napelemes rendszerek technikai veszélyforrásai.* Online cikk, elérhetőség: *https://www.mvmpartner.hu/Szolgaltatasok/Villamos-energia/Erdekessegek/A_napelemes_rendszerek_technikai_veszelyforrasai?fbclid=IwAR2HB1VuSH7GXeMdYLWRVL4hZ73FC2vUtjDR64CtukadZHNh4wMGjlqqLjM* Letöltve: 2021.05.09.

[10] KRISTENSEN et al.: *Fire-induced reradiation underneath photovoltaic arrays on flat roofs.* Szakmai cikk, Fire and Material, Volume 42, Issue 3, 2018, pp. 316-323.

[11] JU et al.: *Impact of flat roof–integrated solar photovoltaic installation mode on building fire safety.* Szakmai cikk, Fire and Material, Volume 43, Issue 8, 2019, pp. 936-948.
[12] KRUPPA, A.: *Épületeken elhelyezett napelemes rendszerek tűzvédelme*. Védelem Katasztrófavédelmi Szemle, 2. szám, 2015. pp. 48-50.
[13] PÁSZTOHY, T.: *A napelemes rendszerek veszélyforrásai és azok kiküszöbölése.* Szakmai cikk, Villanyszerelők Lapja, 2012. május.
[14] DEHN: GYAKORI KÉRDÉSEK, ONLINE CIKKEK, ELÉRHETŐSÉGEK:
1. https://www.dehn.hu/sites/default/files/media/files/gyik-09.pdf
2. https://www.dehn.hu/sites/default/files/media/files/gyik-10.pdf
3. https://www.dehn.hu/sites/default/files/media/files/gyik-11.pdf
Letöltve: 2021.05.09.

STUDY OF PREPAREDNESS AGAINST INDUSTRIAL ESPIONAGE AMONG HUNGARIAN ORGANIZATIONS

AZ IPARI KÉMKEDÉSSEL SZEMBENI FELKÉSZÜLTSÉG VIZSGÁLATA A MAGYAR SZERVEZETEK KÖRÉBEN

MÉSZÁROS Alexandra Ágnes[1] – TICK Andrea[2]

Abstract

In the recent dynamic economic environment, industrial espionage is a serious threat to innovative organizations. From the viewpoint of this study, industrial espionage is the acquisition of competitors' trade secrets using unethical or illegal tools, to increase the organization's competitiveness and reduce the cost and time of R&D&I activities. The purpose of this research is to reveal how Hungarian organizations manage the threat of industrial espionage. This study also aims to explore what level of risk industrial espionage is considered at Hungarian organizations and whether they make efforts to prevent becoming a victim of it. During the quantitative research, the data was collected using questionnaires, the number of respondents involved in this study was 273. Based on the results Hungarian organizations are well aware of the problem and make effort to prevent the threat of industrial espionage. However, according to the results, organizations do not consider industrial espionage as high risk.

Keywords

industrial espionage, information safety, business information, innovation

Absztrakt

Napjaink dinamikusan változó gazdasági környezetében az ipari kémkedés magas kockázatot jelent az innovatív szervezetek számára. A kutatás szempontjából az ipari kémkedés a versenytársak üzleti titkainak etikátlan vagy illegális eszközökkel való megszerzése, melynek a céljai a saját versenyképesség növelése és a K+F+I tevékenységek költség- és időigényének csökkentése. A kutatás célja feltárni, hogy a magyar szervezetek mennyire vannak tudatában az ipari kémkedés jelentette fenyegetésnek, milyen fokú kockázatként tartják számon, továbbá tesznek-e preventív lépéseket a negatív hatások elkerülése érdekében. A kvantitatív kutatás során az adatgyűjtés kérdőív segítségével történt. A kutatás eredményei alapján (n=273) a magyar szervezetek tudatában vannak az ipari kémkedés jelentette kockázatnak, továbbá törekednek annak megelőzésére. Azonban az eredmények arra engednek következtetni, hogy a megkérdezettek nem tartják magas kockázatnak, hogy a szervezet ipari kémkedés áldozatává váljon.

Kulcsszavak

ipari kémkedés, információbiztonság, üzleti információ, innováció

[1] meszaros.alexandra@uni-obuda.hu | ORCID: 0000-0003-3652-0203 | PhD student, Óbuda University | PhD hallgató, Óbudai Egyetem

[2] tick.andrea@uni-obuda.hu | ORCID: 0000-0002-3139-6509 | associate professor, Óbuda University, Keleti Károly Faculty of Business and Management, Department of Management and Quantitative Methods | egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar, Módszertani és Menedzsment Intézet

BEVEZETÉS

Az ipari kémkedés a legrégebbi üzleti tevékenységek közé sorolható, és bár a módszerek jelentős átalakuláson mentek keresztül az évszázadok során, a tevékenység a mai napig szerves része a gazdaságnak. A történelem első dokumentált esetéért egészen az időszámításunk előtti 4. századig kell visszatekinteni, amikor Kína selyemhernyó tenyésztési és selyem készítési titkait megfigyelték, ellopták és alkalmazni kezdték Japánban, Koreában, Indiában és Európa szerte [1]. Az ipari kémkedés történetének egy másik jelentős esete a 19. század során zajlott, amikor a Brit Birodalomhoz tartozó Kelet-Indiai Társaság felbérelt egy botanikust, hogy tudja meg Kína tea termesztési titkait, aminek eredményeként India történelmi versenyelőnyt szerzett Kínával szemben a tea piacán [2]. Egy másik, napjainkban is aktívan zajló példa az ipari kémkedésre Kína, amely évtizedek óta működtet egy minden elképzelhető eszközt magában foglaló, alaposan kidolgozott rendszert a külföldi technológiák felkutatására és megszerzésére, hogy azt saját, versenyképes termékeivé transzformálja az eredeti tulajdonos teljes kompenzációjának hiányában [3, 4].

Kétség nem fér hozzá, hogy napjaink dinamikusan változó gazdasági környezetében a legnagyobb érték az információ. Az a piaci szereplő képes a versenyképesség megtartására, illetve fejlesztésére, akinek rendelkezésére áll az innovatív üzleti információ. Ennek a megszerzési módja elméletileg a külső környezet elemzéséből, és a belső K+F+I tevékenységekből összetevődő, hosszú és költséges folyamat. A gyakorlatban azonban ez a tevékenység gyakran megy végbe etikátlan, illegális eszközök felhasználásával. A versenyben maradásért a vállalatok hatalmas összegeket fektetnek az innovációs tevékenységbe, amely rendkívül vonzó azon szereplők számára, akik hajlandók etikátlan vagy illegális eszközökhöz nyúlni. Az ipari kémkedés a versenytársak üzleti titkainak illegális eszközökkel való megszerzése, melynek okai a saját versenyképesség növelése és a K+F+I tevékenységek költségeinek és időigényének csökkentése. A gazdasági célú ipari kémkedés jelensége nem egy modern probléma, azonban a digitális forradalom csak tovább fokozta, amelynek hatására az üzleti titok illegális eltulajdonításához már nincs szükség speciális eszközökre. A fejlődés, továbbá a hozzáférés egyszerűsödése felbátorítja a gazdasági entitásokat az információ lopásra, amihez az is nagyban hozzájárul, hogy a tevékenység biztonságosan végezhető úgy, hogy az elkövető meg sem jelenik személyesen az információ fizikai tárolásának helyszínén, vagy akár az adott országban. A jelenséget súlyosbítja, hogy bizonyos térségekben szemet hunynak az illegális üzleti információgyűjtési módszerek fölött, mivel felismerték, hogy abból profitálnak a helyi vállalatok [5].

Az ipari kémkedés témakörében kevés a rendelkezésre álló magyar nyelvű szakirodalom. Ennek oka, hogy a probléma nehezen vizsgálható. A legtöbb esetben hónapok telnek el, mire észreveszi az adott szervezet, hogy valaki jogtalanul eltulajdonította és felhasználta az immateriális tulajdonát. Amennyiben felismeri, hogy ipari kémkedés történt, akkor sem biztos, hogy a szervezet jelenti az esetet annak negatív következményeitől tartva. Abban az esetben, ha hivatalos úton vizsgálják a történteket, az információt bizalmasan kezelik, ami megnehezíti, hogy átfogó kutatás készüljön a témáról. Magyarországon is hasonló fenyegetésekkel kell szembenézni a szervezeteknek, mint más fejlett országokban működő vállalatoknak. Hatalmas mennyiségű üzleti információt tárolnak digitalizálva, közvetlen internetes hozzáféréssel. Kockázatot jelent a mobiltelefonok és más okos eszközök jelenléte. Sok magyar gazdasági entitás nincs tisztában a szabadalmaztatás folyamatával, vagy nem képes megfizetni annak magas költségeit. Amennyiben a termék még fejlesztési folyamatban van,

a szabadalmaztatás kérdése még komplexebb, mivel az újdonság még változhat, majd a megújult terméket ismét szabadalmaztatni szükséges. Az ipari kémkedés kockázatát növelheti, hogy Magyarországon bizonyos tudásintenzív iparágakban kevés a kimagaslóan jó szakember, tudásuk megszerzéséért folyamatos a verseny a vállalatok között. A szervezet érintettjeinek elégedettsége, lojalitásának kérdése is kockázati tényező.

KUTATÁSI KÉRDÉSEK ÉS MÓDSZERTAN

Az elmúlt években az ipari kémkedés gyakoriságában, és az általa okozott negatív hatásokban jelentős növekedés volt megfigyelhető, amely már nem csak az egyéni szervezetre, hanem a teljes globális gazdaságra hatást gyakorol. A probléma kutatását indokolja, hogy jelenlegi környezetben az ipari kémkedés valós és magas kockázatot jelent a szervezeteknek. A vállalatok vezetői számára fontos a probléma felismerése, és megértése, hogy lépéseket tudjanak tenni a jövőbeni ipari kémkedésből eredő veszteségek elkerülése érdekében. A kutatás célja átfogó képet adni, hogy a magyar szervezetek mennyire vannak tudatában az ipari kémkedés veszélyének, milyen fokú kockázatként tartják számon, továbbá, hogy tesznek-e megelőző lépéseket a negatív hatások elkerülése érdekében.

A kvantitatív vizsgálat során a következő kutatási kérdések kerültek megfogalmazásra:

K1: A magyar szervezetek mennyire vannak tudatában az ipari kémkedés veszélyeinek?

K2: A magyar szervezetek tesznek-e preventív lépéseket az ipari kémkedés kockázatával szemben?

K3: A magyar szervezetek milyen fokú kockázatnak tartják az ipari kémkedést?

Az adatgyűjtés online és papír alapú kérdőívek alkalmazásával ment végbe. A papír alapú megoldás a kitöltési hajlandóság növelése érdekében történt. A szerzők tapasztalata alapján a papír alapú módszer adatgyűjtési szempontból hatékonyabb a kézből-kézbe történő átadás, továbbá a személyes kontaktus miatt. A mintába olyan szervezetek kerültek kiválasztásra, amelyeknél magas az innovációs hajlam. A kutatás szempontjából feltételezhető, hogy azok a szervezetek, amelyek a nyereséges működés érdekében időt és költségeket áldoznak az innovációs tevékenység támogatására, kiemelten vonzók a versenytársaknak, így magas az ipari kémkedés kockázata. Az innovatív szervezeteknél a versenyelőnyt biztosító üzleti információ áramoltatása és felhasználása része az operatív feladatok ellátásának, ami további információbiztonsági kockázatokat vet fel. A kutatás során az elsődleges cél a felső-, és középvezetők megkérdezése volt majd bevonásra kerültek az alkalmazottak, mivel egy teljesen más nézőpontot képviselnek a kutatás szempontjából. Bár a minta mérete (n=273) miatt az eredmény nem tekinthető reprezentatívnak, azonban szektor szempontjából heterogén összetétele okán a kutatás jó alapot ad további vizsgálati irányok definiálásához. A minta 12 szektort foglalt magában, melyeket az 1. táblázat ismertet a Demográfiai adatok fejezetben. A gyűjtött adatok SPSS szoftver alkalmazásával kerültek elemzésre.

SZAKIRODALMI ÁTTEKINTÉS

A digitális technológia innovációja soha nem látott ütemben haladt az elmúlt évtizedekben, melynek eredményeként ma már az Ipar 4.0 által definiált környezetben működnek a vállalatok. Ez a napjainkban is jellemző, dinamikusan változó technológiai környezet

a megszámlálhatatlan előnye mellett, számtalan negatív hatással befolyásolja a gazdaság szereplőit. Az Ipar 4.0 adaptálásának hajtőerői között azonosítható a termelékenység és hatékonyság növelésének lehetősége, a piaci verseny, a cégvezetés elvárásai, ugyanakkor figyelembe kell venni az előrehaladott digitalizáció teremtette ipari kémkedés új szintjét és kockázatait [6]. Az ipari kémkedés egy interdiszciplináris megközelítésű probléma, amelynek nincsen egy standard, általánosan elfogadott definíciója [1, 5, 7]. Az ipari kémkedés egy szervezet üzleti titkainak vagy más bizalmas információjának rossz szándékkal való engedély nélküli megszerzése [8], olyan illegális és etikátlan tevékenységeket foglal magában, amely során a szervezet szisztematikusan összegyűjti, elemzi és kezeli a versenytársakra vonatkozó információkat azzal a céllal, hogy versenyelőnyhöz jussanak velük szemben [9] Az ipari kémkedés célja üzleti titkok szerzése vállalatoktól vagy kormányzati szervektől, hogy egy másik vállalat vagy állam profitáljon belőle [7].

Az egyik legkritikusabb üzleti döntés, hogy az adott szervezet elkezdje-e tevékenységét egy bizonyos iparágban. Ma már bevett gyakorlatnak számít, hogy a vállalkozások értékes és bizalmas információkat gyűjtenek a célpiacon versenyző szervezetekről a piacra lépési döntés meghozatala előtt [10]. Az a piaci szereplő, amelyik elsőként képes adaptálni a piacon a legújabb digitális technológiát anélkül, hogy időt és forrásokat költenek kutatásra és fejlesztésre, potenciális globális előnyt élveznek magas költségek nélkül [11]. Az egyre kiélezettebb globális versenyben, ahol a vállalatot a rendkívül gyorsan változó piaci lehetőségekre reagálva képesek csak profitot termelni, az üzleti titkok, információ és szellemi termékek felhasználása és védelme kulcsfontosságú a siker szempontjából [5]. Abban az esetben amikor a szervezet sem belső forrásból, sem külső nyilvános (nyílt) forrásból nem képes vagy nem hajlandó erősfeszítéseket tenni a szükséges információ megszerzéséért, akkor folyamodik ipari kémkedéshez [12]. Az elkövető szempontjából az üzleti információ és innováció lopásának szignifikáns előnyei vannak a fejlesztéssel szemben. Nem csak az az előnye, hogy a minősített anyagok és innovációk hozzájárulnak a szervezet képességeinek a fejlesztéséhez, hanem az így megtakarított költségek átcsoportosíthatók egyéb gazdasági vagy társadalmi projektekre [13].

Ahogy egyszerűsödik a kivitelezés módja, azzal arányosan tapasztalható, hogy egyre több szervezet bátorodik fel élni a törtvényt sértő információszerzési módszerekkel [10]. A digitális forradalom okozta információbiztonsági kockázat nem csak abból ered, hogy a szervezetek hatalmas mennyiségű értékes információt tárolnak elektronikusan, és ezek a rendszerek csatlakoznak az internethez, hanem ennek hatására az ipari kémkedés sokkal biztonságosabb és kevesebb kockázatot jelent az elkövető számára [14]. A problémát tovább élezi, hogy a fejlődő országokban szemet hunynak az illegálisan szerzett üzleti intelligenciával való gazdálkodás fölött, mivel ráébredtek, hogy az növeli a térség gazdasági teljesítményét [5, 15]. Ezt felismerve a fejlett országok folyamatosan erőfeszítéseket tesznek a szellemi tulajdonjog védelmére vonatkozó törvényeik erősítésének érdekében, mivel ipari kémkedést motiváló tényezők között található a szellemi jogokat védő törvények gyengesége [16], továbbá az innováció szorosan összefügg a fejlődéssel, és meghatározó tényező az ország versenyképességének szempontjából [15]. Azonban a problémát tetézi, hogy egyre növekszik az állami szereplők részvétele a technológiák illegális eltulajdonításában [13]. A főbb szektorok, melyek leginkább ki vannak téve a kevésbé fejlett országok által támogatott ipari kémkedésnek a repülőipar, a telekommunikáció, a biotechnológia, energiaipar, az elektromos ipar, és a hadiipar [13, 16]. A jelenséget már lehetetlen az országok

önálló, koordinálatlan fellépéseivel kezelni, eredményeket elérni egy globális közösségként, közösen elfogadott stratégiát és szabályokat alkalmazva, holisztikusabb szemléleten keresztül lehetne [15].

Az ipari, gazdasági célú kémkedés egy súlyos bűncselekmény, amely zavaros és nehezen áttekinthető felépítése ellenére globálisan hatalmas materiális és immateriális károkat képes okozni a szervezeteknek, azonban jelenség elleni fellépések mégsem hoznak komolyabb előrelépést [17]. A szervezetek, melyek áldozatul esnek ennek az etikátlan tevékenységnek, a negatív hatásokról félve nem mutatnak hajlandóságot az eset jelentésére, ritkán történik meg az ipari kémkedés hivatalos úton való kezelése [7, 14]. A probléma annyira súlyos, hogy a számtalan nyilvánosságra kerülő ipari kémkedéssel kapcsolatos eset csak a jéghegy csúcsát teszi ki [18]. Akár elkövető, akár áldozat a szóban forgó szervezet, amennyiben az eset nyilvánosságra kerül, magas a kockázata, hogy elveszíti az érintettek bizalmát, ami a részvények árának esését okozhatja [14], ezenfelül az a tényező is visszatartja a szervezeteket az ipari kémkedés gyanújának jelentésétől, hogy a nyomozás esetleg más, általuk elkövetett illegális gyakorlatot is a felszínre hozhat [7]. Ezt igazolja, hogy a szervezetekre globálisan jellemző, hogy bármilyen összeget hajlandók megfizetni a lopott ipari, kereskedelmi és marketing titkokért a saját versenyképességük fenntartása érdekében [11]. Továbbá az is megnehezíti a tevékenység által okozott veszteség valós értékének meghatározását, hogy hónapok vagy évek telnek el, mire a szervezet észreveszi, hogy ipari kémkedés áldozatául esett. Amennyiben az ipari kémkedés esetének hivatalos kivizsgálására kerül sor, szigorúan korlátozó titoktartási szerződések kerülnek aláírásra, ami ebben az esetben azt jelenti, hogy az elkövető és az áldozat valós kiléte jellemzően nem kerül napvilágra [14].

Az üzleti információk és titkok jogtalan eltulajdonítására napról napra újabb és modernebb módszerek állnak az erre hajlandó gazdasági entitások rendelkezésére. Kétségtelen, hogy a tevékenység művészete és módszerei sokat változtak az évtizedek során, de a lényege változatlan maradt, avagy az ellopott információt nem védték megfelelően [19]. Az IT fejlődésével párhuzamosan fejlődtek a digitálisan tárolt anyagok védelmét biztosító szoftverek, azonban az információ védelmét nem szabad csak a digitálisan tárolt titkok védelmére korlátozni. Egy darab papírra leírt információ ellopása is hatalmas károkat képes okozni, mivel az ipari kémek gyakran dolgoznak információ morzsákból, ami nagyon fontossá teszi minden információ védelmét, függetlenül annak a tárolási módjától [1]. A legegyszerűbb módszer a nyílt forrású információk felhasználása, amelyek könnyen megszerezhetők többek között szakmai kiállításokon, a közösségi médiából vagy folyóiratokból. Klasszikus és hatékony taktikák a versenytárs szemetét átnézni értékes információkat keresve, a konkurencia termékének megvásárlása és lemásolása, vagy a munkavégzés helyszínén elhelyezett fizikai eszközzel való megfigyelés [7]. A szervezeteknél az üzleti titkokat általában olyan eszközökön tárolják, amelyekhez hozzá lehet férni az interneten keresztül, ezt használják ki kibernetikus bűnözők és kémek a rendszerek feltörésével, akiknek a kiléte gyakran ismeretlen marad [19]. Az információ védelem során a leggyengébb láncszem a humán tényező az emberi természet komplexitásának köszönhetően, bár ez egy kevéssé kutatott terület, mivel a probléma kutatói a legtöbb esetben technológiai megközelítésből vizsgálják az ipari kémkedést [20]. Az ipari kémkedés egyik legetikátlanabb módszere a belső munkatársak felhasználásával való üzleti titok megszerzésére, amelynek eszközei lehetnek kényszerítés, megvesztegetés vagy zsarolás [7, 19].

EREDMÉNYEK

Demográfiai adatok

A kutatás során elemzett adatok gyűjtése kérdőív alkalmazásával történt. Olyan magyar vállalkozások kerültek a mintavétel során kiválasztásra, ahol jellemző a K+F tevékenység és magas az innovációs hajlam, mivel feltételezhetően ezen a területen a legnagyobb a gazdasági célú ipari kémkedés kockázata. A vizsgálat első szakaszában a vállalatok vezetőinek megkérdezése történt, majd a következő fázisban az alkalmazottak kerültek megkérdezésre, mivel egy egészen más nézőpontot képviselnek a probléma feltárása során. A minta nagysága n=273 fő, amelyben 49% a közép- vagy felsővezető, és 47% alkalmazott, amely jó, kiegyensúlyozott arányt mutat. A kitöltők többsége, 119 fő nagyvállalkozásnál dolgozik, 90 főt foglalkoztatnak kisvállalkozások, csak 34 fő képviselte a középvállalkozásokat. A szektor megválasztása során az innovációs hajlam volt a fő szempont, továbbá azt is követelményt határoztuk meg, hogy több ágazattól történjen az adatgyűjtés, ami megfigyelhető az eredményekben is. Az 1. táblázat a megnevezett iparágakból beérkezett válaszok számát ismerteti.

Szektor	Beérkezett válaszok száma (N=273)
Autóipar	42
Gép- és műszeripar	35
Bank- és pénzügyi szektor	31
Kiskereskedelem és disztribúció	29
Szolgáltatás	29
Hadiipar	27
Információs technológia és telekommunikáció	25
Vegyi- és gyógyszeripar	18
Technológia	17
Egészségügy és biotechnológia	9
Közszféra	7
Ingatlan	4

1. táblázat: A kutatás során megkérdezett szektorok
Forrás:Saját szerkesztés, 2021, n=273

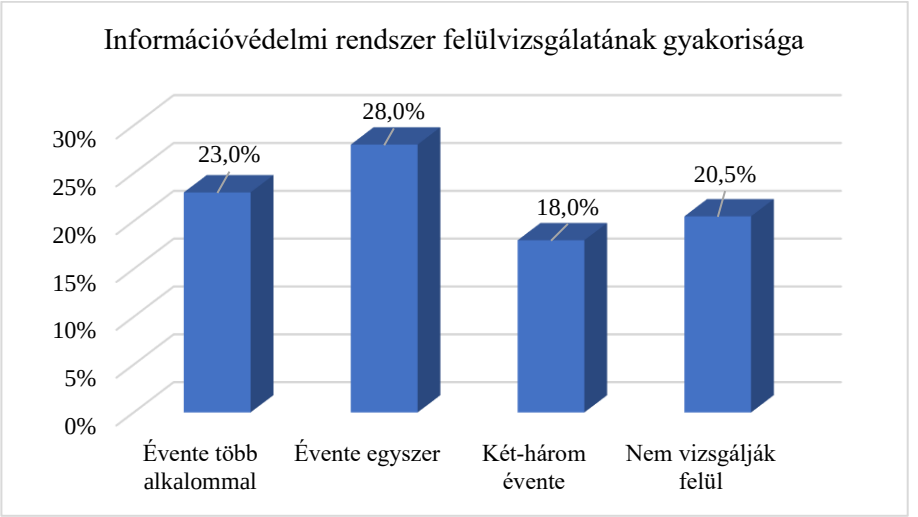
Az információvédelem humán aspektusai

A kutatás során feltárásra került, hogy a vállalatok rendelkeznek-e írott biztonságpolitikával, mivel ez keretrendszert ad a szervezet információvédelmi eszközeinek. A megkérdezettek 80%-a válaszolta, hogy a szervezet rendelkezik írott biztonságpolitikával. A nagyvállalatok 82%-a, középvállalatok 61%-a, a kisvállalatok 85%-a alkalmaz biztonságpolitikai előírásokat. A vállalkozás mérete és az írott biztonságpolitika megléte közötti kapcsolat Pearson féle khi-négyzet próbával vizsgálva közepes erősségű szignifikáns kapcsolatot mutat (χ^2= 59,267, p=0,000, Cramer's V=0,474, n=264), azaz a vállalat mérete befolyással van az írott biztonságpolitika alkalmazására. Az eredmények azt mutatták, hogy minél nagyobb a vállalkozás mérete, annál gyakoribb az írott biztonságpolitika alkalmazása. Az eredmények arra is rávilágítottak, hogy az írott biztonságpolitika megléte magában foglalja a munkavállalókkal kötött titoktartási szerződést is. A titoktartási szerződés alapvető eszköz a munkaadó kezében, mivel az ipari kémkedés legkritikusabb és legnehezebben

kontrollálható módszere a belső alkalmazottak által szándékosan elkövetett információlopás és átadás a piac egyéb szereplőjének, bár hatékonysága megkérdőjelezhető. A kutatásban résztvevő szervezetek csak 28%-ban vizsgálják a munkatárs hátterét, mielőtt hozzáférést adnak az üzleti titkokhoz és információkhoz. A nagyvállalkozások 41%-ban, a középvállalkozások 40%-ban, a kisvállalkozások 8%-ban vizsgálják a munkatársak előéletét, a megkérdezettek 18%-a jelölte a „*nem tudom*" választ a kérdésben. A khi-négyzet próba eredménye szerint a szervezet mérete és a munkatársak hátterének vizsgálata között közepesnél gyengébb szignifikáns kapcsolat van (χ^2= 59,768, p=0,000, Cramer's V=0,335, n=266), a nagyobb létszámú szervezeteknél feltételezhetően gyakoribb a háttérvizsgálat elvégzése, mielőtt hozzáférést adnak a munkatársaknak a bizalmas üzleti információkhoz.

Bár az eredmények alapján a szervezetek 80%-a rendelkezik biztonságpolitikai szabályzattal, alig több, mint a fele, 51% vizsgálja felül a rendszer aktualitását évente legalább egyszer. A rendszeres, gyakori felülvizsgálat fontossága a dinamikusan változó technológiai környezet fejlődésével arányosan növekszik, Pearson féle khi-négyzetpróba eredménye alapján a vállalat mérete és a felülvizsgálat gyakorisága között gyenge szignifikáns kapcsolat található (χ^2= 53,697, p=0,000, Cramer's V=0,259, n=266). A 2. ábra ismerteti a felülvizsgálat gyakoriságát százalékban kifejezve.

A felülvizsgálat mellett az alkalmazottak és a vezetőség folyamatos képzése és az ipari kémkedés kockázatára való felkészítése is kiemelten fontos információbiztonsági szempontból. Függetlenül attól, hogy szándékosan elkövetett cselekedet vagy véletlen hiba folytán, de a belső humán tényező legtöbb esetben hozzájárul az ipari kémkedés kockázatának növekedéséhez. Képzéssel a véletlen kialakult helyzetek jelentősen visszaszoríthatók, amit felismertek a magyar szervezetek, ugyanis a válaszadók 64%-a évente legalább egy alkalommal képzi a munkavállalókat az üzleti titkok biztonságos használatáról és tárolásáról. A kisvállalkozások 15%-a, a közepes vállalkozások 18%-a, a nagy vállalkozások 13%-a tart információbiztonsági képzést a belső érintetteknek évente egynél több alkalommal. . A vállalkozás mérete és a képzés gyakorisága közötti kapcsolat Pearson féle khi-négyzet próbával vizsgálva közepesnél gyengébb szignifikáns kapcsolatot mutat (χ^2= 115,191, p=0,000, Cramer's V=0,325, n=264).



2.ábra: Az információvédelmi rendszer aktualitás felülvizsgálatának gyakorisága
Forrás: Saját szerkesztés, 2021, n=266

Információvédelmi eszközök

A kutatás során feltárásra kerültek a szervezetek fizikai beléptető megoldásai. Az ipari kémkedés szempontjából a beléptető rendszer feladata az illetéktelen behatolások elleni védelem. A kutatásban résztvevő magyar szervezetek 79,5%-a alkalmaz beléptető rendszert a munkavégzés helyszínén, amelynek jelentős része, 72%-a belépőkártya. A megkérdezett alkalmazottak 70,5%-a tartja az alkalmazott beléptetőrendszert biztonságosnak, ezzel szemben a vezetők csak 43%-ban. A megkérdezett pozíciója és a véleménye között a kérdésben, khi-négyzetpróba eredménye alapján közepesnél gyengébb szignifikáns kapcsolat van (χ^2= 29,393; p=0,000; Cramer's V=0,332; n=264), a Kendall féle tau-b mutató (τ_b=-0,186; p=0,000) szignifikáns negatív kapcsolatot jelez, vagyis az alkalmazottak szerint biztonságosabb a beléptető rendszer, mint a vezetők véleménye alapján. A kapott eredményből az a következtetés vonható le, hogy a vizsgált probléma szempontjából a vezetőket nagyobb felelősség terheli, hogy megvédjék a szervezet versenyelőnyét biztosító üzleti információt, így számukra relevánsabb kérdés a beléptető rendszer megbízhatósága. A válaszadók 21%-a nem alkalmaz beléptető rendszert, amely megnöveli a külső behatoló általi információ lopás kockázatát. A kutatásban résztvevő kis- és középvállalkozások 27%-ban, a nagyvállalkozások 6%-ban nem alkalmaznak beléptető rendszert, a vállalkozás mérete és a beléptető alkalmazása között a khi-négyzetpróba eredménye alapján közepes erősségű szignifikáns kapcsolat van (χ^2= 128,978; p=0,000; Cramer's V=0,402; n=252), amely arra mutat rá, hogy a nagyobb méretű szervezeteknél jellemzőbb a beléptető rendszer alkalmazása.

A munkavégzéshez használt számítógépek védelmére 95%-ban használnak jelszót a megkérdezett szervezetek. A vizsgálat kiterjedt a szervezetek által alkalmazott titkosított adattátolási módszerekre, a kérdésben a Pearson féle khi-négyzet értéke χ^2= 80,635; p=0,000. A vizsgálat eredményeit a 2. táblázat ismerteti.

Vállalkozás mérete	Titkos adattárolás eszköze				
	Felhő	Külső eszköz	Szerver	Számítógép	**Összesítve**
Egyéni vállalkozó	2	8	15	15	**18**
Kisvállalkozás	37	29	48	15	**82**
Középvállalkozás	13	6	35	6	**35**
Nagyvállalkozás	55	53	95	33	**116**
Összesítve	**107**	**96**	**193**	**69**	**251**

2. táblázat: A szervezetek által alkalmazott titkosított adattárolási megoldások.
Forrás: Saját szerkesztés, 2021, n=251

A 2. táblázatban ismertetett eredmények összehasonlító értékelését a 3. táblázat ismerteti. A megkérdezett egyéni vállalkozók az adatok titkosított tárolására használnak külső eszközt és szervert is, azonban leggyakrabban az üzleti információ számítógépen való titkosított tárolását részesítik előnyben. A kisvállalkozások titkosított adattárolási megoldásainál nem található szignifikáns különbség. A középvállalkozások a szerveren való tárolást alkalmazzák leggyakrabban. A vizsgált nagyvállalkozások titkosított adattárolási megoldásai között nem található szignifikáns különbség, a megkérdezett eszközöket jellemzően alkalmazzák.

Vállalkozás mérete	Titkos adattárolás eszköze			
	Felhő (A)	Külső eszköz (B)	Szerver (C)	Számítógép (D)
Egyéni vállalkozó		A	A	ABC
Kisvállalkozás				
Középvállalkozás			B	
Nagyvállalkozás				

3. táblázat: A szervezetek által alkalmazott titkosított adattárolási megoldások összehasonlítása.
Forrás: Saját szerkesztés, 2021, n=251

A gyűjtött adatok elemzése során készült olyan vizsgálat, amelybe bevonásra kerültek a „*nem alkalmazunk titkosított adattárolási eszközt*” válaszok. A vizsgálat során készült összehasonlító elemzésben az egyéni vállalkozók bár leggyakrabban a számítógépen való titkosított adattárolási megoldást alkalmazzák, a külső eszköz és a szerver mellett hasonló arányban jelent meg a nem alkalmaznak ilyen megoldást válasz. A kisvállalkozók esetében a nem alkalmaznak titkosított adattárolási megoldást volt a szignifikánsan leggyakrabban előforduló válasz. Ez az eredmény azonban nem azt jelenti, hogy a kisebb létszámú szervezetek nincsenek tisztában az ipari kémkedés kockázatával, hanem a szervezetek infrastruktúrájának kiépítettségére vonatkozóan lehet következtetéseket levonni.

A szervezetek 92%-ban biztosítanak mobil eszközöket a munkavégzéshez, amelyeket ugyanebben az arányban használhatnak a munkatársak az otthonukban. Ez a megoldás bár az ipari kémkedés szempontjából kockázatos, az megemlítendő, hogy az adatfelvétel időszaka során a COVID-19 járvány miatt a magyar szervezetek jelentős részében volt otthoni munkavégzés. A válaszadók 80 %-a tarthatja magánál a magán mobiltelefonját bekapcsolt állapotban tárgyalások, meetingek alkalmával. A jelenlegi gazdasági környezetben, amikor a mobiltelefonok egy olyan ablakot nyitnak, amelyen át külső szereplők betekinthetnek, és azonnal tudomást szerezhetnek a szervezeten belüli innovációs tevékenységről, a

mobiltelefonok jelenléte tárgyalásokon és megbeszéléseken kiemelt kockázatot jelent az ipari kémkedés szempontjából.

Az eredmények elemzése során összehasonlításra került a vezetők és az alkalmazottak véleménye a vizsgált problémával kapcsolatban, mely pontos eredményeit a 4. táblázat ismerteti. A vezetők fele, 51%-a gondolja úgy, hogy a szervezet biztonságosan tárolja az üzleti titkokat és információt, a megkérdezett alkalmazottak 82%-a szerint biztonságos az alkalmazott adattárolási megoldás. A kérdésben a khi-négyzet próba eredménye közepesnél gyengébb erősségű kapcsolatot mutat (χ^2= 36,675; p=0,000; Cramer's V=0,376; n=259), a Kendall féle tau-b mutató (τ_b=-0,335; p=0,000) szignifikáns negatív kapcsolatot jelez.

A megkérdezett közép- és felsővezetők 25%-a tartja magas kockázatnak, hogy a piac szereplői ellopják és felhasználják a szervezet versenyelőnyét biztosító üzleti információt és titkokat, az alkalmazottak a vezetőknél többen, 41%-ban tartják magas kockázatnak a definiált problémát. A megkérdezettek véleményében az ipari kémkedés kockázatáról a khi-négyzet próba eredménye szintén közepesnél gyengébb kapcsolatot mutat (χ^2= 20,797; p=0,000; Cramer's V=0,283; n=259), a Kendall féle tau-b mutató (τ_b=-0,221; p=0,000) szignifikáns negatív kapcsolatot mutat.

A vezetők 52%-a szerint a szervezet képes kivédeni egy ellenük irányuló ipari kémkedési kísérletet. Az alkalmazottak a vezetőknél magasabb arányban, 67%-ban gondolják úgy, hogy a szervezet fel van készülve a külső, információlopás céljából megkísérelt támadásokra. A megkérdezettek véleménye között a szervezet felkészültségéről közepesnél gyengébb szignifikáns kapcsolat mutatható ki (χ^2= 24,052; p=0,000; Cramer's V=0,305; n=259), a Kendall féle tau-b mutató (τ_b=-0,207; p=0,000) szignifikáns negatív kapcsolatot jelez.

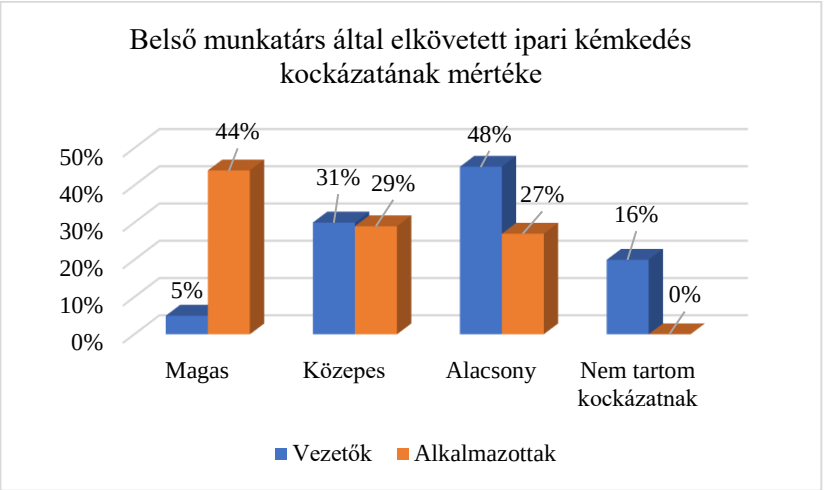
A vezetők jelentős többsége, 90%-a nyilatkozta, hogy a szervezet még nem esett áldozatul ipari kémkedésnek. Ez a magas arány igazolja a [7, 14] kutatási eredményt, mely szerint amennyiben a vezetőség tisztában van a ténnyel, hogy ipari kémkedést követtek el a szervezet ellen, abban az esetben is törekednek arra, hogy ez ne kerüljön nyilvánosságra a számtalan lehetséges negatív következmény elkerülése érdekében. A vezetők 10%-a, az alkalmazottak 29%-a gondolja úgy, hogy követtek már el ipari kémkedést a szervezet ellen. A kérdésben, hogy a szervezett esett-e már áldozatul ipari kémkedésnek, szintén közepesnél gyengébb szignifikáns kapcsolat található (χ^2= 15,519; p=0,004; Cramer's V=0,245; n=259), a Kendall féle tau-b mutató (τ_b=-0,126; p=0,026) szignifikáns negatív kapcsolatot jelez.

Állítás	Vezetők (N= 133 fő)	Alkalmazottak (N=126 fő)	Pearson χ^2	Cramer's V	Kendall's tau-b
A szervezet biztonságosan tárolja az üzleti titkokat és információkat.	51% szerint igen.	82% szerint igen	36,675 p=0,000	0,376 p=0,000	-0,335 p=0,000
A szervezet potenciális külső fenyegetésként tartja számon, hogy a versenytársak ellopják és felhasználják az üzleti információkat és titkokat.	25% szerint potenciális kockázat.	41 % szerint potenciális kockázat.	20,797 p=0,000	0,283 p=0,000	-0,221 p=0,000
A szervezet fel van készülve az ipari kémkedés kivédésére.	52% szerint igen.	67% szerint igen.	24,052 p=0,000	0,305 p=0,000	-0,207 p=0,000
A szervezet esett már áldozatul ipari kémkedésnek.	10% szerint igen.	29% szerint igen.	15,519 p=0,004	0,245 p=0,004	-0,126 p=0,026

4. táblázat: A vezetők és alkalmazottak válaszainak összehasonlítása
Forrás: Saját szerkesztés, 2021, n=273

Szervezeten belüli ipari kémkedés

A magyar szervezetek körében végzett kutatás során felmérésre került, hogy a közép- és felsővezetők, továbbá az alkalmazottak hogyan viszonyulnak a belső érintett által elkövetett ipari kémkedés kérdéséhez. Az információvédelmi rendszer leggyengébb láncszeme az emberi tényező, továbbá az ipari kémkedés nagy gyakorisággal egy belső személy közbenjárásával történik [7, 19, 20]. A két megkérdezett csoport válaszaiban jelentős eltérés tapasztalható, amelyet a 4. ábra ismertet. A megkérdezettek pozíciója és a belső érintettekbe vetett bizalom között Pearson féle khi-négyzet próbával végzett tesz eredménye alapján közepesen erős szignifikáns kapcsolat található (χ^2= 76,724; p=0,000; Cramer's V=0,542; n=259), a Kendall féle tau-b mutató (τ_b=-0,480; p=0,000) szignifikáns negatív kapcsolatot jelez. Az eredményből feltételezhető, hogy a vezetők megbíznak a szervezet belső érintettjeiben, az alkalmazottak többsége kevésbé, azonban a probléma mélyebb megértéséhez további kutatások szükségesek. A belső személy által elkövetett szándékos információlopást a vezetőség csak 5%-a, ezzel szemben az alkalmazottak 44%-a tartja potenciális fenyegetésnek. A vezetők 20%-a egyáltalán nem tartja a belső személy által elkövetett ipari kémkedést veszélynek, az alkalmazottak ezt a kérdést mind besorolták valamilyen fokú kockázatnak.



4. ábra: Belső munkatársak által elkövetett ipari kémkedés kockázatának mértéke
Forrás: Saját szerkesztés, 2021, n=259

KÖVETKEZTETÉSEK

Jelen kutatás során az ipari kémkedés fogalma a következőképpen került definiálásra: a versenytársak üzleti titkainak etikátlan vagy illegális eszközökkel való megszerzése, melynek a céljai a saját versenyképesség növelése és a K+F+I tevékenységek költség- és időigényének csökkentése. Az ipari kémkedés bár egyidős a gazdaság fogalmával, eszközrendszere jelentős fejlődésen ment keresztül, aminek eredményeként bármely entitás számára elérhető, amely hajlandó élni ezzel az eszközzel. Az egyre kiélezettebb gazdasági versenyben és a gyorsan változó piaci viszonyok között csak az a szervezet tud életben maradni, amely azonnal képes reagálni a környezetére, aminek kulcsa az információ. A vizsgálat során három kutatási kérdést került megfogalmazásra, melyek a következők:

K1: A magyar szervezetek mennyire vannak tudatában az ipari kémkedés veszélyeinek?

K2: A magyar szervezetek tesznek-e preventív lépéseket az ipari kémkedés kockázatával szemben?

K3: A magyar szervezetek milyen fokú kockázatnak tartják az ipari kémkedést?

A kutatás eredményei alapján a **K1** kutatás kérdés esetén a magyar szervezetek tudatában vannak az ipari kémkedés jelentette külső fenyegetésnek. Erre utal a rendszeresített biztonságpolitika, a munkatársak képzése, és az alkalmazott információbiztonsági megoldások. Azonban az eredményekből az a következtetés vonható le, hogy az emberi tényező jelentette belső fenyegetést a vállalatok vezetői nem tartják potenciális kockázatnak. Bár általában titoktartási szerződést kötnek, de nem végeznek háttérvizsgálatot a személyeken, mielőtt hozzáférést kapnak az üzleti információhoz. A megkérdezett vezetők több mint a fele egyáltalán nem, vagy alacsony kockázatnak tartja a belső ipari kémkedést. A **K2** kutatási kérdés esetén elmondható, hogy a magyar szervezetek törekednek az ipari kémkedés megelőzésére. Alkalmaznak információvédelmi megoldásokat, melyeket időközönként felülvizsgálnak. Jellemző, hogy az alkalmazott rendszerek használatára oktatják az érintett

személyeket. A kutatás eredményei rávilágítottak, hogy a nagy vállalatok több információvédelmi eszközt alkalmaznak a gyakorlatban mint a magyar kis- és középvállalkozások. Ez nem minden esetben enged arra következtetni, hogy a kisebb vállalatok nincsenek tudatában az ipari kémkedés veszélyének, hanem gyakran a probléma hátterében financiális, gazdasági okok és döntések találhatók. A **K3** a szervezet által érzékelt kockázat mértékére vonatkozik. A különböző kockázatok elemzése, azonosítása és csoportosítása a menedzsment feladata, akik meghatározzák annak valószínűségét és a szervezetre gyakorolt lehetséges hatását. A biztonsági rendszer nem túl gyakori felülvizsgálata, továbbá a hasonló arányú képzések arra engednek következtetni, hogy a magyar szervezetek nem tartják magas kockázatnak az ipari kémkedést. A megkérdezett vezetők fele úgy gondolja, hogy a szervezet biztonságosan tárolja az információt, továbbá fel van készülve egy esetleges ipari kémkedés kivédésére, továbbá csak a megkérdezettek 25%-a tartja számon potenciális kockázatként a szervezet ellen irányuló információlopást. A belső érintett általi ipari kémkedést a vezetők alacsony, míg az alkalmazottak magasabb kockázatnak tartják.

KONKLÚZIÓ ÉS JAVASLATOK

Az ipari kémkedés Magyarországon is fenyegeti az innovatív szervezeteket, amely több okra vezethető vissza. A K+F+I tevékenységek hosszú és költséges folyamata pénzés időgazdálkodás szempontjából is megterheli a szervezeteket. A piacon megszerzett pozíciót megtartani, vagy növelni viszont csak versenyképes üzleti információval lehetséges. Ezek a tényezők teszik az etikátlan vagy illegális módszerekkel való információszerzést olyan vonzóvá bizonyos piaci szereplők számára. Amennyiben a szervezet versenyelőnyt biztosító üzleti információja a piacon jelenlevő másik szereplő kezébe kerül, az rendkívül súlyos anyagi és hírnévbeli károkat okozhat. A kutatás eredményei alapján a nagyobb szervezetek jellemzően több információvédelmi eszközt alkalmaznak, mint a kisebb vállalkozások. Ez azonban nem arra enged következtetni, hogy a kis- és közép vállalkozások nincsenek tudatában az ipari kémkedés jelentette fenyegetésnek, hanem financiális döntéseik során jellemzően a profit termelő tényezőket helyezik előterébe az információ védelmi beruházásokkal szemben.

Az ipari kémkedés vizsgálatánál a munkavállalók elégedettsége és lojalitása is fontos tényező. Egy külső szereplő által megtervezett ipari kémkedési kísérlet, mely során anyagi- vagy egyéb jellegű kompenzációval próbál egy belső szereplőt rávenni információátadásra, az emberi természetből fakadóan magas kockázatot jelent egy innovatív szervezetnek, amelyet nem szabad figyelmen kívül hagyni. A tudás specializálódásának eredményeként egyes ágazatokban a szakemberek értéke rendkívül megnövekedett, tudásukból hiány van a piacon. A titoktartási szerződés, mint információvédelmi eszköz, elterjed Magyarországon, de megszegése gyakran nem bizonyítható, nem szankcionálható. A problémát még komplexebbé teszi, amennyiben a magyar vállalat egy külföldi szakembert foglalkoztat, és vele szemben merül fel az ipari kémkedés gyanúja. A teljeskörű biztonsághoz javasolnánk az üzleti információhoz hozzáférő belső érintettek tevékenységének folyamatos monitorozását. Jellemző a szervezetekre, hogy az ipari kémkedés kockázatának vizsgálatakor az információs technológiai nézőpontot helyezik előtérbe, ezzel szemben javasoljuk, hogy a problémakört minél komplexebb, a humán tényezőt is magába foglaló szempontból vizsgálják. A szigetszerű információbiztonsági megoldások helyett a kutatás eredményei alapján javasoljuk a komplex, átfogó rendszerek alkalmazását. Azoknak a szervezeteknek,

amelyek jelentős értékű innovatív üzleti információt hoznak létre, tárolnak és használnak fel a munkavégzés során javasoljuk az alkalmazott információbiztonsági rendszer legalább negyedévenkénti felülvizsgálatát, és a belső érintettek oktatását, továbbá felkészítését az esetleges információbiztonsági támadásokra.

Az eredmények arra engednek következtetni, hogy a vezetők megbíznak a szervezet belső érintettjeiben, azonban az alkalmazottak többsége kevésbé. A probléma mélyebb megértéséhez további kutatások szükségesek, amely olyan tényezőket foglal magában, mint a válaszadók személyisége, és az őket körülvevő szervezeti kultúra. Az eredmény érdekes, mert a két megkérdezett csoport különböző nézőpontból vizsgálja a munkavégzés mindennapos rutinját. Feltételezve, hogy az alkalmazottak számára több lehetőség adódik megfigyelni a belső érintetteket a munkavégzés során, mint a vezetőség tagjainak, arra enged következtetni, hogy a vezetőkre jellemző a szervezeti vakság. A kérdésben a megkérdezettek neme és a belső érintettekbe vetett bizalom között elhanyagolható erősségű kapcsolat van.

A vizsgálat során az adatfelvétel 2021 tavaszán történt. A kutatás végzésének időpontjában a munkavégzés gyakorlata, Magyarországon és globálisan egyaránt, az új körülményekhez alkalmazkodva változáson megy keresztül. A megjósolható, de pontosan nem előrejelezhető változások újfajta biztonsági fenyegetéseket hoznak, amire válaszul új biztonsági megoldások születnek. A szervezet folyamatos működését és versenyképességét biztosító üzleti intelligencia védelme kiemelten fontos, függetlenül attól, hogy a munkavégzés irodában, telephelyen, gyárban, vagy amely munkakörökben ez lehetséges, otthoni körülmények között történik. Az otthoni munkavégzés számos új információbiztonsági kockázattal szembesítette a vállalatokat, akár interneten, felhőn vagy fizikai adattározón szállítják a munkavégzéshez szükséges adatokat a munkatársak. Az ipari kémkedés szempontjából ez a digitális és a fizikai adatlopást is egyszerűsítette, amely kivédésére komplex információbiztonsági rendszerek alkalmazása szükséges.

IRODALOMJEGYZÉK

[1] B. Wimmer, Business Espionage: Risks, Threats, and Countermeasures, 1. szerk., Oxford: Elsevier, 2015.

[2] S. Rose, For all the tea in China: how England stole the world's favourite drink and changed history, 1. szerk., Westminster: Penguin, 2010.

[3] W. C. Hannas, J. Mulvenon és A. B. Puglisi, Chinese Industrial Espionage, Technology Acquisition and Military Modernization, 1. szerk., London: Routledge, 2013.

[4] M. K. Lewis, „Criminalizing China," 2021. [Online]. Available: https://scholarlycommons.law.northwestern.edu/jclc/vol111/iss1/3. [Hozzáférés dátuma: 12. Szeptember 2021].

[5] T. Hou és V. Wang, „Industrial espionage –A systematic literature review (SLR)," *Computers & Security,* 98. kötet, pp. 1-12, 2020.

[6] L. Szerb, É. Komlósi és B. Páger, „Új Technológiai Cégek az Ipar 4.0 Küszöbén – A Magyar Digitális Vállalkozási Ökoszisztéma Szakértői Értékelése,"

Vezetéstudomány / Budapest Management Review, 51. kötet, 6. szám, pp. 81-96, 2020.

[7] M. Button, „Economic and industrial espionage," *Security Journal,* 33. kötet, pp. 1-5, 2020.

[8] D. A. Jameson, „The Rhetoric of Industrial Espionage: The Case of Starwood V. Hilton," *Business Communication Quarterly,* 74. kötet, 3. szám, pp. 289-297, 2011.

[9] A. Vashisth és A. Kumar, „Corporate espionage The insider threat," *Business Information Review,* 30. kötet, 2. szám, pp. 83-90, 2013.

[10] A. Barrachina, Y. Tauman és A. Urbano, „Entry with two correlated signals: the case of industrial espionage and its positive competitive effects," *International Journal of Game Theory,* 50. kötet, pp. 241–278, 2021.

[11] Y. B. Choi és W. Teresa, „The Rise of Industrial Espionage and How to Prevent It," *International Journal of Cyber Research and Education,* 2. kötet, 2. szám, pp. 9-16, 2020.

[12] E. M. Roche, „Industrial Espionage," 2016. [Online]. Available: https://www.afio.com/publications/ROCHE_Industrial_Espionage_from_AFIO_INTEL_SPRING2016_Vol22_no1.pdf. [Hozzáférés dátuma: 14. Augusztus 2021].

[13] M. Pellegrino, „The threat of state-sponsored industrial espionage," 2015. [Online]. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_26_Industrial_espionage.pdf. [Hozzáférés dátuma: 25. Szeptember 2021].

[14] K. Solberg, „Economic and Industrial Espionage at the Start of the 21st Century - Status Quaestionis," *Journal of Intelligence Studies in Business,*6. kötet, 3. szám, pp. 51-64, 2016.

[15] C. Konopatsch, „Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland," *Security Journal,* 33. kötet, pp. 83-118, 2020.

[16] S.-K. Kim, „Intellectual property right infringement, state involvement in industrialespionage, and North-South trade," *Economic Modelling,* 91. kötet, pp. 110-116, 2020.

[17] S. Knickmeier, „Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries," *Security Journal,* 33. kötet, pp. 6-26, 2020.

[18] I. I. Androulidakis és F. –. E. Kioupakis, Industrial Espionage and Technical Surveillance Counter Measurers, 1. szerk., Switzerland: Springer International Publishing, 2016.

[19] N. Duckworth és E. De Silva, „Teaching New Dogs Old Tricks: The Basics of Espionage Transcend Time," *National Security: Breakthroughs in Research and Practice,* pp. 479-496, 2019.

[20] D. Ashenden, „In their own words: employee attitudes towards information security," *Information and Computer Security,* 26. kötet, 3. szám, pp. 327-337, 2018.

IMPACT OF CORONAVIRUS EPIDEMIC ON THE GLOBAL SUPPLY CHAIN

KORONAVÍRUS JÁRVÁNY HATÁSA A GLOBÁLIS ELLÁTÁSI LÁNCRA

SZALÁNCZI-ORBÁN Virág[1]

Abstract

The coronavirus epidemic has highlighted the complexity of international supply chains and their system of cross-border dependence, as well as the fragility of global supply chains. In the recent past, many new challenges and unforeseen problems have made the daily lives of players in the logistics sector more difficult. The new changed environment called for quick solutions. In addition to quick solutions, forward-looking, well-thought-out, short- and long-term strategies and solutions and new directions must be defined. The coronavirus epidemic has highlighted some of the problems and challenges to be addressed, the fragility of the systems at the time. The aim of this study is to explore the main causes of supply chain fragility during the coronavirus epidemic and the impact of recent measures on global supply chains, the challenges faced by players in the logistics sector and the solutions and changes in the sector.

Keywords

supply chain, coronavirus, stock shortage, fragility, reconsidered supply chain

Absztrakt

A koronavírus járvány rávilágított a nemzetközi ellátási láncok összetettségére és azok határokon átívelő függési rendszerére, valamint a globális ellátási láncok törékenységére. Az elmúlt időszakban rengeteg új kihívás és előre nem látható probléma nehezítette a logisztikai szektor szereplőinek mindennapjait. Az új megváltozott környezet gyors megoldásokat kívánt. A gyors megoldások mellett, előremutató, átgondolt, rövid és hosszútávú stratégiát és megoldásokat, új irányvonalakat kell meghatározni. A koronavirus járvány rávilágított néhány problémára és megoldandó feladatra, az akkori és régi rendszerek törékenységére. A tanulmány célja feltárja az ellátási lánc törékenységének fő okait a koronavírus járvány idején, és azt, hogy a globális ellátási láncokra milyen hatással voltak az elmúlt időszak intézkedései, milyen problémákkal szembesültek a logisztikai szektor szereplői valamint milyen megoldások és változtatások alakultak a szektorban.

Kulcsszavak

ellátási lánc, koronavírus, készlethiány, törékenység, újragondolt ellátási lánc

[1] szalancziorban.virag@uni-obuda.hu | ORCID: 0000-0002-1073-2788 | doctoral candidate, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

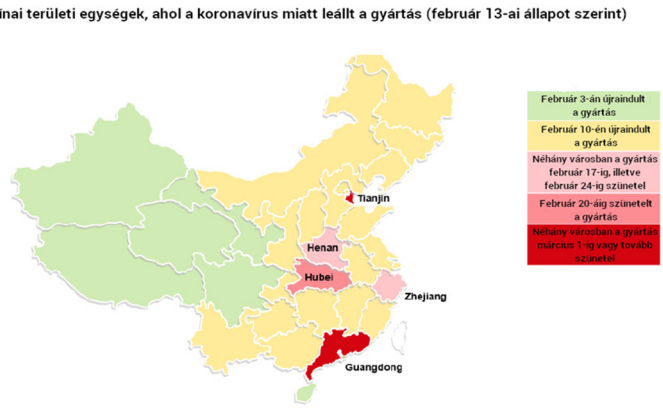
BEVEZETÉS

A COVID-19 vagy a koronavírus-járvány jelentős fennakadásokat okozott a globális ellátási láncokban. Ez az új helyzet rengeteg kihívás elé állította globális, regionális és helyi piac szereplőit. Az ellátási láncok törékenyek. A folyamatos helyzetértékelések és folyamatos változások gyors reagálást és újragondolt megoldásokat, újragondolt ellátási láncokat eredményeztek. Ez a folyamat mai napig érzékelhető és elmondható, hogy a koronavírus járvány miatti változások befolyásolják mindennapjainkat és formáló erővel bírnak a jövő globális ellátási láncaira és azok megoldásaira. Ebben a tanulmányban célom feltárni a járvány kitörése utáni állapotokat és fontosabb dilemmákat, megoldandó helyzeteket, melyek elvezettek az újragondolt ellátási láncokhoz. A vezető vállalatok és a globális piac szereplőinek megoldásai jelentősen változtatták meg az ellátási láncokat és azok jövőben való alakulását. Az elmúlt időszak tanulságai és megoldáskeresései, a piaci változások jelenleg is zajlanak és következtetések vonhatóak le arra vonatkozóan, hogy ennek az ágazatnak milyen lehetőségei, milyen iránymutatásai lehetnek. Célom ezen megoldások, ezen átrendeződések feltárása, valamint következtetések levonása.

KÍNA SZEREPE A KEZDETEKBEN

A világ nem először szembesül az ellátási láncok zavaraival. Kereskedelmi háborúk, éghajlati események, szabályozások és szabályozási változások, túloptimalizálás, nehéz átláthatóság is előre nem látható problémákat gördítettek az ágazati szereplőkre [1]. A COVID-19 vagy a koronavírus-járvány kitörésekor az első fontos helyszín Kína volt. Kína és Délkelet-Ázsia régiójára a világ számos vállalata támaszkodik termelési és ellátási lánc szempontból.

A járvány kitörésének gócpontja Vuhan egyben ipari és szállítási csomópont, egy olyan tartományi főváros, mely a kínai GDP 4%-ának előállításáért felelős. Az itt elrendelt első korlátozások (áruk és emberek szabad mozgását érintő korlátozások) gyorsan átterjedtek Kína más tartományaiba is (1.ábra). A nem létfontosságú árukat előállító gyárakat lezárták, fontos centrumok, ipari létesítmények Kína egész területén érintetté váltak és zavart okoztak a komplex logisztikai rendszerben. [2]



1.ábra: Kína területi egységei a koronavírus járvány okozta leállás idején [3]

Akkor még nem tudhattuk, hogy a járvány milyen hatással lesz a globális ellátási láncokra, milyen gyorsan lehet megfékezni, milyen problémákkal kell majd szembesülnie a világ többi részének is. Sejthető volt, hogy sok szektorban (autóipar, értékesítés, gyógyszeripar) lesznek fennakadások vagy jelentősebb problémák. A probléma gyökere a kínai importtól és exporttól való függőség, a komplex rendszerben való jelentős részvétel. [4]

A járvány globális üzleti hatásainak felmérésére a Dun & Bradstreet készített egy speciális tájékoztatót. A koronavírus járvány üzleti hatását vizsgálták Kínában, mely szerint bizonyos iparág kiemelkedően érintett, de a globális vállalkozások érintettégi köre is jelentős. Fő érintett iparágak a szolgáltatások, gyártás és a nagykereskedelem., ezen kívül a kis és mikovállalkozásokat érintette a járvány súlyosabban. [5]

Mivel a kínai beszállítók nem voltak képesek termékeket és anyagokat szállítani az elvárt ütemben így a kezdeti hatás a függőségi kapcsolatok miatt elérte a globális piacot is és egye hullámot indított el a komplex ellátási láncok ökoszisztémájában. [6]

Egy másik felmérésből megtudhatjuk, hogy ebben a kezdeti időszakban Kínában és a határain átnyúló kereskedelmi tevékenység több mint a felére csökkent, a kínai belföldi és nemzetközi tranzakciók volumene először 17%-al csökkent, melynek ok a már említett járvány terjeszkedést megelőző intézkedések (gyárlezárások, korlátozások) voltak. A teljes kereskedelmi aktivitás a régióban később 50-60%-al csökkent, majd a kínai és nemzetközi cégek közötti tranzakciók száma 50%-al csökkent. [7]

Ezek az események és fennakadások indították el azt a folyamatot, amit globális szinten érzékeltünk és az ellátási láncok zavarát okozták.

ELLÁTÁSI LÁNCOK TÖRÉKENYSÉGE

Tudjuk, hogy a probléma gyökere a kínai export-importtól való függőség. Az ellátási láncok törékenyek. Nem csak a függőségi kapcsolatok miatt, mivel ez a rendszer is egy komplex rendszer, egy komplex hálózat így több tényező és ok is befolyásolja annak működését és esetleges fennakadásait, zavarait. Ezen okok és problémák közül öt fő okot jelölnék meg:

- Csökkentett készletek, időben történő gyártás
- Merev ellátási láncok
- Manuális ellátási lánc menedzsment
- Átláthatóság hiánya
- Konszolidált termelési központok

Csökkentett készletek és készletszintek megjelenésének röviden ismertetett oka, hogy a vállalatok a hatékonyság és költségoptimalizálás érdekében időben történő gyártásra rendezkedtek be. Egy olyan nem várt helyzetben, mint a koronavírus okozta fennakadások és lezárások a vállaltoknak gyorsan kellett változtatniuk a stratégiáikon és gyártási metódusaikon. Az időben történő gyártás esetében kevésbé rugalmas a rendszer az ilyen jellegű hirtelen helyzetek kezelésére, így az ellátáshiány komoly problémákat okozott.

Merev ellátási láncok az előbb említett hirtelen eseményen bekövetkező fennakadások kezelése miatt fontos. Mivel akadozott és rugalmatlan volt az ellátási lánc, a vállalatoknak a megszokott és bevált beszállítóin kívül más alternatívák után kellett nézniük. Amennyiben a vállalatok mereven ragaszkodnak a saját hálózatukhoz, úgy egy ilyen váratlan helyzetben nehezen találnak alternatívákat, illetve ezen alternatívák felkutatása több időt vesz igénybe, ami hatást gyakorol és gyakorolt a termelésre.

Az ellátási menedzsment is tekinthető merev rendszernek sok vállalat esetében, ennek egyik fő oka, hogy manuálisan kezelik azt. Minden változtatás hosszadalmas és összetett feladat, ezért egy merev manuálisabb rendszer kevésbé tudja kezelni ezeket. A rugalmasság és a digitális eszközök használata kulcskérdés.

Az átláthatóságának hiánya. Az ellátási láncok átláthatósága és teljes nyomon követése, illetve annak hiánya is fő okként határozható meg abban, hogy a koronavírus járvány miatti fennakadások milyen mélységekben okoztak problémát a globális ellátási láncban. Amennyiben egy vállalat nem tudja az ellátási lánc rétegeit átláthatóvá tenni, nem tudja termelési kapacitását maximálisan átlátni, úgy az ilyen helyzetek proaktív kezelése is sok időt vesz igénybe.

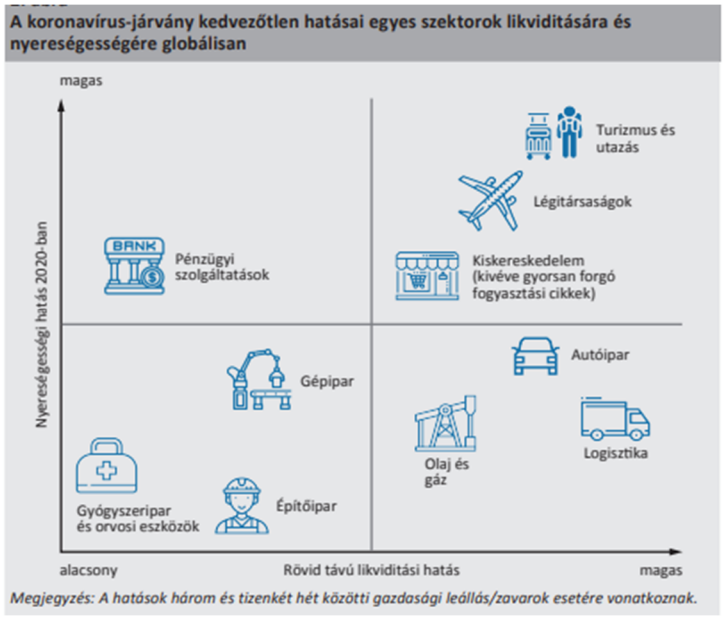
Konszolidált termelési központok problémája, a függőség. Az ellátási lánc globalizációja során különböző területet, régiók, országcsoportok specializálódtak és termelési zónák alakultak ki. Így egyes országok, területek akár városok lettek kulcs fontosságúak a termelésben és ellátásban. Jól látható, hogy egyes területek kiesése, mint Kína kezdeti szerepe, hogyan befolyásolta a globális ellátási láncot. [8]

A KORONAVÍRUS JÁRVÁNY HATÁSA A GLOBÁLIS ELLÁTÁSI LÁNCRA ÉS MAGYARORSZÁGRA

A koronavírus járványig a vállalatok inkább az időben történő gyártásra, a hatékonyság és a költségcsökkentés kérdéseire fókuszáltak. Mondhatni berendezkedtek egy folytonos, kiszámítható és kevésbé változékony állapotba, mely jelentős biztonságot okozott a vállalatoknál nem is gondolva vagy készülve arra, hogy egy előre nem várt globális esemény kockázata komoly fennakadásokat okozna a logisztikai rendszerekben, az ellátásban és a globális termelésben. A járvány miatti megváltozott helyzet erről a rugalmatlanabbnak mondott állapotból a hangsúlyt a rugalmasság felé helyezte.

Ennek a gazdasági válságnak a bonyolultsága abban gyökerezik, hogy ez nem egy gazdasági oldalról indult válság, hanem egy egészségügyi válság következménye. Szokatlan és váratlan helyzet elé állítva a globális piacot. Az ellátási láncokat ez a válság azonnal érintette és egyszerre jelent meg keresleti és kínálati probléma. Az ellátási láncok kimaradtak, vagy korlátozottak voltak, termeléskiesések, beszállítói problémák, felgyülemlett szállítmányok jelentkeztek.

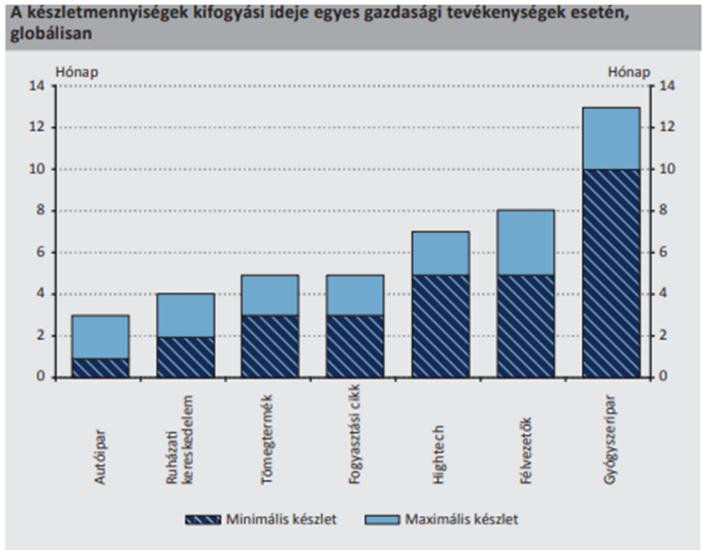
A járvány gazdasági hatásai bár globálisak voltak, mégis voltak területek melyeket jobban és voltak olyan területek, amelyeket kevésbé érintett a járvány gazdasági hatása. A járványkezelés során hozott intézkedések és folyamatok több szektort befolyásoltak és érintettek. Likviditási és nyereségességi szempontból leginkább érintett a légiközlekedés, turisztika, kiskereskedelem, járműipar, logisztikai szektor (2.ábra).



2. ábra: Koronavírus járvány hatása az egyes szektorokban [9]

Összetett és komplex hatások jelentek meg, melyek a globális termelés és ellátási lánc egészét megrázták és befolyásolták. A globális piac szereplői igyekeztek a lehetőségekhez képest is mihamarabb visszaállni a járvány előtti állapotra, a termelést, ellátást és gyártást fokozatosan növelni, új megoldásokat találni.

A korábban említett időben történő gyártási rendszer problémája, az ellátási láncok akadozása vagy kimaradása jelentős gondot okozott a készletmennyiségek optimalizálásban és szinten tartásában.



3. ábra: Készletmennyiségek kifutási ideje [10]

A 3. ábrán jól láthatjuk, hogy bizonyos szektorok milyen tartalékokkal, raktárkészletekkel rendelkeztek és rendelkeznek. A minimális készlet az a készlet, amivel átlagosan rendelkeznek ezek az iparágak. Jól látható, hogy egyes iparágak készletszintjei rövid időre elegendőek, így ezek iparágakat érzékenyebben érintette a válság és a beszállítói problémák.

Az ellátási láncokon is megtalálható keresleti és kínálati probléma a globális gazdaság egészét érintette. A vállalatok jelentős üzleti és működési zavarokkal szembesültek. Ebben a váratlan és szokatlan helyzetben gyorsan kellett reagálni. A rugalmasság tehát kulcstényező lett a járvány időszakában. Az egyes régiók és országok hamar felismerték, hogy a járvány gazdasági hatása milyen területeket fog érinteni leginkább, igy a járványkezelés és a gazdasági válság kezelése a kormányzatokkal együttesen történt.

Magyarországot is érzékenyen érintette a minden ágazatra kiterjedő válsághelyzet. Hazánkban húzóágazatnak számító autóipart is gyorsan elérte a járvány miatti fennakadás. Kapacitásproblémák és ellátási lánc zavarok jelentek meg hazánkban is. Többi országhoz hasonlóan hazánkban is a gazdasági szereplők és a kormányzat együttműködésével a legfontosabb teendők közé tartozott a gyors reagálás, a rövidtávú hatékony válságkezelés, és a hosszútávú logisztikai fejlesztések megalkotása. A koronavírus járvány miatti gazdasági fennakadások és zavarok minden országot hasonlóan érintettek, a válságkezelés nagy része globálisan történt. Hazánkban is komoly problémát okozott logisztikai területen az ellátási láncok akadozása, kiesése. A logisztikai szektor szerepkőinek továbbá komoly gondot okozott a kisvállalkozások megmentése, a munkaerőkiesés kezelése. A logisztikai szektor adminisztratív szabályozása, az elektronikus rendszerekre való áttérés, az általában vett digitális képességek elmaradottsága is okozott jelentősebb fennakadásokat, valamint jelentős probléma mutatkozott a fizetőképességekkel is. [11]

A korábban már említett készlet és termelési problémákon és kiváltó okokon kívül, más tényezők is nehezítették a gazdasági válság enyhítését. Mivel a gazdasági válság kiváltó oka egy egészségügyi vészhelyzet, komoly problémát okozott minden szektorban a munkaerő kiesése. A határ és légtérlezárások is jelentősen korlátozták a szabad mozgást. Például a turisztikai szektor jelentős kiesésre számíthatott. A szabad mozgás korlátozásának és a bevezetett járványügyi intézkedések hatására az online kereskedelem és online szolgáltatások egyre nagyobb szerepet kaptak. Több vállalat és kereskedelmi cég ált át online szolgáltatások nyújtására és az online ügyintézés lehetőségére. Gondolok itt például a vendéglátóipari egységek kiszállítási, házhoz szállítási szolgáltatásra való átállására, a kereskedelmi egységek, boltok ugyancsak házhoz szállításra való átállására, banki és egyéb szolgáltatások online ügyintézésre. A globális válság szereplői nemcsak globálisan keresték a megoldást a járvány kezelésére, hanem helyspecifikusan is kezelniük kellett a fennálló problémákat. A világjárvány okozta nyersanyag és munkaerőhiány, a járványkezelés és a járványhelyzet alapvetően változtatta meg a vállalati és kormányzati stratégiákat.

ELLÁTÁSI LÁNC ÉS JÁRVÁNYKEZELÉS AKTUALITÁSAI

A koronavírus járvány okozta gazdasági válság alapvetően és alapjaiban változtathatja meg az ellátási láncot és logisztikai szektor szereplőinek stratégiáját. A korábbi termelési és gyártási metódusok, a készletezés, a szállítás, az átláthatóság és függőségi rendszer újratervezése nem elkerülhető. A válság hatásait és kezelésének módjait elemezni szük-

séges. A régóta bevált gyakorlatok elhagyása, a rugalmasság és a digitális képességek fejlesztése sokkal nagyobb szerephez jut a jövőben. A koronavírus járvány az automatizálásra való igényt is jelentősen felerősítette.

A jelenlegi járvány okozta gazdasági válságon még nem vagyunk túl, így bizonytalanság érezhető. A járványkezelés folyamatos. A helyreállítás és a válság hatásának lecsengése és a visszarendezős fokozatos. Azonban ebben a jelenlegi helyzetben is már elmozdulásokat és tendenciákat tudunk felfedezni. A vállalkozások nagy része képes volt alkalmazkodni a változásokhoz, melyhez az ellátási láncuk elemzése fontos segítség volt. A gazdaságújraindító tervek és előrejelzések, az eddig levont tapasztalatok támpontot adhatnak arra vonatkozóan, hogy az ellátási láncokban és a logisztikai szektorban milyen területeken lehet változás.

Azonban a koronavírus járvány okozta gazdasági válság mellett más befolyásoló tényezők is alakítják a logisztikai szektor változásait és az ellátási láncok reformját valamint a korábbi függőségi rendszerek változását. Ilyen befolyásoló tényezők és aktualitások például:

- Áfamentesség: megszűnt a harmadik országból, tehát nem EU tagországból érkező áruk áfa-mentessége.
- A Brexit hatása
- A Szuezi csatorna gazdasági jelentősége

Ezen hatások együttese és főleg a koronavírus járvány miatti egyedülálló helyzet is okot ad arra, hogy a különböző rendszerek és folyamatok változásokra való reagálását felülvizsgáljuk. A közelmúlt eseményeiből le kell vonnunk a tanulságokat és elemezni kell az eredményeket, amiket a jövőre való felkészüléshez felhasználhatunk.

GLOBÁLIS ELLÁTÁSI LÁNCOK JÖVŐJE

A globális ellátási láncok jövőjét jelenleg több hatás is befolyásolja. Egyértelmű cél a vállalkozások támogatása és a munkahelyek megőrzése. A gazdasági növekedés elérése. Az ellátási láncok törékenységeként felsorolt öt jellemző ok és probléma területén is jelentős változásokra lehet számítani. Véleményem szerint az alábbi néhány területeken jelentős változás várható:

- Digitális fejlődés, átláthatóság, automatizáció
  Manuális megoldások helyett a digitális megoldásokra való átállás, a digitális kultúra fejlesztése kulcskérdés. A digitalizáció és az automatizáció bevezetése átalakító hatással van egy vállalatra és ellátási láncra is. A folyton növekvő igények naprakész digitális technológiákat és hálózatokat kívánnak. A folyamatok átláthatóságának digitalizálása elengedhetetlen. A rugalmasságot és hatékonyságot a robosztus hálózatok alkalmazása, a felhőalapú adatkezelés, az automatizálás és a kiberbiztonság fokozása növelheti tovább. Az ellátási láncokhoz kapcsolódó vállalatoknak egyre több naprakész adatra, egyre magasabb fokú átláthatóságra, gyorsaságra és rugalmasságra lesz szüksége.
- Készletezés, beszerzési hálózatok újragondolása
  A készletezési minimumok újragondolása, nagyobb készlettartalékok fenntartása mindenképpen várható lépés lehet a vállalatok és a gazdasági szektor résztvevőinél.

A készletezési stratégia mellett a beszerzési stratégia átgondolása, a függőségi viszonyok átrendeződése és a beszerzési források diverzifikálása lehet a cél.

- Kína szerepének csökkentése
  Világszinten sok vállalat függ és támaszkodik Kínára és Délkelet-Ázsiára. Ennek a függőségnek a csökkentése cél lehet a jövőben. A vállalatoknak újra kell gondolniuk az ellátási láncukat és fontóra venni más beruházási lehetőségeket.
- Ellátási láncok lerövidítése
  Az ellátási láncok rövidítése és regionalizálása valamint beszállítói bázis központúvá tétele is várható változás lehet az ellátási láncok. [12]

ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

A meglévő ellátási láncok megváltozása és változtatása nem egyszerű feladat. Mindamellett, hogy valamilyen reakció és változás várható az ellátási láncokban és a logisztikai szektorban ezen változások rövid és hosszútávú elemzése a továbbiakban is elengedhetetlen. Bizonyos hibák és problémák feltárása, a folyamatok újragondolása mindenképpen egy várható lépés. Fontos, hogy továbbra is törekedni kell a költséghatékonysági törekvések megvalósulására. A közeljövőben várható, hogy a vállalatok és a szektor szereplői több területen is változtatásokat fognak eszközölni és megfontolni, aminek átalakító hatása lesz a globális ellátási láncokra. A rugalmasság, a szerteágazóbb beszállítói bázis keresése, a készletezési stratégia átgondolása, a költséghatékony és átlátható ellátási láncok kialakítása rövid távú feladat. Kulcskompetencia lesz továbbá a digitális eszközök használata és megléte, valamint az automatizálásra való átállás, a digitalizáció fokozása. Több forgatókönyv és több modell is várható. Az elindult fejlesztések és folyamatokat nyomon kell követni és elemezni kell azok hatását és eredményét. Megállapítható hogy a járvány előtti állapotokhoz nem lehet visszatérni és mindenképpen az ellátási láncok és a logisztikai szektor újragondolásán lesz a cél.

IRODALOMJEGYZÉK

[1] Hedwall, Mattias. The ongoing impact of COVID-19 on global supply chains. Világgazdasági Fórum. 2020. június 22. [online] Available: https://www.weforum.org/agenda/2020/06/ongoing-impact-covid-19-global-supply-chains/ letöltés ideje: 2021.07.13.

[2] Brown, Sara. Reshoring, restructuring, and the future of supply chains. MIT Sloan School of Management. 2020, [online] Available: https://www2.deloitte.com/content/dam/insights/articles/emea-164529-after-the-crisis/DI_After-the-crisis.pdf , letöltés ideje: 2020. július 22.

[3] Portfolio- Megkongatták a vészharangokat a koronavírus miatt – Veszélyben a globális ellátási lánc, 2020 [online] Available: https://www.portfolio.hu/uzlet/20200227/megkongattak-a-veszharangokat-a-koronavirus-miatt-veszelyben-a-globalis-ellatasi-lanc-417201, letöltés ideje: 2021. február 27.

[4] PwC – Covid19: Az ellátási lánc védelme, 2021 [online] Available: https://www.pwc.com/hu/hu/covid-19/mukodesi-ellatasi-lanc/koronavirus-ellatasi-lanc-vedelme.html , letöltés ideje: 2021.06.03.

[5] The Dun & Bradstreet,: The Worldwide Business Impact of the Coronavirus, 2021, [online] Available: https://www.dnb.com/perspectives/supply-chain/coronavirus-business-impact.html, letöltés ideje: 2021.08.12.
[6] Mikkel Hippe Brun, Supplychaindigital, Coronavirus and the antifragile supply chain, 2020 [online] Available: https://supplychaindigital.com/supply-chain-2/coronavirus-and-antifragile-supply-chain, letöltés ideje: 2021.04.17.
[7] Businesswire: Tradeshift Sees Chinese Trade Activity Drop 56% on a Week by Week Basis as Coronavirus Hits Global Supply Chains, 2020 [online] Available: https://www.businesswire.com/news/home/20200305005305/en/Tradeshift-Sees-Chinese-Trade-Activity-Drop-56, letöltés ideje: 2021.05.12.
[8] Mikkel Hippe Brun, Supplychaindigital, Coronavirus and the antifragile supply chain, [online] Available: https://supplychaindigital.com/supply-chain-2/coronavirus-and-antifragile-supply-chain, letöltés ideje: 2021.04.17.
[9] Husmann Róbert, Hitelintézeti Szemle, 19. évf. 3. szám, 2020. szeptember, 130–153. o. A globális ellátási láncok átalakulása a feldolgozóiparban a koronavírus-járvány következtében
[10] Jaubert Szilvia, Supply Chain Monitor,2020. június-július: Exkluzív interjú dr. Chikán Attila közgazdász professzorral a koronavírus gazdasági hatásairól, [online] Available: https://www.scmonitor.hu/cikk/20200619/koronavirus-es-az-ellatasi-lancok, letöltés ideje: 2021.07.11.
[11] Alicke, Gupta és Trautwein, 2020, Alicke, Knut Richa Gupta, és Vera Trautwein. Resetting supply chains for the next normal. McKinsey & Company., letöltés ideje: 2021.06.12.
[12] Szalánczi-Orbán Virág, „Magyarország és az Európai Unió közlekedési hálózatának fejlesztése és annak logisztikai hatása," Külügyi Műhely, pp. 7-19, 2019.

STUDY ON SPORT FACILITIES IN REGARDING THE CONTRIBUTION OF MATCH OFFICIALS

SPORTLÉTESÍTMÉNYEK VIZSGÁLATA A HIVATALOS SZEMÉLYEK KÖZREMŰKÖDÉSÉNEK SZEMPONTJÁBÓL

DOLNEGÓ Bálint[1] – GÉCZI Gábor[2]

Abstract

The sports federations are responsible for the management of the sports. However, in team sports, the match organisers are the sports organisations. The federation delegates officials to the venues, to ensure that matches are properly organised. In our study, we investigated how the federations regulate the infrastructural conditions in which officials are required to work, regarding the sports of ice hockey, handball and football, and also how the sports organisations implement the regulations. We carried out a primary research among representatives of sports organisations, conducting structured interviews with match officials of first division teams, N=9 persons. As a secondary research, We examined the regulations of the federations using a document analysis method. The results showed that among the domestic federations, football is the one with the most elaborated regulations, and handball the least. Safety issues are the most regulated and the sports organisations place the greatest emphasis on this. can also have an impact on the outcome of the match.

Keywords

sports federation, match officials, referee, regulation

Absztrakt

A sportágak gondozásáért a sportági szövetségek felelősek. A csapatsportágakban azonban a mérkőzések szervezői a sportszervezetek. A szövetség a mérkőzések szabályszerű megrendezése érdekében hivatalos személyeket delegál a helyszínekre. Kutatásunkban során kíváncsiak voltunk, vajon a jégkorong, a kézilabda és a labdarúgás sportágakban a szövetségek milyen módon szabályozzák a hivatalos személyek számára munkavégzésükhöz biztosítandó infrastrukturális feltételeket? Továbbá kíváncsiak voltunk, hogyan valósítják meg az előírásokat a sportszervezetek. Primer kutatást végeztünk a sportszervezetek képviselőinek körében, első osztályú csapatok mérkőzésrendezésért felelős munkatársaival készítettünk strukturált interjút, N=9 fő. Szekunder kutatásként pedig a szövetségek szabályzatait vizsgáltuk dokumentumelemzés módszerrel. Az eredmények során kiderült, hogy a hazai szövetségek közül a labdarúgó az, amelynek szabályzata a leginkább kidolgozott, a kézilabdáé a legkevésbé. Leginkább a biztonsági kérdések szabályozottak és a sportszervezetek is erre fektetik a legnagyobb hangsúlyt.

Kulcsszavak

sportszövetség, hivatalos személyek, játékvezető, szabályzat

[1] dolnego.balint@tf.hu | ORCID: 0000-0002-8110-5052 | University of Physical Education Department of Sport Management, assistant lecturer | egyetemi tanársegéd, Testnevelési Egyetem Sportmenedzsment Tanszék
[2] gabor@tf.hu | ORCID: 0000-0002-6996-1550 | professor, University of Physical Education Department of Sport Management | egyetemi tanár, Testnevelési Egyetem Sportmenedzsment Tanszék

BEVEZETÉS

Ahhoz, hogy bármilyen sporttevékenységet végezzünk, sportlétesítményekre van szükségünk. A sportlétesítmények speciális létesítmények több szempontból is. Mindenekelőtt a biztonsági szempontokat kell figyelembe venni. A versenysport létrehozását számos kiszolgáló tevékenység is támogatja, amelyek elhelyezésére szintén gondolni kell. A versenyeken, mérkőzéseken versenybírók vagy játékvezetők működnek közre, szükség van orvosi ellátás biztosítására alkalmas helyiségre, csak hogy néhányat említsünk. Sokszor már az utánpótlás versenyeken is megjelennek nézők, rendszerint a szülők. Az egyre magasabb rangú versenyeken egyre több néző jelenik meg érdeklődőként. Ahol pedig sok ember gyülekezik, kiemelten kell a biztonságuk megőrzésére figyelni. A csapatsportágak esetén a sportág és a társadalom kultúrájától függően pedig sokszor ellenérdekeltek a szurkolók, a másik fél szurkolóit is ellenfélként kezelik és viták alakulnak ki. Továbbá a látványsportokban a televízió és más médiumok is jelen vannak és így az ő igényeiket is ki kell szolgálni, hiszen a bevételek az ő tevékenységükhöz is köthetők. Mindezeket összegezve látható, hogy a sportlétesítményeket úgy kell tervezni, megépíteni és üzemeltetni, hogy az érintetteket úgy szolgálja ki a lehető legmagasabb szinten, hogy azok biztonságát és egészségmegőrzését garantálja.

A fentiek biztosításáról hazai és nemzetközi jogforrások is gondoskodnak. Egy adott nemzet törvényekben és rendeletekben szabályozza a sportlétesítmények létrehozásának és üzemeltetésének feltételeit, elsősorban a biztonságos igénybevételre fókuszálva. Azonban minden sportág más és más sportszakmai igénnyel bír, illetve eltérő normák és trendek tapasztalhatók. Egy sportág gondozására a nemzetközi sportági szakszövetség hivatott, amelyeknek kontinentális és nemzeti képviseletei is működnek. Ezek hierarchikus rendszerében is szabályozzák a sportlétesítményekkel kapcsolatos kérdéseket. Itt már a biztonsági szempontok és a nézők kiszolgálása mellett sportszakmai érdekek is előkerülnek. A szabályzatok betartását a szövetségnek kell felügyelni, mint a sportág képviseletének.

A sportági szövetségek, mint a versenyrendszerek működtetői, nemcsak a létesítmények szabályszerű üzemeltetésével foglalkoznak, hanem más szabályok tekintetében is gondoskodnak a sportág képviseletéről. Bár a versenyrendszer üzemeltetéséért a szövetség a felelős, a versenyszervezés már a sportszervezetek feladata, hiszen ők adják a helyszínt egy versenyre vagy mérkőzésre. Ezért a sportági szövetségek képviselőket, úgynevezett hivatalos személyeket delegálnak. A játékszabályok betartásáért játékvezetőt, az ő munkájuk ellenőrzésére játékvezető-ellenőrt küldenek a mérkőzésekre. A szövetségi szabályzatok betartásának ellenőrzésére szövetségi ellenőröket foglalkoztatnak, de küldhetnek biztonsági ellenőröket, helyszíni menedzsereket, videóbírókat is, függően a verseny professzionalizáltságának szintjétől. Az ő munkájuk elvégzéséhez szükséges feltételeket a sportszervezetknek kell biztosítani. Mindezt úgy kell tenniük, hogy a biztonságuk ne forogjon veszélyben. Mindez számos feladatot ró a verseny szervezőire.

A látványsportágakban, a nagy helyszíni- és médiaérdeklődésre való tekintettel több funkcióban is közreműködhetnek hivatalos személyek. Feladatuk a biztonsági kérdések mellett kiterjedhet arra is, hogy a sportági verseny lebonyolítása illeszkedjen a szövetség célkitűzéseihez. Kutatásunkban a jégkorong, a kézilabda és a labdarúgás sportágak hazai első osztályú mérkőzésein vizsgáljuk azt, hogy a hivatalos személyek fogadása és kiszolgálása hogyan valósul meg a létesítményüzemeltetők és a sportszervezetek részéről.

IRODALMI ÁTTEKINTÉS

Versenyek és versenyrendszerek jellemzői a hivatalos személyek és a sportlétesítmények fókuszában

A látványsport sport sava-borsa a verseny. A verseny azonban akkor izgalmas és érdekes a néző számára, ha a résztvevők számára egyenlő feltételeket biztosítanak és bizonytalan a kimenete. Fontos azonban, hogy a bizonytalanság sportteljesítményből fakadjon [1]. Simth és Westerbeek [2] szerint a versenyeket az alábbi szempontok alapján jellemezhetünk: Formátum, Hierarchia, Multiplicitás, Tagság, Kormányzás, Munkaerő, Pénzügyek, Disztribúció, Integráció, Professzionalizáció. Kutatásunk témájához a versenyeket a kormányzás és a professzionalizáció alapján vizsgáljuk. A kormányzás szempontjából a versenyt irányító és szabályozó szervezetet, illetve az irányítás módját vizsgáljuk. A professzionalizáció kapcsán pedig azt, hogy az adott verseny résztvevői (sportolók, sportszakemberek, a versenyt működtetők és egyéb kiszolgáló személyzet) mennyire hivatásszerűen végzik a tevékenységüket. Magyarországon az országos sportági szakszövetségek látják el ezt a funkciót, amelyek civil szervezetek, tehát demokratikus működésűek és alulról szerveződve jönnek létre. A jégkorong sportágban a Magyar Jégkorong Szövetség (továbbiakban MJSZ), a kézilabdában a Magyar Kézilabda Szövetség (MKSZ), a labdarúgásban pedig a Magyar Labdarúgó Szövetség (továbbiakban MLSZ) a kormányzó szervezetek a sportágban. A hatályos, 2004. évi I. törvény a sportról (továbbiakban sporttörvény) az országos sportági szakszövetségek kapcsán az alábbi módon rendelkezik: *22. § (1) A szakszövetség alapvető feladata:*

- *a) szabályzatok kiadásával biztosítani a sportág rendeltetésszerű és a nemzetközi sportszövetsége szabályzatainak megfelelő működését,*

Vagyis az országos sportági szakszövetségnek feladata a versenyrendszer kialakítása, szabályozása és működtetése. Ezek mellett azonban további feladata a versenyrendszer ellenőrzése is a sporttörvény szerint.: *a 23. § (1) bekezdés d) pontja szerinti szabályzatában meghatározottak alapján ellenőrizni az adott sportág versenyrendszerében szervezett, vagy versenynaptárában egyébként szereplő sportrendezvények biztonságos lebonyolítását [3].*

Bár a jogtulajdonos az adott országos sportági szakszövetség, a sportversenyek szervezői a sportszervezetek, a helyszínük pedig a sportszervezetek sportlétesítményei. A sportszervezeteknek tehát az országos sportági szakszövetség szabályzatai szerint kell megszervezniük és lebonyolítaniuk a versenyeket és mérkőzéseket. A szabályzatok betartásának biztosítására pedig hivatalos személyeket (match officals) delegálhatnak a mérkőzésekre. Ezek funkciói sportáganként eltérő lehet, hivatalos személyeknek nevezzük azokat a sportszakembereket, akiket a szövetség egy feladat ellátására delegál a sportrendezvényre.

A sporttörvény a létesítményekkel kapcsolatos szabályzatok kidolgozását is az országos sportági szakszövetségek feladatai közé sorolja a 21 § 2 bekezdésében, *e) meghatározza a sportlétesítmények használatával, illetve a sporteseményekkel kapcsolatos sportági követelményeket [3].* A sporttörvényben a sportlétesítményekkel kapcsolatos rendelkezések is találhatók. A szövetségek feladatai közé delegálja a sportversenyek helyszínéül szolgáló létesítmények ellenőrzését. *63§ (4) Sportlétesítményben sportszövetségi versenyt rendezni csak a sportszövetség által évente az első verseny megkezdése előtt kiadott engedély alapján lehet. Az engedély megtagadásával szemben az üzemeltető a sportszövetség elnökségénél*

15 napon belül panasszal élhet [3]. Sportlétesítmény a törvény definíciója szerint*: 73§ s) sportlétesítmény: sportrendezvény megrendezésének helyszínéül szolgáló építmény és terület,*

Az országos sportági szakszövetségek sportlétesítményeivel kapcsolatos szabályzatok hivatalos személyeket érintő kivonata

A jégkorong sportágban a szövetség az MJSZ Infrastruktúra szabályzata [4] című szabályzatban rendelkezik arról, hogy a sportlétesítményekben milyen feltételeket kell biztosítani a hivatalos személyek számára. A zsűritagok részére szükséges biztosítani egy ún, zsűrifülkét, amelynek hosszúsága minimum 5,5 m, szélessége 15m, amelyet körbe kell keríteni, hogy illetékesek ne léphessenek be. A létesítményben orvosi szobát is szükséges kialakítani, amelynél szintén előírják, hogy higiénikus környezetet kell biztosítani. Az Erste Liga versenyszabályzata is rendelkezik arról milyen feltételeket szükséges biztosítani a játékvezetők részére. A szabályzat szintén előírja a zárható öltözőt, amelyet legalább 120 perccel a mérkőzés kezdete előtt biztosítani kell. Rendelkezik továbbá arról, hogy a szervezőnek biztosítani kell a játékvezető öltöző előtti folyosószakaszt úgy, hogy a mérkőzés előtt 60 perccel valamint a mérkőzést követő 30 percig csak a Játékvezetői Testület képviselője, a szövetségi ellenőr, a Versenyiroda képviselője és a közreműködő egyesület versenybírósági tagjai léphessenek be. A IIHF Ice Rink Guide [5] dokumentumában a játékvezetők számára minimum 20 m2-es öltözőt ír elő. Ezeket külön mellékhelyiséggel és zuhanyzóval kell ellátni. Az öltözőkben általánosan minimum 20˚C-ot kell biztosítani, illetve 300 LUX fényerőt.

Az MLSZ a sportlétesítményekre vonatkozó követelményeket az önálló, Infrastruktúra [6] szabályzatban rögzíti. A szabályzat a játékvezetői öltöző kapcsán előírja, hogy a harmadosztályú pályákig 2 db helyiség biztosítása kötelező, amelyek zárhatók, kellően megvilágítottak, továbbá a szabályzat a kulturált öltözködési és tisztálkodási lehetőségek biztosításáról is rendelkezik. A stadionban ki kell alakítani orvosi szobát, amelynek a csapatöltözők közelében és a játékos kijáróhoz minél közelebb kell lennie. Az orvosi szoba felszereltsége: 1 db vizsgálóágy, 1 db hordágy, 1 db üvegszekrény, 1 db oxigénpalack (maszkkal), 1 db vérnyomásmérő, 1 db telefonkészülék, 1 db újraélesztő készülék, 1 db hűtőszekrény. A stadionban kötelező Dopping ellenőrző szoba kialakítása is. Olyan helyen kell kialakítani a szobát, amely nem érhető el a nyilvánosság és a média részéről. Az alapterületének legalább 20 m²-nek kell lennie és három elválasztott részből kell állnia, amelyek: váróhelyiség, teszthelyiség, mintavételi helyiség. A szabályzat szintén előírja az ellenőri szoba létrehozásának kötelességét, amelynek közel kell lenni a csapatok és a játékvezetők öltözőjéhez. A rendkívüli helyzetek kezelésére a létesítmények rendelkeznie kell Krízisszobával, ahol nyolc fő részére kell biztosítani a rendkívüli helyzetek kezelésének feltételeit. A felszereltsége: internet elérés, tárgyalóasztal, 8 db szék, vezetékes telefon, fax, fénymásoló. A krízisszoba kialakítását úgy kell elvégezni, hogy az ellenőri helységből és a vezetési pontból védett úton megközelíthető legyen: A szabályzat szerint a játékvezetők részére hat, az ellenőrök részére 5 főnek, az öltöző épület közvetlen közelében kell megfelelően elkülönített parkolót biztosítani. A szabályzat továbbá előírja, hogy a vendégcsapat szurkolóinak, a VIP-nek, a sajtó munkatársainak, a sportszakmai stábnak (csapatok, játékvezetők, hivatalos személyek stb.), és az üzemeltető személyzetnek külön-külön belépési

pontot kell biztosítani Külön kiemeli, hogy a digitális jegyzőkönyv elkészítéséhez szükséges feltételrendszert működőképes asztali számítógépen vagy laptoppal, ajánlottan, vezetékes vagy mobil internet kapcsolattal kell biztosítani. Ezen felül előírja, hogy a játékvezetői öltözőben rádióvezérelt órát kell elhelyezni, amely szinkronban működik a hazai és a vendég öltözőbe valamint a játékos kijáróban elhelyezett órákkal. A FIFA Footbal Stadiums [7] dokumentum alapján a játékvezetői öltöző legalább 24 m^2, 4 személynek komfortos. Közvetlen, védett hozzáférést kell biztosítania a játéktérhez, és hozzáférhetetlennek kell lennie a nyilvánosság és a média számára. Külön kell lennie, de közel a csapatok öltözőihez. A játékvezetők helyiségeinek: jól szellőztethetőnek kell lennie a friss levegőt biztosítani kell, légkondicionáltnak és központi fűtésűnek kell lenniük, könnyen tisztítható padlóval és higiénikus anyagú falakkal és csúszásmentes padlóval kell rendelkezniük. A világításnak erős fényűnek kell lennie. A WC- és egészségügyi helyiségnek közvetlenül az öltöző szomszédságában kell lenniük, és közvetlen privát hozzáféréssel kell rendelkezniük az öltözőhöz. A modern stadionnak külön területeket kell biztosítania mindkét nem számára. Ezért egy öltözőt öt játékvezető számára és egy területet két játékvezető számára kell biztosítani a szükséges lehetőségekkel.

A Magyar Kézilabda Szövetség a Biztonsági szabályzatában [8] rendelkezik a hivatalos személyek számára biztosítandó infrastrukturális feltételekről. Ebben külön fejezet foglalkozik a hivatalos személyekkel. A parkoló kapcsán előírja a szabályzat, hogy a hivatalos minőségben megjelenő játékvezető versenybírók ellenőrök és a vendégcsapatok járműveit biztonságosan kell elhelyezni, a hivatalos személyek esetén zárt vagy őrzött parkolóban. A szabályzat azt is leírja, hogy a parkolóban elhelyezett járművekben keletkezett kárért a szervező felelős. Ez alól mentesül a szervező, ha a hivatalos személyek nem az általuk kijelölt parkolóban helyezték el a járműveiket. A szabályzat játékvezetőkre vonatkozó paragrafusban megemlíti, hogy ha a játékvezetőket a mérkőzés előtt, alatt és után bármilyen atrocitás éri vagy a sportrendezvények rendjének megzavarása esetén kötelesek fegyelmi feljelentést készíteni. Ezek az esetek a szabályzat alapján:

- illetéktelen személyek bejutása a játékos folyosóra, a játéktérre, illetve a biztonsági zónába;
- a játéktérre, illetve a biztonsági zónába történő bedobálások;
- a hivatalos személyek rendbontása, szabályszegése esetén;
- a Mérkőzés Rendezési Előírások súlyos megsértése esetén;
- rasszista, kirekesztő rigmusok skandálása, melyet a Szervező felszólítására sem hagynak abba;
- pirotechnikai eszközök működésbe hozása esetén.

A szövetségi ellenőr számára a szervező a játékos folyosón és a lelátón egy fő rendező kísérletét biztosítja a szabad mozgás érdekében. A szabályzat kiemeli, hogy a szövetségi ellenőr a szövetség biztonsági szabályát és mérkőzés rendezési előírásainak betartását ellenőrzi döntési és büntetés jogkörrel nem rendelkezik. Az 54/2004 Kormányrendelet a sportrendezvények biztonságáról [9] hatálya alá tartozó sportrendezvények esetén a biztonsági feladatok irányítására és végrehajtására vezetési pontot kell kialakítani. A vezetési ponton sportrendezvény biztosításában részt vevő hatóságok és szervezetek (a rendőrség, a katasztrófavédelem, a szervező, a rendező szerv, az egészségügyi szolgáltató és a sportlétesítmény képviselője) képviselői tartózkodhatnak. A szabályzat rendezői feladatok között külön említi a hivatalos személyek védelmével kapcsolatos teendőket. Ebben leírja, hogy a

játékvezetők, versenybírók és ellenőrök védelmét a megérkezésüktől a sport rendezvény helyszínéről való távozásunkig kell biztosítani. Szintén leírja, hogy a hivatalos személyek útvonalát, a játékos folyosók, öltözők és a játéktér közötti területet biztosítani kell a számukra úgy, hogy oda kizárólag a szervező által feljogosított személyek léphetnek be. Az IHF Bid and Event Manual [10] dokumentumában részletesebben foglalkoznak a hivatalos személyek számára előírt infrastrukturális feltételekről. A játékvezetői öltöző kapcsán minimum 2 öltözőt kell biztosítani, legalább 20 m^2 alapterülettel, amely 4 személy számára kényelmes lehetőségeket biztosít. A további hivatalos személyek számára ún. Delegates' Room kialakítása szükséges, amely 5-10 fő számára biztosít férőhelyet, ahol a találkozhatnak, vagy frissíthetnek magukon. Az öltözőnek zárhatónak kell lennie, továbbá televízió biztosítása szükséges, ahol a mérkőzést lehet követni.

Az egyes sportágak között számos különbség merül fel, tekintettel azok játékszabályira, kultúrájára, a létesítmények jellegére, amely hatással van arra is, hogy a mérkőzések lebonyolítása hogyan történjen. Ezek hatással vannak a hivatalos személyek működésére is. Az adott létesítmények jellege, a nézők elhelyezkedése és száma hatással van a biztonsági kérdésekre. is. Ezen felül akár a játékvezetők működését is befolyásolhatja a nézőtéri nyomás, ami a nézők számából, a közelségükből és a létesítmény akusztikájából is adódhat. A lenti táblázatban személtetem a sportágak közötti különbségeket, amelyek hatással vannak a hivatalos személyek közreműködésére.

	Jégkorong	Kézilabda	Labdarúgás
Játéktér mérete	Hossza: 60 m, szélesség: 25-30 m	Hossza 40 m, szélessége 20 m	Hossza 68 m, szélessége 105 m (a legmagasabb besorolásban)
Kifutók méretei	palánkkal ellátott	oldalvonal mellet legalább 1 m	kapuvonal 5 m, oldalvonal 3 m
Átlagos nézőszám a 2018-19 bajnoki évben	632 fő	922 fő	3300 fő
Játékvezetők száma (legmagasabb bajnoki osztályban)	2 játékvezető, 1 időmérő, 1 titkár	4 játékvezető	4 játékvezető
Szövetségi ellenőr jelenléte a mérkőzésen	alkalmi	alkalmi	kötelező

1. táblázat: A sportágak mérkőzésrendezésével kapcsolatos jellemzői a hivatalos személyek közreműködésének szempontjából (saját szerkesztés) Források: IIHF Rule Book[11], IHF Rules of the Game[12], IFAB The Laws of the Game,[13], www. sportszatisztika.blog.hu [14]

Tömeghatás a mérkőzéseken

Nevill és mtsai [15] megvizsgálták, hogy a szurkolók jelenléte milyen hatással van a játékvezetők tevékenységére a labdarúgásban. Három különböző szobába két-két játékvezetőt ültettek, akik számára levetítettek egy mérkőzést és meg kellett ítélniük a játékvezető által hozott döntések helyességét. Az egyik szóba üres volt, a másik két szobában pedig Atletico Madrid és Real Madrid szurkolók voltak. A mérkőzést történetesen a két csapat

játszotta. A kutatók két féle inkonzisztenciát állapítottak meg, az egyik, hogy mindkét szurkolókkal teli szobában többször találták helytelennek a játékvezetői ítéleteket, illetve az adott szurkolótábor csapata ellen is több hibás ítéletet találtak.

28 EHF tehetségprogramban szereplő játékvezetőn végzett vizsgálatot Kiss és mtsai [16] a kézilabda játékvezetők kognitív képességeivel kapcsolatban. Ezek a pszichológiai, Vienna Test System és a figyelem, Determination Test-ek voltak. Bár alapvetően jól teljesítettek a játékvezetők, a kutatók kimutatták, hogy az egyre nagyobb nyomásra romlottak a teljesítmények.

A 2007-es olasz labdarúgó bajnokságban szurkolói összecsapások miatt néhány csapat nézők nélkül volt kénytelen játszani a szankciók miatt. Peterson-Libdom és Priks [17] arra jutott, hogy a nézők nélküli mérkőzéseken a hazai csapat számára 23%-kal több döntésük volt kedvező a szabálytalanságok tekintetében, a torzító hatás a hazai csapat javára a sárga lapokat illetően 26%, míg a piros lapok esetében ez 70% volt.

CÉLKITŰZÉS

Kutatásunk célkitűzése megvizsgálni, hogy a sportlétesítményekben hogyan biztosítják a szervezők, vagyis a sportszervezetek, a mérkőzések szabályosságának irányító és felügyelő hivatalos személyek számára a munkájuk elvégzéséhez szükséges biztonsági infrastrukturális feltételeket. Az országos sportági szakszövetségek szabályzatainak kidolgozottságának mértéke a sportág professzionalizációjának szintjéhez igazodva eltérő. További célunk megvizsgálni, hogy a szabályzatokban szereplő tárgyi feltételek biztosítása hogyan valósul meg a sportlétesítményekben? Érdekel bennünket továbbá, hogy a sportszervezetekre milyen feladatokat ró a mérkőzések hivatalos személyeinek tevékenysége és ezeknek ellátását milyen módon szervezik meg? Ezen felül fontos kérdés, hogy a hivatalos személyek biztonságának garantálása hogyan valósul meg?

Mindezek alapján az alábbi kutatási kérdéseket fogalmaztuk meg:

- Milyen mértékben szabályozott a jégkorong, kézilabda és labdarúgó szövetségek hivatalos személyek közreműködésével kapcsolatos infrastrukturális feltételek biztosítása a mérkőzéseken? Milyen hasonlóságok és különbségek vannak az egyes szabályzatokban?
- Hogyan valósulnak meg a létesítményekben a szövetség által előírt infrastrukturális feltételek?
- Hogyan történik a hivatalos személyek feladat végezésnek biztosításával kapcsolatos feladatok megszervezése a gyakorlatban a szervezők részéről.

ANYAG ÉS MÓDSZER

A kutatási kérdéseink megválaszolásához primer és szekunder módszereket egyaránt alkalmaztunk. A sportági szabályzatok vizsgálatához alkalmaztam szekunder módszert, dokumentumelemzést, amely egy deduktív, kvalitatív módszer, ami olyan dokumentumok esetén alkalmazható, amelyek nem vizsgálati céllal jöttek létre, de hasznos információkat nyerhetünk ki belőle a kutatásunk számára. Az általunk vizsgált szabályzatok kutatási témája szerint szervezeti dokumentáció, címzettje szerint hivatalos dokumentum [18]. A dokumentumelemzést a jégkorong, a kézilabda, a labdarúgás infrastruktúrával kapcsolatos

szabályzatai alapján végeztük el. A szabályzatok tartalmát egy általunk felállított szempontrendszeren keresztül elemeztük és szakértői értékelést alkalmaztunk egy 0-3-ig terjedő skálán, ahol a

0 –nincs szabályozva,
1 – említést tesz vagy ajánlás szerepel,
2 – tételes, konkrét előírás,
3 – teljeskörű, minőségi előírásokkal.

Az vizsgált tartalmak a következők: szabályzatok részletessége, biztonsági kérdések, parkolás, vezetési, irányító pont, közlekedők biztosítása.

Primer kutatásunk során a strukturált interjú módszerét használtunk, illetve a kérdéseink közül az utolsó kettőt a félig strukturált interjú kategóriába sorolnám (melléklet). Azért választottuk ezt a módszert, mert a gyakorlati megvalósítás során pontos adatokra és mérhető dolgokra voltunk leginkább kíváncsiak, hiszen a három sportágban tapasztaltak összehasonlítása így történhetett meg. Az interjúalanyaink első osztályú sportszervezetek meccsnapi lebonyolításért felelős munkatársai voltak. A jégkorongban a DVTK Jegesmedvék, és a Győri ETO HC, illetve egy csapat nem vállalta a megnevezését, a kézilabdában az ALBA Fehérvár KC, Balatonfüredi KSE, és a Pick Kézilabda Zrt, a labdarúgásban pedig a Diósgyőr FC Kft és két csapat nem vállalta a megnevezésüket, munkatársai válaszoltak a kérdéseimre, N=9. Az interjúk elkészítése nehézkes volt, a kutatásunk készítésekor zajló pandémiára való tekintettel személyes találkozót nem tudtunk egyeztetni. Sajnos nem volt egységes ezek lebonyolítása, mert volt, aki számára az volt a kényelmesebb, hogy a megküldött kérdésekre írásban válaszol. Ilyenkor a megkapott válaszok alapján még tehettem fel további kérdéseket a válaszok pontosítása miatt. Volt, aki telefonon válaszolt a feltett kérdésekre, amelyeket rögzítettem a későbbi feldolgozáshoz. Az interjúk elkészítése átlagosan kb. 15 percet vett igénybe. A kapott válaszokat az alábbi szempontok alapján elemeztük:

- a hivatalos személyek fogadása,
- a hivatalos személyek biztonsága,
- kommunikáció a hivatalos személyek és a szervezők között,
- a szövetségi szabályzatokban foglaltak gyakorlati megvalósítása
- tapasztalatok az interjúalanyok saját elmondása alapján.

A kapott válaszokat aszerint vizsgáltuk meg, hogy az egyes sportágakban milyen válaszokat adtak az interjúalanyok, azok azonosak vagy különbözőek voltak, illetve összevetettem a sportágak közötti különbségekre vonatkozóan is.

EREDMÉNYEK

Dokumentumelemzés

A szabályzatok szekunder elemzése során az alábbi eredményeket kaptam a vizsgált három sportágban.

A hivatalos személyekkel kapcsolatos szabályzatok részletessége, tagoltsága és elérhetősége.

Megvizsgáltuk, hogy az egyes szövetségek milyen szabályzataiban jelennek meg a hivatalos személyekkel kapcsolatos infrastrukturális kérdések, illetve azok milyen részletesen, pontosan és tételesen szabályoznak.

A MJSZ önálló Infrastruktúra szabályzatot [4] alkotott, amelyben az egyes helyiségek leírása külön pontokban szerepel. Korábban a Versenyszabályzatban szerepeltek pályával és a rendezéssel kapcsolatos követelmények, de ezek az kevésbé voltak kidogozottak. Mennyiségi és minőségi előírásokat is tartalmaz. A jegkorongszövetseg.hu oldalon könnyen megtalálható. Az MLSZ szintén önálló Infrastruktúra szabályzatot [6] alkotott, amely külön pontokban rendelkezik a különböző helyiségek kialakításáról és felszereltségéről. Szintén tartalmaz mennyiségi és minőségi feltételeket, különös tekintettel a kulturált környezet kialakítására. A szabályzat világos, és a mellékletek között táblázat formátumban is szerepel az Előírások jegyzéke, ami nagyban megkönnyíti a szabályzat felhasználását. A rádióvezérelt órák könnyítik a mérkőzés résztvevői és a média közötti együttműködést. A szabályzat a dokumentumtar.mlsz.hu oldalon könnyen elérhető. Az MKSZ a Biztonsági szabályzatban [8] rögzíti a hivatalos személyekkel kapcsolatos pontokat. Önálló szabályzata az infrastruktúrára vonatkozóan nincs. A hivatalos személyek számára biztosított helyiségek leírása hiányzik. A dokumentumok nehézkesen érhetők el, az egyes bizottságok és albizottságok oldalán találhatók a vonatkozó dokumentumok. A laikus számára nem biztos, hogy egyértelmű mivel foglalkozik az adott bizottság.

	MJSZ	MKSZ	MLSZ
A hivatalos személyekkel kapcsolatos szabályzatok részletessége, tagoltsága és elérhetősége.	2	1	3

2. számú táblázat: A hivatalos személyekkel kapcsolatos szabályzatok részletessége, tagoltsága és elérhetősége.

Biztonsági kérdések

A jégkorongban a versenyszabályzat előírja, hogy a szervezőknek biztosítani kell a játékvezető öltöző előtti folyosószakaszt a mérkőzés előtt 60 perccel egészen a mérkőzést követő 30 percig. A Biztonsági szabályzatban [19] nem kezeli külön a hivatalos személyeket a VIP vendégeket. Az ellenőr részére nem ír elő folyamatos biztosítást, ha az ellenőr a mérkőzés időtartama alatt a lelátón szeretne helyet foglalni. A kézilabdában a Biztonsági szabályzatban [8] rendelkeznek a hivatalos személyek jelenlétének feltételeiről. A játékvezető feladatai közé delegálja a szabályzat, hogy a mérkőzés előtti, alatti és utáni atrocitások esetén fegyelmi feljelentést kell készíteniük. Itt előírják, hogy a szövetségi ellenőr szabad mozgásának érdekében egy fő rendezői kíséretet biztosítanak. A szabályzat a rendezői feladatok között külön említi, hogy a hivatalos személyeket a megérkezésüktől a sport rendezvény helyszínéről való távozásig biztosítani kell, ideértve az általuk használt útvonalakat, úgy hogy oda csak a szervező által feljogosított személyek léphetnek be. A labdarúgásban

Biztonsági szabályzatot [19] hoztak létre. A biztonságiakkal érintett területek között szerepelnek az ellenőri szoba és a hivatalos személyek által használt területek is. Kiemeli, hogy a játékvezetők és ellenőrök biztonságához kötődő feladatokat a versenyszabályzattal összhangban kell kivitelezni. A feladatokat nem részletezik, de mivel minden mérkőzésen kötelező a Biztonsági terv elkészítése, illetve a sportrendezvényt biztosítását biztonsági szolgálat látja el, ezért a biztosítási feladatok nem közvetlenül a szervezők feladata.

	MJSZ	MKSZ	MLSZ
Biztonsági kérdések	2	2	1

3. számú táblázat: Biztonsági kérdések a szabályzatokban

Parkolás

A jégkorongban a Biztonsági szabályzat [20] rendelkezik a parkolással kapcsolatos kérdésekről. Leírja, hogy a hivatalos személyek számára külön a szurkolóktól elzárt területen kell parkolóhelyet biztosítani úgy, hogy az autókban ne tehessenek kárt. Azonban a parkolók számáról és elhelyezéséről nem rendelkezik.

A labdarúgásban az Infrastruktúra szabályzat [6] rendelkezik, hogy az első osztályban a játékvezetők részére hat fő, az ellenőrök részére öt fő, az öltöző épület közvetlen közelében kell elkülönített parkolót biztosítani. Azonban a szabályzatból nem derül ki, milyen eloszlásban, hiszen a játékvezetők és az ellenőrök is külön autóval érkezhetnek. Azt is leírja, hogy a parkolóhelyet úgy kell elhelyezni, hogy az azt használók útvonala a részükre fenntartott belépési pontig lehetőleg ne keresztezze más típusú résztvevők útvonalát.

A kézilabdában a Biztonsági szabályzat [8] önálló paragrafusban rendelkezik a hivatalos személyek gépjárműveinek parkoltatásáról. Leírja, hogy a járműveket zárt vagy őrzött parkolóban kell elhelyezni illetve azt, hogy ezért a szervező a felelős a sportrendezvény ideje alatt. A szabályzat azonban a parkolóhelyek elhelyezéséről és számáról nem rendelkezik.

	MJSZ	MKSZ	MLSZ
Parkolás	1	1	2

4. számú táblázat: A parkolással kapcsolatos szabályok

Vezetési, irányító pont biztosítása

A vezetési pont kialakítása rendeletből származó kötelezettség, így mindegyik szövetség rendelkezek ezekről a szabályzataiban. Az MLSZ azonban krízisszoba kialakítását is előírja, illetve ezeknek a felszereltségét is.

	MJSZ	MKSZ	MLSZ
Vezetési, irányító pont biztosítása	1	1	2

5. számú táblázat: Vezetési, irányító pont biztosítása

	MJSZ	MKSZ	MLSZ
A hivatalos személyekkel kapcsolatos szabályzatok részletessége, tagoltsága és elérhetősége.	2	1	3
Biztonsági kérdések	2	2	1
Parkolás	1	1	2
Vezetési, irányító pont biztosítása	1	1	2
Összesen	6	5	8

6. számú táblázat: Összesítés

Interjú

Az interjúk során válaszokból általánosságban kiderült, hogy feltett kérdésekkel kapcsolatos feladatokért nem egy ember a felelős és több szervezeti egység összehangolt munkája szükséges. Több esetben külön szervezetet is érintett, hiszen nem a sportszervezetek tulajdonában vannak az egyes létesítmények éltérő módon jelennek meg a mérkőzéseken a létesítmény képviselői.

Hivatalos személyek fogadása

A jégkorongban és a labdarúgásban hivatalos személyek szövetség által kibocsátott regisztrációs kártyával léphetnek a létesítmény területére, melynek birtokában a biztonsági személyzet beengedi őket. Az létesítményen belüli akkreditációs rendszerekben olyan passt vagy karszalagot kapnak az ellenőrök, amellyel a biztonsági személyzet beengedi őket, ahova szükséges. A kézilabdában a szövetség előzetes Akkreditációs listát küld a hivatalos személyek névsorával. A szövetségek informatikai rendszerében a csapatok számára elérhetők a közreműködő hivatalos személyek nevei, de az, hogy ők hány autóval fognak érkezni, az nem. A parkolást tekintve minden létesítményben megoldott a nézőktől elzárt parkoló biztosítása. Fenntartva 1, maximum 2 parkolóhelyet biztosítanak a játékvezetők számára, 1-et a szövetségi ellenőr, 1-et a játékvezetői ellenőr számára. Amennyiben több parkolóra lenne szükség, azok fogadását minden létesítményben meg tudják oldani.

A hivatalos személyek biztonsága

A hivatalos személyek biztosítása külső biztonsági szolgálat közreműködésével történik a Sportrendezvények biztonságáról szóló kormányrendelet alapján [9]. Ez egységes volt az összes válaszadónál. Mindegyik válaszadó megemlítette az öltözőfolyosó felügyeletét biztonsági őrökkel. A labdarúgásban két biztonsági őr áll a játékvezető öltöző előtt, ebben egységes válaszok születtek. Az ellenőrök számára a kézilabda sportágban a külön biztonsági őrt biztosítanak, aki kíséri őt. Egy esetben tettek említést arról, hogy a lelátón helyet foglalva is felügyeli. A labdarúgásban a VIP szektor ülőhelyein foglalhatnak helyet az ellenőrök. A jégkorongban a VIP szobában vagy szektorban kapnak helyet, azonban ha a nézőtérről követnék a mérkőzést, akkor nem biztosítanak számára felügyeletet egyik helyen sem.

Kommunikáció a hivatalos személyek és a szervezők között

Minden válaszadó az elsődleges kommunikációs csatornaként a mobiltelefon használatát jelölte meg. Ebben a kézilabda sportág proaktív, hiszen minden esetben az említett Akkreditációs listát küld. A jégkorongban és labdarúgásban az ellenőrök a helyszínen cserélnek telefonszámot a szervezőkkel. A játékvezetők kapcsán erre nincs szükség. Öt válaszadó említette, hogy a biztonsági őrök által használt CB rádión is tudnak üzenni a hivatalos személyek. A dokumentumok átadása kapcsán kiemelendő, hogy minden válaszadó említette a Biztonsági terv és a Rendezői névsor átadását a szövetségi ellenőr részére, hiányában a játékvezetők részére.

A kézilabda sportágban két válaszadó említette, hogy a mérkőzés kezdetét megelőzően 1 órával a hivatalos személyek, a szervezők és a biztonsági szolgálat képviselői egyeztetést tartanak a játékvezetői öltözőben. A jégkorongban egy fő említette, hogy néhány ellenőr egyeztetést hív össze a szervezőkkel és a biztonsági szolgálat embereivel, ahol megfogalmazza az elvárásait. A labdarúgásban ilyen közös egyeztetés nincs, de a szervezőknek az ellenőröket és a játékvezetőket tájékoztatni kell. A Krízisszobával és a Vezetési pontokkal történő kommunikáció is telefonos, esemény esetén személyes egyeztetés történik, amelynek az infrastrukturális feltételei biztosítottak-. A kézilabda sportágból egy esetben nem kaptunk választ az erre irányuló kérdésre.

A szövetségi szabályzatokban foglaltak gyakorlati megvalósítása

Nem kaptunk olyan választ, ami arról számolt volna be, hogy az ő létesítményükben valami másképp valósul meg, mint ahogyan az a szabályzatban szerepel. A jégkorongban egy válaszadó megjegyezte, hogy bár az ő létesítményükben minden rendben van (nemzetközi mérkőzés megrendezésére alkalmas csarnok), az országos viszonylatban nagyon eltérő tapasztalatok szerzett az ideiglenesen engedélyezett csarnokokról, tehát amikor bizonyos időre valamilyen hiányosság ellenére kap engedélyt az adott létesítmény mérkőzés szervezésére.

Tapasztalatok az interjúalanyok saját elmondása alapján

A jégkorong sportágban egy válaszadó megfogalmazta, hogy hasznos lenne számukra is, ha Akkreditációs listát küldene a szövetség a mérkőzés előtt, ahogy a kézilabdában. A kézilabdában egy válaszadó azt fogalmazta meg, hogy sokat javultak a versenyszervezési körülmények országos szinten, ami szerinte a szabályzatoknak köszönhető. Szintén a szabályzatok hasznosságát és a mérkőzésrendezési feltételek egységesítését eredményezi a jégkorongban az Infrastruktúra szabályzat két válaszadó szerint. Szintén a jégkorongban egy válaszadó megjegyezte, hogy a szabályok inkább legyenek szigorúak, mintsem probléma legyen. Az összes interjúalany válaszából megállapítható, hogy a hivatalos személyeknek bármely kérése van az előírásokon felül, vagy felmerül egy probléma, a versenyszervezők nyitottak és partnerként állnak rendelkezésre.

MEGBESZÉLÉS ÉS KÖVETKEZTETÉSEK

A primer és szekunder kutatások eredményei alapján a célkitűzésben megfogalmazott kérdéseimre az alábbi válaszokat adom.

Milyen mértékben szabályozott a jégkorong, kézilabda és labdarúgó szövetségek hivatalos személyek közreműködésével kapcsolatos infrastrukturális feltételek biztosítása a mérkőzéseken? Milyen hasonlóságok és különbségek vannak az egyes szabályzatokban?

A dokumentumelemzés alapján a labdarúgás sportágban a leginkább szabályozottak a feltételek, a megszerezhető 12 pontból 8 pontot értek el. A jégkorongban 6 pont, a kézilabdában 5 pont. Megállapítható, hogy a biztonsági kérdésekben a legkidogozottabbak és a legrészletezettebbek a szabályzatok. Ebben a kérdésben a jogszabályok is számos kötelezettséget írnak elő a szövetségek és sportszervezetek számára. A kézilabdában az infrastrukturális feltételekkel kapcsolatban szinte alig található követendő szabály. A játékvezetői öltözők felszereltségének kialakítását a csapatokra bízzák. A jégkorongban megjelennek mennyiségi előírások, néhol minőségi jelzőket is alkalmaznak. A labdarúgásban részletezett mennyiségi és minőségi előírások egyaránt megjelennek minden kérdésben. Itt a szervezőknek csak követniük kell a leírtakat. Megjegyezném, hogy a minőségi felkészülés lehetősége és a kényelem biztosítása nagyon fontos a játékvezetők számára, hiszen nagy utat tesznek meg a mérkőzések előtt és magas színvonalú teljesítményt várunk el tőlük.

Hogyan valósulnak meg a létesítményekben a szövetség által előírt infrastrukturális feltételek?

Az interjúkból egyértelműen kiderült, hogy a vizsgált létesítményekben megvalósulnak az előírt feltételek, azonban az előírások a fentiek alapján nagyon eltérőek. Az interjúalanyok megjegyezték, hogy a hitelesítéskor a létesítményeket a szövetségek képviselői minősítik és döntenek az alkalmiságáról, azonban az ideiglenes engedélyek, amelyekre a bajnokságok folyamatosságának biztosítása miatt van szükség, sok esetben nagyon különböző színvonalon valósulnak meg. A vizsgálatban kizárólag első osztályú sportszervezetek szerepelnek, érdemes lenne további kutatásokat végezni alacsonyabb osztályokban is.

Hogyan történik a hivatalos személyek feladat végezésnek biztosításával kapcsolatos feladatok megszervezése a gyakorlatban a szervezők részéről?

A feladatvégzéshez a biztonságot a legmagasabb szinten garantálják minden sportágban. A professzionális biztonsági szolgáltatók feladatai közé delegálják a sportszervezetek a hivatalos személyek biztonságának garantálását. Ez a kézilabdában személyes kísérettel valósul meg, a jégkorongban vegyes ennek a megvalósítása, a labdarúgásban területi védelem az elsődleges. A tárgyi feltételek biztosításának szabályozása a kézilabdában minimális, így a megvalósítása is eltérő. Pl. az interjúkból az derült ki, hogy van, ahol fogast biztosítanak, van, ahol öltözőszekrényt, a labdarúgásban mindenhol megvalósul az öltözőszekrény. Kényelmi és higiénés szempontok a jégkorongban és a labdarúgásban jelennek meg. A labdarúgásban minden válaszadó említette a catering bekészítését, a jégkorongban és a kézilabdában ez esetleges, de a partneri viszonynak köszönhetően mindenhol teljesítik az ésszerű kéréseket, illetve a VIP terembe bejutást biztosítanak.

A sportversenyek Smith és Westerbeek [2] szerinti jellemzők alapján a vizsgált kérésekben a labdarúgásban tapasztalható leginkább professzionalizáltság. Érdemes lenne más sportágak szövetségeinek is részletesebb szabályzatokat létrehozni, hiszen a sportszervezetek válaszaiból érezhető, hogy ezek betartására törekednek. A leírt szabályok pedig általánosságban véve, (az ideiglenes engedélyeket leszámítva) nemcsak az év eleji hitelesítéskor, hanem év közben is megvalósításra kerültek. Szintén az interjúk alapján megállapítható, hogy sok esetben a sportszervezetek számára is könnyebb, ha a szabály részletesebb,

hiszen akkor pontosan tudják, milyen körülményeket kell teremteniük. Minőségi, kényelmi és higiéniai kérdések a labdarúgásban több helyen, de a jégkorongban is néhányszor megemlítésre kerül. Ez fontos, hiszen jó teljesítményt várunk el pl. a játékvezetőktől, akik nagy nyomás alatt tevékenykednek a tétre és a közönségre való tekintettel.

Az is megállapítható, hogy a biztonsági szempontok kidolgozása a legpontosabb a szabályzatokban. Ez üdvözölendő, hiszen a résztvevők biztonsága a legfontosabb, ide értve nemcsak a sporttevékenységet előállítókat, hanem a nézőket is. A közreműködők munkájához szükséges feltételek mellett a szabályzatokkal a hivatalos személyeket védeni is tudják a szövetségek. Az FTC labdarúgó csapatát pénzbüntetéssel sújtották a hivatalos személyek parkolási feltételeinek biztosításával kapcsolatos szabályzatok megsértéséért, továbbá pontlevonást is kilátásba helyeztek [21]. A továbbiakban érdemes lenne a nemzetközi szabályzatok részletesebb elemzését is elvégezni, hiszen azok alapján kell kidolgozni a hazai szabályzatokat. A nemzetközi mérkőzések alkalmakor az ottani szabályzatoknak kell megfelelni, így ha valamelyik csapat először szembesül a feltételekkel, mert nemzetközi porondra kerül a csapat, alkalomszerűen kell ellátni ezeket a feladatokat. Az interjúk során nemzetközi rutinnal rendelkező csapatok képviselőivel beszélgettem, akik a már kialakított gyakorlatot mondták el. A többi első osztályú csapat bevonásával szükséges tovább folytatni a kutatást. Illetve szükséges megkérdezni a szövetségek és a hivatalos személyek véleményét is a témában. Magyarországon a vizsgált sportágakban a létesítményhelyzet jelentős fejlődésen ment keresztül az elmúlt időszakban, amelyekben nemzetközi szintű mérkőzéseket lehet tartani. A szövetségeknek törekedniük kell ezen a téren is arra, hogy a hazai első osztályú mérkőzések a nemzetközi színvonalhoz közelítsenek.

IRODALOMJEGYZÉK

[1] Sterbenz T., Géczi G. (szerk.).(2016): Sportmenedzsment. Testnevelési Egyetem. Budapest
[2] Smith A., Westerbeek, H. (2004). The Sports Business Future. Palgrave. New York
[3] 2004. évi I. törvény a sportról
[4] MJSZ Infrastruktúra szabályzat (www.jegkorongszovetseg.hu)
[5] IIHF Ice Rink Guide
[6] MLSZ Infrastruktúra szabályzat (dokumentumtár.mlsz.hu)
[7] FIFA Footbal Stadiums (www.fifa.hu)
[8] MKSZ Biztonsági szabályzat (www.mksz.hu)
[9] 54/2004 Kormányrendelet a sportrendezvények biztonságáról
[10] IHF Bid and Event Manual (www.IHF.info)
[11] IIHF Rules Book (www.iihf.com)
[12] IHF Rules of the Game
[13] IFAB Laws of the Game (www.theifab.com)
[14] sportstaisztika.blog.hu (letöltve: 2021. április 28.)
[15] Nevill AM, Hemingway A, Greaves R, Dallaway A, Devonport TJ. Inconsistency of decision-making, the Achilles heel of referees. J Sports Sci. 2017 Nov;35(22):2257-2261.
[16] Kiss, B., Balogh, L., & Münnich, Á. (2020). A sport-psychological diagnostic examination of young EHF handball referees with a focus on mental skills. Journal of Physical Education and Sport, 20(4), 1984-1995

[17] Pettersson-Lidbom P. és Priks M. (2010): Behavior under social pressure: Empty Italian stadiums and referee bias. Economics Letters 108 (2010) 212–214.
[18] Lengyelné M.T., Tóvári J. (2001): Kutatásmódszertan. Eszterházi Károly Főiskola. Eger.
[19] MJSZ Biztonsági szabályzat (www.jegkorongszovetseg.hu)
[20] MLSZ Biztonsági szabályzat (dokumentumtár.mlsz.hu)
[21] www.nemzetisport.hu/labdarugo_nb_i/fegyelmi-akar-pontlevonassal-is-buntethettek-volna-a-fradit-2571495)letöltve 2021. április 28.)

THE ROLE AND DISEASE OF THE HUNGARIAN PRIVATE SECURITY SECTOR IN RELATION TO SPORT SECURITY TASK

A HAZAI MAGÁNBIZTONSÁGI ÁGAZAT SZEREPE ÉS KÓRKÉPE A SPORTBIZTONSÁGI FELADATOK TEKINTETÉBEN

FÁBIÁN Péter[1]

Abstract

"Sport is part of the public good," the preamble to the Sports Act states, stating that "in order to achieve the socially useful goals of sport, the state […] ensures public safety at sporting events and contributes to the safe conduct of sporting events".
One of the most obvious areas of interconnection between public and private security is the provision of sporting events and sports facilities. Although Baron Coubertin still hoped that the Olympic Games would bring peace and understanding to humanity, in many cases this could not be achieved. The first Olympics after the September 11, 2001. terrorist attacks were held in 2002 in Salt Lake City. It was the first Olympics, the first major sporting event to have already given high priority to security issues [1].

Keywords

security, public safety, private security, sporting events, terrorism

Absztrakt

„A sport a közjó része” – szögezi le a sporttörvény preambuluma, majd az állami feladatokról szólva rögzíti, hogy „a sport társadalmilag hasznos céljainak megvalósítása érdekében az állam […] gondoskodik a sportrendezvényeken a közbiztonságról, hozzájárul a sportrendezvények biztonságos lebonyolításához”.
A köz- és a magánbiztonság összekapcsolódásának egyik legnyilvánvalóbb terepe a sportrendezvények és sportlétesítmények biztosítása. Ugyan Coubertin báró még azt remélte, hogy az olimpiai játékok a békét és megértést hozzák el az emberiség számára, ám ez jónéhány esetben nem teljesülhetett. A 2001. szeptember 11-i terrortámadás utáni első olimpiát 2002-ben rendezték Salt Lake City-ben. Ez volt az első olimpia, az első nagyszabású sportrendezvény, melyen már kiemelt prioritást élveztek a biztonsági kérdések [1].

Kulcsszavak

biztonság, közbiztonság, magánbiztonság, sportrendezvények, terrorizmus

[1] fabianpeter@topcopgroup.com | ORCID: 0000-0003-0640-6557 | founder, Top Cop Group | Alapító, Top Cop Group

BEVEZETÉS

A sportrendezvények biztonságos lebonyolításának nélkülözhetetlen eleme a hatékony rendezvénybiztosítás, mely sok esetben még napjainkban is komoly kihívást jelent a sportélet szereplői számára.

A sportrendezvények biztonságának jogszabályi alapját a sportról szóló 2004. évi I. törvény jelenti, a részletszabályokat pedig a sportrendezvények biztosításáról szóló 54/2004. (III. 31.) Kormányrendelet határozza meg, illetve további speciális rendelkezéseket találunk az egyes sportági szövetségek szabályzataiban. Miként az ezekből a normákból kiderül, az állam több ponton is szerepet vállal a sportrendezvények biztonságos előkészítése és lebonyolítása érdekében. Így például, a sportrendezvényekkel kapcsolatos kitiltás, habár magánjogviszonyt érint, közjogi normában (a Btk.-ban) nyert szabályozást: a kitiltott néző nem vehet jegyet és nem mehet be a sportrendezvényre, mely nem vitásan magánjogi természetű rendezvény. Tanulmányomban a biztonság–közbiztonság–magánbiztonság főbb aspektusainak egybevetését követően a sportrendezvények biztosításának legfontosabb szabályait tekintem át, és megvizsgálom azt is, hogy a magánbiztonsági vállalkozások mely pontokon vonhatók be a sportrendezvények biztosításába, a vagyonőrök, személyőrök e feladatkörükben eljárva milyen jogosítványokkal rendelkeznek, illetve milyen feladatokat látnak el.

Kutatási módszerem a témához igazodóan leíró-elemző módszer, mely a rendelkezésemre álló szakirodalom másodelemzésén és a vonatkozó jogszabályok kritikai elemzésén alapul.

ELMÉLETI ALAPVETÉSEK

„Istenek ajándéka, szépség, igazságosság, bátorság, tisztesség, öröm, termékenység, haladás, béke” – ekként méltatta a sportot a modernkori olimpiai játékok atyja, Pierre de Coubertin [2]. A sportnak, legyen szó a szellem vagy a test edzésének bármely formájáról, valóban számos pozitív hozadéka van – és ezen előnyök közül jónéhány olyan akad, melyet nemcsak a sport gyakorlói, hanem a sportrendezvények nézői is élvezhetnek.

A sport méltatása

A sport szó francia eredetű, a szórakozást jelentő *„desport”* kifejezésre vezethető vissza, mai értelmében először 1829-ben használták, értve alatta minden olyan fizikai aktivitást, melyhez a testi erő mellett szellemi tevékenységre is szükség van, és amely, túl azon, hogy hozzájárul az ember egészségéhez, még örömet is okoz [3].

A sport jótékony hatásai az élet számos területén megmutatkoznak. Jelentős szerepet játszik az egészségmegőrzésben és egészségfejlesztésben, a nevelésben, az oktatásban. Lehetővé teszi az olyan magasztos érzelmek kifejezését és megélését, mint amilyen a hazaszeretet, a nemzeti büszkeség, a szolidaritás. Közösséget épít, kötődést alakít ki emberek között.

Az, hogy a sport hatást gyakorol a nemzetgazdaságra, aligha képezi vita tárgyát. A sportnak politikai vonatkozásai is lehetnek, köszönhetően a gazdasági hatalom és a politikai hatalom közötti sajátos viszonyrendszernek; az ókori olimpiai játékokat is politikai célzattal szervezték meg, azért, hogy a valamiképpen enyhíteni tudják a görög városállamok közötti feszült helyzetet, és legalább a játékok idejére fel tudják függeszteni a háborúskodást [4].

A magyar kormány egy évtizede kiemelt prioritásként kezeli a sportot, számottevő összegeket fordít és jelentékeny energiákat mozgósít arra, hogy hazánk minél több nemzetközi sportesemény megrendezésének jogát nyerje el, illetve, hogy megfelelő számban álljanak rendelkezésre ezen sportesemények befogadására szolgáló létesítmények.

Szokás a nemzetközi sporteseményekre az erőszak és a rasszizmus elleni fellépés eszközeként tekinteni, e kérdésben ugyanakkor érdemes óvatosnak lennünk, a tapasztalat ugyanis azt mutatja, hogy a futballrendezvények nézői közül némelyek olykor elragadtatják magukat, és gyűlöletkeltő, rasszista megnyilvánulásokkal rombolják a sport nemes eszméjét [5].

A sportesemények pszichológiája

A nagy nézőközönséget vonzó sporteseményeket – így az olimpiákat, a labdarúgó tornákat – speciális arénákban, stadionokban rendezik meg. A stadion minden tekintetben különleges, egyedi atmoszférájú hely, vagy – ahogy Freyer Tamás [6] fogalmaz – *„misztikus szentély”*, melyben az ókori görögök az isteneikhez fohászkodtak a győzelem reményében, ám amelynek sajátos hangulata a ma emberét sem hagyja érintetlenül. Ezt a sajátos hangulatot erősíti a stadionok kialakítása, a hozzáadott technika: a küzdőteret körbe ölelő lelátók felerősítik a hangokat, a hangszórókból zene harsog, a hatalmas kivetítőkön úgy láthatjuk a játékosokat vagy a stadion másik végében ülő szurkolókat, mintha ott állnánk mellettük. A sajátos hangulatért azonban leginkább a jelenlévő embertömeg felelős: a modern arénák befogadóképessége több tízezer fő [7].

A sportrendezvények modern elméletei

A XX. század kutatói ennél árnyaltabban ítélik meg a kérdést, többségük (például Reicher, Stott, Drury) azt az álláspontot képviseli, hogy a tömeg részévé válás nem jelenti egyúttal az identitását feladását, pusztán csak arról van szó, hogy az egyén átmenetileg fontosabbnak tartja a társas identitást [8]. Reicher ebből kiindulva mutat rá azokra a veszélyekre, melyek abból adódnak, ha a rendbontás okán fellépő rendőri szervek homogén egészként kezelik a tömeget. Mindaddig ugyanis, amíg a rendezvények békés mederben folynak, a résztvevők meghatározó többsége mérsékeltnek tekinti magát és ekként is viselkedik, ha pedig rendzavarást tapasztal, maga is igényli, hogy a hatóságok fellépjenek a renitensekkel szemben. Ám amennyiben a rendőrség a tömeget homogénnek és annak valamennyi tagját egyformán veszélyesnek tekinti, az aránytalan és eltúlzott fellépés *„radikalizálja és az erőszakos kisebbség mellé állítja a mérsékelt tömeget, minek következtében beindul az eszkalációs folyamat”* [9.], [10].

A BIZTONSÁG ASPEKTUSAI

Az emberiség történetét végigkíséri az egyén biztonság iránti vágya és a biztonság ellen ható tényezők folytonos küzdelme. Az ember *„környezete és saját maga által veszélyeztetett lény”* [11], fenyegetést jelent rá a másik ember, a társadalom, a természeti és technikai környezet, nemritkán pedig önnön cselekedetei. Ezzel együtt minden ember örök vágya, hogy életét a lehető legnagyobb biztonságban élhesse. Nem egyszerű dolog megtalálni a biztonság azon szintjét, mely egyszerre optimális az egyén, az egyének közösségei és a társadalom egésze számára. Totális biztonság nincsen, az ennek megközelítésére irányuló

kísérletek egyfelől a fejlődés ellen hatnak, másfelől nagyban csorbítják az emberi szabadságokat. A biztonság hiánya vagy alacsony mértéke sem kedvező azonban, az állandó bizonytalanság, a félelemérzet ugyanis negatívan hat az emberek teljesítményére [12].

A biztonság fogalma

A biztonság összetett, több tényező által meghatározott fogalom, mely egy olyan optimális állapotot fejez ki, melyben egy adott ország, társadalom értékei és érdekei, lakossága és vagyona mentes mind a külső, mind a belső fenyegetésektől [13].

A biztonság fogalmának értelmezése kultúránként, történelmi koronként változik, függ az adott ország, közösség politikai berendezkedésétől, gazdasági, társadalmi helyzetétől, de még az aktuálpolitikától is. Míg a korábbi évezredekben a biztonság alatt kizárólag katonai, védelempolitikai biztonságot értettek, addig ez mára jelentősen megváltozott: előtérbe kerültek a biztonság egyéb – társadalmi, gazdasági, politikai, pénzügyi, egészségügyi, környezeti stb. – aspektusai. Tovább bonyolítja a kérdés megítélését, hogy a biztonságnak létezik objektív és szubjektív értelmezése: az előbbi esetben a fenyegetettség valós, míg az utóbbi esetében csak vélelmezett, az pedig korántsem biztos, hogy e két értelmezés fedésben van egymással. Ráadásul, nem minden ország, közösség esetében alakul azonosan a fenyegetettség-küszöb, könnyen lehet ugyanis, hogy ugyanazt a szituációt az egyik ország, közösség a biztonságot veszélyeztető fenyegetésként, a másik ellenben elfogadható helyzetként értékeli [14].

A közbiztonság mibenléte

A közbiztonság a biztonság elsődleges, meghatározó jelentőségű eleme, melyet definiálhatunk közállapotként és államcélként [15.]. A közbiztonság – hasonlatosan a biztonsághoz – egyfelől egy szubjektív kategória, egy olyan optimális állapot, melyben a polgárok biztosak lehetnek abban, hogy sem személyüket, sem vagyontárgyaikat nem fenyegeti semmilyen veszély. E megközelítésben az, hogy az egyén mit gondol a közbiztonságról, döntő módon függ az érdekeitől, értékrendszerétől, és legalább ennyire attól, hogy milyen információkkal bír a körülötte lévő világ dolgairól, a kívülről érkező tényleges veszélyekről. Másfelől értelmezhetjük a közbiztonságot államcélként, olyan célként, melynek elérésére és fenntartására a végrehajtó hatalom tesz kötelezettségvállalást: az állam garantálja polgárai számára, hogy nem kell semmiféle veszélytől tartaniuk, ha pedig a veszély ennek ellenére bekövetkezne, úgy mindent megtesz annak elhárítására [16]. Az ezirányú állami kötelezettségvállalásnak ugyanakkor van egy súlyos korlátja: az állam a közbiztonság sérthetetlenségére nem tud garanciát vállalni, pusztán csak annak védelmére vállalkozhat [17].

A közbiztonság értelmezése az Alkotmánybíróság több határozatában is előkerül, ezek közül is kiemelendő a 13/2001. (V.14.) AB határozat, mely kimondja, hogy a közbiztonság *„alkotmányos értéktartalommal bír”*, *sine qua non*-ja minden demokratikus államnak, tartalmát ugyanakkor meghatározza az adott társadalom demokrácia szintje [18], [19]. Ezzel együtt azonban a közbiztonság egy, a fenyegetések elhárítására, a bekövetkezett veszélyek megszüntetésére szolgáló komplex rendszer is, mely működőképességéhez elengedhetetlen az állam és az állampolgárok közötti együttműködés: az állam csak abban az esetben tud eleget tenni a közbiztonság védelmére tett vállalásának, ha a polgárok maguk is megtesznek mindent a veszélyek elkerülése érdekében. A közbiztonság – mutat rá Németh [20] – *„kollektív társadalmi termék, messze nem kizárólag a rendészeti tevékenység produktuma”*. A közbiztonság tehát nem létezhet állampolgári „önvédelem” nélkül; ez utóbbi

hiánya azt mutatja, hogy az állam és az egyének közötti, biztonság megteremtésére és védelmére szolgáló kooperáció nem megfelelő. A biztonság ugyanis az állam és a társadalom együttműködésének, közös munkájának az eredményeként jöhet csak létre, mindebben pedig fontos szerephez jutnak a rendvédelmi szervek, a települési önkormányzatok, a polgárok különféle szerveződései (leginkább a polgárőrség) – nem utolsó sorban pedig a magánbiztonsági vállalkozások.

A magánbiztonság fogalma és alkotmányjogi megalapozottsága

A magánbiztonság – a legáltalánosabb értelmezést alapul véve – *„olyan kívánatos jogállapot, amelyben a személy és a jogi személy a magánjogban kifejeződő szabadságjogainak, gazdasági, szociális és kulturális jogainak egyenjogúsága, valamint jogos érdekeinek érvényesülése szavatolt”* [21]. A magánbiztonság megteremtése sokáig az állam kizárólagos feladata volt, az állam rendészeti monopóliuma azonban az elmúlt néhány évtized során megtört, a kormányok, döntéshozók pedig kénytelenek tudomásul venni, hogy pusztán közhatalmi eszközökkel már képtelenség a polgárok vagyoni biztonságát garantálni, az esetek nagy részében jóval hatékonyabb és gazdaságosabb, ha meghatározott tevékenységeket kiszerveznek [22]. Napjainkra nemzetközi trenddé vált, hogy az állam egyre szélesebb körben engedi a magánszemélyek és a jogi személyek számára, hogy piaci alapon működő magánbiztonsági cégek szolgáltatásait vegyék igénybe [23].

A magánbiztonság alkotmányjogi alapjait az Alaptörvény V. cikke rögzíti, eszerint *„mindenkinek joga van törvényben meghatározottak szerint a személye, illetve a tulajdona ellen intézett vagy az ezeket közvetlenül fenyegető jogtalan támadás elhárításához”*. Ez a rendelkezés egy teljesen új, a korábbi Alkotmányban nem szereplő jogot határoz meg, lényegében a büntetőjogi jogintézmény, a jogos védelem alkotmányjogi elismerését jelenti. Lényeges leszögezni, hogy az Alaptörvény csak az alapjog kereteit, főbb pontjait határozza meg: a támadásnak, melyet az arra jogosult el kíván hárítani, jogtalannak és közvetlenül fenyegetőnek kell lennie. További feltétel, hogy a támadásnak közvetlenül a személy vagy a tulajdon ellen kell irányulnia. Azt ugyanakkor az Alaptörvény nem határozza meg, hogy a megtámadott természetes személynek személyesen kellene fellépnie a jogtalan támadás ellen, márpedig, ebből az következik, hogy az érintett igénybe veheti magánbiztonsági vállalkozások e célra irányuló szolgáltatásait is [24].

Magyarországon a magánbiztonság intézményi, szervezeti feltételeit a személy-, vagyonvédelmi és magánnyomozói kamaráról szóló 1998. évi IV. törvény teremtette meg, jelenleg e törvény alapján nyílik lehetőség magánbiztonsági vállalkozások alapítására és működtetésére. Az 1998-as kamarai törvény egyes szakaszait vizsgálva mondta ki az Alkotmánybíróság, hogy a köztulajdon és a magántulajdon védelme között nem tehető különbség [25]. A tulajdonosok – legyenek azok akár az állam szervei, akár természetes vagy jogi személyek – megbízást adhatnak az arra feljogosított vállalkozásoknak meghatározott biztonsági feladatok ellátására. Lényeges ugyanakkor hangsúlyozni, hogy a magánbiztonsági vállalkozások jogosítványai jóval szűkebb körűek, mint azok, amelyekkel az állami, rendvédelmi szervek rendelkeznek. Tevékenységüket a megbízóval kötött szerződés alapján végzik, a közöttük fennálló jogviszonyra a polgári jog szabályai vonatkoznak, jogosultságaik pedig csakis addig terjednek, ameddig a megbízó jogosítványai [26]. Működésük engedélyezése és ellenőrzése ugyanakkor a rendőrség hatáskörébe tartozik, a tevékenység végzésének szabályai így a közjog területére esnek [27].

A SPORTRENDEZVÉNYEK BIZTONSÁGOS LEBONYOLÍTÁSA

A sportrendezvények biztonságos lebonyolítása két, szakmai, technikai szempontból jól elkülöníthető, ám egymással mégis szoros kapcsolatban álló területre tagolható: az egyik a létesítménybiztonság, a másik pedig a rendezésnek, a rendezvény lebonyolításának a biztonsága, vagyis a biztosítás [28].

A sportrendezvények biztosítása

Rendezvénybiztosításon – legáltalánosabb megközelítésben – a tudatos elemzések, hatástanulmányok, a tervszerű intézkedések, a folyamatos monitorozás és helyzetértékelés összességét értjük, mely az adott rendezvény zavartalanságának, a személy- és vagyonbiztonság lehető legnagyobb fokának elérését célozza. Konkrétabban megfogalmazva: a rendezvénybiztosítás azt igyekszik elérni, hogy „a rendezvényt a szervezőktől független rendkívüli esemény ne zavarja meg, ne hiúsítsa meg" [29].

A rendezvénybiztosítás feladatai a következőképpen azonosíthatók: a rendezvény jellege, célja által indokolt tárgyi és személyi feltételek, a szükséges infrastruktúrák biztosítása; a rendzavarások megelőzése, a feltehetően rendzavaró magatartást tanúsítani kívánó személyek felismerése, kiszűrése, kiemelése; a rendezvényen részt vevő személyek (legyenek jelen bármilyen minőségben) személyi és vagyonbiztonságának megőrzése; a havária, rendzavarás stb. miatt megbomlott rend mielőbbi helyreállítása; a rend megbomlására vezető okok feltárása, a rendezvénybiztosítás elemzése, értékelése [30].

A sportrendezvények biztonságának jogszabályi alapját a sportról szóló 2004. évi I. törvény (a továbbiakban: sporttörvény) jelenti, a részletszabályokat pedig a sportrendezvények biztosításáról szóló 54/2004. (III. 31.) Kormányrendelet határozza meg, illetve további speciális rendelkezéseket találunk az egyes sportági szövetségek szabályzataiban.

A sporttörvény elsődlegesen az állam sportrendezvényeket érintő szerepét és felelősségének terjedelmét határozza meg, eszerint az állam köteles gondoskodni a közbiztonságról, emellett köteles hozzájárulni e rendezvények biztonságos lebonyolításához [31].

A sportrendezvények biztonsági szempontból háromfélék lehetnek: normál, fokozott, illetve kiemelt biztonsági kockázatú. A minősítést az úgynevezett Minősítő Bizottság javaslata alapján az Országos Rendőr Főkapitányság (a továbbiakban: ORFK) végzi; a Minősítő Bizottságba az ORFK hat, a látványsportágak országos szakszövetségei egy–egy, további, a sporttörvényben meghatározott szervek ugyancsak egy–egy tagot delegálnak [32].

A sporttörvény külön fejezetben rendelkezik a sportlétesítményekről, illetve a sportrendezvények szervezési kérdéseiről. Elegendő felidéznünk a közelmúlt stadionkatasztrófáit ahhoz, hogy felismerjük, mennyire fontos az a rendelkezés, mely szerint csak olyan új sportlétesítmény építésére, illetve már létező építmény felújítására adható engedély, amely minden tekintetben megfelel a biztonságosság követelményeinek [33]. A *„versenyrendszerben szervezett versenyek lebonyolítására alkalmas sportlétesítmények"* esetében ellenőrzési kötelezettséget ír elő a törvény: minden verseny előtt, de legalább évi egy alkalommal biztonságtechnikai ellenőrzést kell tartani a rendőrség, a szakhatóságok és érintett szervek (például katasztrófavédelem, mentőszolgálat), valamint az érdekeltek (így többek között a sportszövetség, az ingatlantulajdonos, a rendezvény szervezője, illetve rendezője) bevonásával [34].

A biztonságtechnikai ellenőrzésnek ki kell terjednie a sportlétesítmény vizsgálatára (például, hogy milyen állapotban vannak a kerítések, a bejáratoknál vannak-e szűkítő folyosók, áll-e rendelkezésre elegendő parkolóhely stb.), a nézőtéri lelátó és a szektorok vizsgálatára (milyen állapotban vannak az ülőhelyek, a büfék, a mellékhelyiségek, mennyire vannak felszerelve az elsősegélynyújtó helyek, biztosítottak-e a menekülőutak, biztonságosan el vannak-e választva egymástól a hazai és a vendég szurkolói helyek stb.), továbbá a biztonságtechnikai berendezések (beléptető rendszerek, kamerarendszer, hangosbemondó stb.) működőképességének vizsgálatára [35].

A sportlétesítmények tulajdonosának, illetve üzemeltetőjének a létesítményre vonatkozó, négy évre szóló biztonságtechnikai fejlesztési tervvel és az annak megvalósítását garantáló költségtervvel kell rendelkeznie [36]. A biztonságtechnikai fejlesztési tervet az országos sportági szakszövetség véleményezi [37].

A szervező és a rendező felelőssége a sportrendezvény biztonságos lebonyolításáért

A sportlétesítmény biztonságosságáért – miként azt a fentiekben megállapítottuk – a tulajdonos, illetve az üzemeltető tartozik felelősséggel. A sportrendezvények lebonyolításáért, valamint a rendezvény ideje alatt a létesítményen belüli biztonságért a szervező felel [38]. Sportrendezvény szervezője – főszabály szerint – csak sportszervezet (sportegyesület), sportági szövetség, szakszövetség lehet [39]. A sporttörvény csak a versenyrendszerű labdarúgás esetében rendelkezik úgy, hogy a szervező köteles hivatásos (vagyis megfelelő végzettséggel rendelkező) biztonsági felelőst alkalmazni [40]. A szervező dönthet úgy, hogy rendezőt vesz igénybe a biztonsági, rendfenntartási, szervezési feladatok ellátására; ebben az esetben a szervezőt és a rendezőt egyetemleges felelősség terheli [41].

A szervező felelőssége attól az időponttól áll fenn, amikor a résztvevők megjelennek a sportrendezvény helyszínén, és egészen addig tart, amíg az utolsó résztvevő is elhagyja a sportlétesítményt [42]. 2019 óta a nézők elvonulásának biztosítására is kiemelt figyelmet kell fordítani, ezért, ha a rendőrség vagy a rendőrség távollétében a szervező úgy ítéli meg a helyzetet, hogy az ellenérdekelt szurkolói csoportok közterületi konfrontációja másként nem kerülhető el, megteheti, hogy a nézőket, illetve a nézők egy részét visszatartja (vagyis lényegében a szabad mozgásukban korlátozza) [43]. A kiemelt labdarúgó mérkőzéseket illetően további kötelezettségek terhelik a vendégcsapat sportegyesületét, amennyiben köteles a vendégszurkolók helyszínre utazását, illetve hazautazását megszervezni, továbbá az utazás ideje alatt az utazó rendezőt, a meccs során a vendég rendezőt biztosítani [44].

A szervező (és ha van, a rendező), köteles megtenni minden, a rendezvény biztonságos lebonyolítása érdekében szükséges intézkedést, illetve, ha az adott intézkedésre valamely hatóság jogosult, úgy köteles a hatóságnál kezdeményezni az intézkedés megtételét. Amennyiben a szervező nem tesz eleget a jogszabályokban, sportszövetségi szabályzatokban stb. meghatározott kötelezettségének, úgy a sportszövetség fegyelmi eljárást folytat le vele szemben [45]. A gyakorlat azt mutatja, hogy marasztaló döntés esetén a szervező a helytállási kötelezettség egy részét áthárítja a rendezőre [46]. A fegyelmi büntetéseket a Kormányrendelet sorolja fel; kiszabható például a sportszövetség által folyósított juttatások megvonása; zárt kapus mérkőzés elrendelése; az adott mérkőzés eredményének megsemmisítése; versenyből kizárás; sportszövetségből kizárás; pénzbüntetés [47].

A labdarúgó mérkőzéseknél – miként arról a fentiekben már esett szó – a sportági szövetség köteles biztonsági felelőst alkalmazni. Miután a Magyar Labdarúgó Szövetség (a

továbbiakban: MLSZ) részletesen rögzíti szabályzatában, milyen szakképesítéssel kell rendelkeznie a biztonsági felelősnek, így a szervező felelőssége korlátozott, lényegében arra terjed ki, hogy a lehető legnagyobb gondossággal járjon el a biztonsági felelős kiválasztásakor. A biztonsági felelős helytállási kötelezettsége gyakorlatilag teljes körű, és csak kivételes esetben háríthatja át, mégpedig akkor, ha a vendégszektorban bekövetkezett rendbontás a vendég rendező jogszabálysértő vagy szabályzattal ellentétes eljárására vezethető vissza [48].

Az 54/2004. (III. 31.) Korm. rendelet egyes sportrendezvények vonatkozásában az általánoshoz képest szigorúbb szabályokat állapít meg, ez a helyzet többek között bizonyos sportágak (az úgynevezett látványsportok, vagyis a labdarúgás, a vízilabda, a kézilabda, a kosárlabda, a magasabb bajnoki osztályban játszott jégkorong) esetében, továbbá akkor, ha az esemény jelentősége (például nemzetközi mérkőzés), a rendezvény helyszíne (például közterület), a nézők és résztvevők várható létszáma (minimum ötezer fő), vagy a fellépő csapattal kapcsolatban korábban elkövetett rendbontás indokolja az átlagosat meghaladó figyelmet igényel [49]. Alapesetben a sportrendezvény szervezője saját belátása szerint dönthet rendező alkalmazásáról, ellenben a most (példálózó jelleggel) felsorolt sportesemények szervezőit ilyesfajta választási lehetőség nem illeti meg, kötelesek mindenképpen rendezőt vagy rendező szervet bevonni [50].

A közterületen megrendezett, ötezer fő feletti résztvevővel számoló vagy forgalomeltereléssel, forgalomkorlátozással járó sportrendezvények szervezői a területileg illetékes rendőrkapitányságnál – díjazás fejében – rendőri biztosítást igényelhetnek. Ebben az esetben tehát egy, a rendőrség által nyújtott szolgáltatásról van szó; a feladatra a rendőrök önként jelentkezhetnek, a vállalt munkát szabadidejükben végzik el külön juttatás fejében. Jogállásukra ugyanakkor ezen idő alatt is a szolgálati törvény szabályai vonatkoznak, ha pedig a körülmények indokolttá teszik, akkor *„szolgálatba helyezik magukat”*, és a rendőrségi törvényben írtak szerint intézkednek [51].

A fentebb említett sportrendezvény kategórián belül a rendőrség, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara (a továbbiakban: Kamara) és az érintett sportszövetség képviselőiből álló testület, a korábban már említett Minősítő Bizottság kiemelt biztonsági kockázatúnak minősíthet rendezvényeket. Az ilyen sportrendezvény biztosítását – a szervező és a kötelezően alkalmazandó rendező mellett – a rendőrség közfeladatként látja el, vagyis tevékenységéért ez esetben nem jár külön díjazás [52].

Újabb tendencia, hogy – főként a labdarúgás sportág esetében – a rendező tevékenysége differenciálódik: a *Safety and Security* komplexitás tekintetében az előkészítésre helyeződik át a hangsúly. Ezt mutatja az is, hogy a sporttörvényben megjelent a közreműködő kategóriája (2019 januárjától; [53], amely fogalmilag, feladatkört és jogkört tekintve jelentősen eltér a vagyonőrtől. A közreműködő alkalmazásának rációja azon a felismerésen alapul, hogy a nézők egyre magasabb színvonalú tájékoztatást és az eddigieknél „nézőbarátabb” kiszolgálást igényelnek. Így stewardok, közreműködők fogadják a stadionba belépőket, nem pedig fegyveres biztonsági őrök, így a nézőnek nem kell már a kapukhoz érve kriminalizálva éreznie magát, a rendező, illetve a vagyonőr pedig csak akkor jelenik meg, amikor közbelépése valóban indokolt [54].

A magánbiztonság szerepe a sportrendezvények biztosításában

Rendezőként, illetve rendező szervként alkalmazott személyekkel, vállalkozásokkal szemben a jogalkotó szigorú feltételeket támaszt: rendező csak az lehet, aki személy- és vagyonvédelmi igazolvánnyal rendelkezik, megfelel a jogszabályban és a sportági szakszövetség szabályzatában előírt szakképzettségi, -képesítési elvárásoknak; rendező szervként pedig kizárólag a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: SzVMtv.) hatálya alá eső vállalkozásokkal köthető szerződés. Mindebből az is következik, hogy azoknak, akik rendezőként, rendező szerv vezetőjeként sportrendezvény biztosítására vállalkoznak, be kell tartaniuk a sporttörvény, az SzVMtv., a végrehajtási rendeletek, a sportszövetségi szabályzatok rendelkezéseit is.

Lényeges, hogy a rendező e minősége a külső jelek (ruházat, jelvény stb.) alapján egyértelműen felismerhető legyen. A rendező, a rendező szerv minden esetben a szervező utasításai alapján köteles eljárni, utasításnak kell tekinteni a szervező szabályzatában, valamint a versenykiírásokban írtakat is. A rendezői feladatokat ellátóknak kiemelt figyelmet kell fordítani a beléptetés szabályosságára: önmagában azzal jelentős mértékben csökkenthető a rendbontás veszélye, ha már a belépésnél megszűrik a nézőközönséget [55].

A sportrendezvényről a megtartás tervezett napját megelőzően legalább tizenöt nappal kell írásban értesíteni a területileg illetékes rendőrkapitányságot, Budapesten a Budapesti Rendőr-Főkapitányságot. A tájékoztatásért a szervezőt terheli a felelősség. A szervező ezen túlmenően köteles a potenciális nézőközönséget is tájékoztatni – a sportlétesítményben és azon kívül elhelyezett hirdetményekben – arról, milyen feltételek mellett látogatható a sportrendezvény. E tájékoztatás szövegét – lényegében általános szerződési feltételként – a bérleten, belépőjegyen is szerepeltetni kell. A rendezvényt biztosító őrök egyik lényeges feladata annak ellenőrzése, hogy a sportrendezvényre belépni szándékozó személyek rendelkeznek-e érvényes bérlettel, belépőjeggyel, illetve megfelelnek-e a mondott feltételeknek. Így a belépésre jelentkező személy nem állhat felismerhető módon szeszesital, kábítószer, bármilyen bódító hatású szer hatása alatt, és nem is birtokolhat ilyen szereket. Nem tarthat magánál olyan tárgyakat, melyek veszélyeztetik a rendezvény biztonságát, és amelyek bevitelét a szervező megtiltotta, és erről a belépőjegyet megvásárlókat tájékoztatta. Nem vihet be tiltott önkényuralmi jelképet, gyűlöletre uszító zászlókat, feliratokat. A beléptetést végző őröknek tehát mindezeket ellenőrizniük kell, miként azt is, hogy a belépni szándékozó személy nem áll sem eltiltás, sem kitiltás hatálya alatt [56].

Ha a szervező a nézők egyedi azonosítására alkalmas beléptető rendszert alkalmaz, akkor csak olyan bérletet, jegyet értékesíthet, amely a néző nevére szól. Ebben az esetben a rendező beléptetést végző alkalmazottja jogosult (és egyúttal köteles is) ellenőrizni a belépésre jelentkező személyazonosságát, hogy azt egybe tudja vetni a bérleten, jegyen feltüntetett személyi adatokkal; amennyiben az adatok nem egyeznek, úgy köteles megtagadni a belépést [57].

A sportrendezvények magánbiztosítására vonatkozó szabályozás értékelése

A tömegrendezvények, nagylétszámú nézőközönséget vonzó sportrendezvények biztosítása az egyik legjobb példa az állami és a magánszektor együttműködésére. Arra azonban, hogy ez az együttműködés érdemi és hatékony legyen, minden korábbinál nagyobb szükség van: ugyanis éppen ezek azok a rendezvények azok, melyek az „új típusú

kihívások" – mint amilyen a terrorizmus, a tömeges illegális migráció – szempontjából különösen kitettnek számítanak.

A XXI. század eleje – miként arra a fentiekben rámutattam – egy *„új típusú"* terrorizmust hozott el, a hálózatszerűen működő terrorista sejtek vagy éppen a magányos terroristák kora ez, a terroristáké, akik támadásaikhoz célzottan keresik az olyan helyszíneket, ahol sok ember van egyszerre jelen, és ahol a biztosítás nehezen megoldható. Az elmúlt egy–másfél évtized terrorista támadásai alapján látható a tendencia, hogy az *„olcsó terrorizmus"* irányába tolódnak el az ilyen cselekmények. Ebből következően sokkal nagyobb veszélyt hordoznak magukban a nem állami rendezvények, amelyek biztonságának vonatkozásában a magánszektor a meghatározó. Ez új, eddig ismeretlen veszélyeket, egyben új, eddig ismeretlen feladatokat jelent a szektor számára. Mindeközben lényegében nincsen e vonatkozásban érdemi tapasztalat, nincsen oktatható tudásanyag. Igaz, Magyarországon terrortámadás még nem történt, de a hazai vagyonbiztosítási szakmában dolgozók így is érzékelik a fenyegetettséget.

ÖSSZEGZÉS ÉS HELYZETKÉP

A biztonság megteremtése rendkívül összetett feladat, erre szolgálnak példaként a nagy tömegeket vonzó sportrendezvények, melyek biztosítása nem nélkülözheti az érdekeltek, vagyis a rendőrség, a katasztrófavédelem, a mentők, a sportági szövetségek és a magánbiztonsági vállalkozások együttműködését, azaz a komplex biztonsági együttműködést. Ebből következik az is, hogy törvényes és hatékony magánbiztonsági szolgáltatáshoz nem elegendő pusztán a működés kereteit meghatározó jogszabályokat megalkotni, lényeges az is, hogy megfelelőképpen összehangolják a biztonsági ágazat valamennyi szereplőjének tevékenységét, és emellett elengedhetetlen a szektorban foglalkoztatottak képzési, továbbképzési, sőt, önképzési hátterének a biztosítása. Egyet kell értenem a Cserny–Christián szerzőpáros megállapításával: mivel *„e feltételrendszer hazánkban csupán részlegesen áll rendelkezésre, a sportrendezvények biztonsága területén a feladatellátás szakmai minősége csorbát szenvedhet"* [58].

Tanulmányomban rámutattam arra, hogy Magyarországon a jogalkotó a vagyonvédelmi, magánbiztonsági tevékenység törvényi szabályozása tekintetében folyamatosan késedelemben van. A következőkben szeretném összefoglalni munkám lényegi meglátásait és egyben objektív szókimondó, feltáró kritikával meghatározni az ágazat valós problémáit.

Láthattuk, hogy több, mint nyolc évig nem létezett ágazati törvény, az 1998-ban elfogadott jogszabály pedig már az elfogadása pillanatában több ponton is kifogásolható volt, ám ugyanez elmondható a hatályos normáról, a 2005. évi CXXXIII. törvényről is, melyet kihirdetése óta csaknem harminc alkalommal kellett módosítani. Emögött az a szomorú tény húzódik meg, hogy a döntéshozók mind a mai napig nem tekintik egyenlő partnernek a magánbiztonsági szakmát, az ágazat szereplőit valójában egyetlen esetben sem vonták be a jogalkotás előkészítésébe. További kérdéseket vet fel számomra számos hiányzó vagy téves jogszabályi rendelkezés is.[2]

[2] Értelmezhetetlen azon jogalkotói szándék, mely a 9/2006 (II.27) IM rendelet eredményez. Bár állami képzésben BSC és már MSC szintű végzettséget eredményező képesítést lehet szerezni, ennek ellenére a rendelet alapján ezen szakképesítés birtokosa nem jogosult szakértői tevékenység végzésére, ellenben OKJ-s képzésben szerzett végzettséggel rendelkező igen.

Láthatóak azonban – véleményem szerint – pozitív tendenciák is, leginkább az állami oktatás létrejöttével. Komplex ismereteket biztosító BSc és MSc képzés keretében lehetséges már szakirányú diplomát szerezni, a tudományos szintű szakmai műhelyek a doktori képzést a rendészettudomány és biztonságtudomány megközelítéséből is lehetővé teszik.[3]

Aligha vitatható, hogy a tömegrendezvények, a sportrendezvények az egyik legeklatánsabb példái az állami és a – rendszerváltás során primátust szerzett magántulajdon létrejöttével okszerűen kialakult – magánbiztonsági ágazat speciális szaktudást igénylő területének együttműködésére. Elsődlegesen azért, mert napjainkra a sport – mint az egyik legjelentősebb tömegszórakoztató erő – globalizálódott. A világrendezvények résztvevői és látogatói létszáma progresszívan emelkedő. Egyre több a látványsport. Újabb és újabb sportágak jönnek létre, a sportlétesítmények befogadó képessége, így a kezelendő tömeg mértéke is emelkedik. Ezek újabb és újabb taktikákat és módszereket, új megközelítéseket igényelnek. Ezzel párhuzamosan ugyanakkor azt tapasztaljuk, hogy a világban jelen lévő etnikai, vallási feszültség nem csökken, a terrorizmus egyre inkább az olcsó (viszonylag kis befektetést igénylő), de látványos hatást ígérő cselekmények irányába halad. Ennek okán napjaink legjellemzőbb terrorista célpontjai a sport- és tömegrendezvények, melyeken gyakorlatilag fegyver alkalmazása nélkül, minimális költség és előkészület mellett a korunkra jellemző magányos terrorista elérheti célját. Ezen szempontok is azt igazolják, hogy a rendezvények, sportrendezvények magánbiztonsági feladatai tekintetében a speciális szaktudás és képzettség megkövetelése indokolt és elkerülhetetlen.

Kimondhatjuk, hogy kardinális kérdés a rendezvény helyszínének infrastrukturális megfelelősége is. E vonatkozásban elmondható, hogy hazánkban exponenciális fejlődés tapasztalható, világszínvonalú létesítmények készültek, amely biztonsági szempontból is minden tekintetben alkalmasak funkcióik betöltésére. Számomra optimizmusra ad okot a másik tényező vizsgálata is. Hiszen szemmel látható, hogy a 1990-es/2000-es évek elejére még jellemző sporthuliganizmus szignifikáns mértékben visszaszorult. A sportrendezvények ismét a sportról szólnak. Számos szakszövetség és a nemzetközi szövetségek is életképes együttműködési és biztonsági szabályrendszereket dolgoztak ki. A rendezvények biztosításában részt vevő vagyonőrök tekintetében speciális vizsga megkövetelt. Úgy vélem, hogy a sportrendezvények megfelelő biztosításához szükséges biztonsági együttműködés szakmai keretei létrejöttek.

A rendezvénybiztosítási szakterület talán az egyik legjobban működő és legjobban szabályozott területe az ezer sebből vérző magánbiztonsági ágazatnak. A szakterület további fejlődése és regnálása sem képzelhető el az ágazat generális szabályozása és újjászületése nélkül. Ez meggyőződésem. Egy gyenge ágazat erős része kevésbé lehet életképes, mint egy erős ágazat gyenge része.

A magánbiztonsági szakma hatékony működéséhez – megítélésem szerint – három dologra lenne szükség: először is szükség lenne a modern kor viszonyainak megfelelő általános és ágazati jogszabályokra. Ideértve – a teljesség igénye nélkül – az állami képzések privilegizálását, a szakmában tényked̋ők végzettségi követelményeinek átalakítását, a Szakmai Kamara valós jogkörökkel történő felruházását is. Másodsorban versenyjogi, adójogi

[3] Azonban e tárgykörben is jogalkotói mulasztás okán általános iskolai végzettséggel is van lehetőség magánbiztonsági tevékenységre, ilyen tevékenységgel foglalkozó cég alapítására és szakmai vezetésére.

és büntetőjogi eszközökkel szabályozni kellene a piac egészét, melynek során teljes paradigmaváltás keretében a megrendelői, megbízói felelősséget reális és valós súlyának megfelelően kellene értékelni és szankcionálni. El kellene érni, hogy az olcsó, de nem megfelelő minőségű szolgáltatásokat kínáló vállalkozások ne törjék le a versenyt. Végül pedig, tovább kell formálni a magánbiztonsági szakma tudományos kereteit, színvonalas szakirányú képzéseket kellene szervezni, és érdekeltté kellene tenni a vállalkozásokat, hogy támogassák foglalkoztatottjaik szakmai fejlesztését, továbbképzését.

Ennek tárgyában a magam részéről további speciális szakosítási szükségleteket érzek, fontos lenne, hogy a magánbiztonsági vállalkozások és az ilyen tevékenységet folytató személyek specializálódhassanak érdeklődési körük és a megbízói igények függvényében. Majd ezzel szoros összefüggésben indokolt lenne a szakmai kialakult tudományos hátországának meghatározó szerepet biztosítani a vonatkozó ágazati jogalkotás előkészítésében.

FELHASZNÁLT FORRÁSOK

[1] Nádori L., Gáspár M., Rétsági E., Ekler J., Szegnerné Dancs H., Woth P., Gáldi G., „Sportelméleti ismeretek," Pécsi Tudományegyetem, Szegedi Tudományegyetem, Nyugat-Magyarországi Egyetem, Eszterházy Károly Főiskola, Dialóg Campus Kiadó-Nordex Kft., 2011. Elérhető: https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0025_Nadori-Dancs-Retsagi-Ekler-Gaspar-Sportelmeleti_ismeretek/ch06s04.html (letöltés ideje: 2021.09.11.)

[2] Tóth N. Á., „A sportrendezvények biztosítása az antik Róma sportjogában a hatályos hazai szabályrendszer figyelembevételével," *Sectio Juridica et Politica,* Miskolc, Tomus XXIX/1. (2011) pp. 153–166. p. 153. Elérhető: http://midra.uni-miskolc.hu/document/12292/4364.pdf (letöltés ideje: 2021.09.05.)

[3] Tóth (2011) i.m. p. 153.

[4] Onyestyák N., „A sport és politika kapcsolata Magyarországon az 1980-as években a nyári olimpiai játékok tükrében", Doktori értekezés, Budapest, Semmelweis Egyetem Sporttudomány Doktori Iskola, 2010. Elérhető: http://old.semmelweis.hu/wp-content/phd/phd_live/vedes/export/onyestyaknikoletta.d.pdf (letöltés ideje: 2021.09.04.)

[5] Molnár Cs., Remenyik B., „A megasportesemények turisztikai hatásai Magyarországon," *Területi Statisztika* 2019. (59)3. pp. 300–327. pp. 304–306. Elérhető: https://www.ksh.hu/docs/hun/xftp/terstat/2019/03/ts590303.pdf (letöltés ideje: 2021.09.04.)

[6] Freyer T., „A rendvédelmi erők harca a futball-huliganizmus ellen Magyarországon," Doktori értekezés, Budapest, Semmelweis Egyetem Doktori Iskola Semmelweis Egyetem, Testnevelési és Sporttudományi Kar Nevelés-és Sporttudományi Doktori Iskola, 2004. p. 102. Elérhető: http://old.semmelweis.hu/wp-content/phd/phd_live/vedes/export/freyertamas.d.pdf (letöltés ideje: 2021.09.04.)

[7] Freyer (2004) i.m. p. 102.

[8] Less (2017) i.m. p. 100.

[9] Drury, J., Reicher, S., „Collective Psychological Empowerment as a Model of Social Change: Researching Crowds and Power," *Journal of Social Issues*, Vol. 65, No. 4, 2009.

[10] Less (2017) i.m. p. 106.

[11] Takács A., „Valljuk, hogy a polgárnak és az államnak közös célja a jó élet, a biztonság, a rend, az igazság, a szabadság kiteljesítése," In: Patyi András (szerk.), *„Rendhagyó kommentár egy rendhagyó preambulumról,"* Budapest, Dialóg Campus, 2019. p. 339.
[12] Cserny Á., Christián L., „Gondolatok a (sport)rendezvények biztonságának fokozásához," Belügyi Szemle, 2020/11. pp. 71–88. Elérhető: https://ojs.mtak.hu/index.php/belugyiszemle/article/view/4926/3968 (letöltés ideje: 2021.09.05.)
[13] Boda J., „Rendészettudományi szaklexikon," Budapest, Dialóg Campus, 2019. p. 66.
[14] Gazdag F. (szerk.), „Biztonságpolitika – Biztonsági tanulmányok," Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2011.

[15] Finszter G., „A rendészeti szervek működésének jogi alapjai," Budapest, RTF Alkotmányjogi és Közigazgatási Jogi Tanszék, 2008. p. 55.
[16] Christián L., „Alternatív rendészet," Doktori értekezés. Budapest, Pázmány Péter Katolikus Egyetem, 2010. p. 119.
[17] Finszter (2008) i.m. p. 24.
[18] 13/2001. (V.14.) AB határozat III. 1.6.1. pont.
[19] Christián (2010) i.m. p. 120.
[20] Németh Zs., „A civil szféra a közbiztonságban," In *„Ünnepi kötet Vavró István professzor 80. születésnapjára,"* Magyar Statisztikai Társaság – Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, 2016. pp. 137–147. p. 140.
[21] Kacziba A., „Közrend, magánrend, közbiztonság," In: Gál Gy., Hautzinger Z. (szerk.), Pécsi Határőr Tudományos Közlemények. 2013. XIV. sz. pp. 23–36. pp. 33–34
[22] Kerezsi K., Nagy V., „A rendészettudomány kritikai megközelítése," In Boda J., Felkai L., Patyi A. (szerk.), *„Ünnepi kötet a 70 éves Janza Frigyes tiszteletére,"* Budapest, Dialóg Campus, 2017. p. 275.
[23] Christián L., „A magánbiztonság megközelítésének egyes aspektusai," In: Christián L., *„A magánbiztonság elméleti alapjai,"* Budapest, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014. p. 22.
[24] Christián (2014) i.m. p. 20.
[25] 3/2001. (I.31.) AB hatz. III. 1.1. pont.
[26] Christián (2014) i.m. p. 22.
[27] Boda (2019) i.m. p. 373.
[28] Cserny–Christián (2020) i.m. p. 77.
[29] Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara, „Sportrendezvények biztonsága és biztosítása," Tanulmánygyűjtemény, 2006. p. 41. Elérhető: https://szakmaikamara.hu/files/images/Orszagos/Sportrendezveny/szakkonyv.pdf (letöltés ideje: 2021.09.02.)
[30] Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara (2006) i.m. p. 41.
[31] 2004. évi I. törvény a sportról 49. § k) pont.
[32] 54/2004. (III. 31.) Korm. rendelet a sportrendezvények biztonságáról 2. §
[33] 2004. évi I. tv. 63. § (1) bek. a) pont).
[34] 2004. évi I. tv. 63. § (3) bek.
[35] 54/2004. (III. 31.) Korm. rend. 13. §
[36] 2004. évi I. tv. 63. § (3a) bek.
[37] 54/2004. (III. 31.) Korm. rend. 13. § (4) bek.

[38] 2004. évi I. tv.. 66. § (1) bek., 68/A. § (3) bek
[39] 2004. évi I. tv. 65. § (2) bek.
[40] 2004. évi I. tv. 65. § (3) bek.
[41] 2004. évi I. tv.. 66. § (1) bek.
[42] 2004. évi I. tv. 66. § (3) bek.
[43] 2004. évi I. tv.. 68. § (9) bek.
[44] Cserny–Christián (2020) i.m. 78.
[45] 2004. évi I. tv.. 66. § (4) bek.
[46] Cserny–Christián (2020) i.m. p. 78.
[47] 54/2004. (III. 31.) Korm. rend. 18. §
[48] Cserny–Christián (2020) i.m. p. 78.
[49] 54/2004. (III. 31.) Korm. rend. 1. § (1) bek.
[50] 54/2004. (III. 31.) Korm. rend. 6. §
[51] 54/2004. (III. 31.) Korm. rend. 5. §
[52] 2004. évi I. tv. 68/A. § (4) bek.
[53] 2004. évi I. tv. 69/B. §
[54] Cherny–Christián (2020) i.m. p. 81.
[55] Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara (2006) i.m. pp. 58–59.
[56] Csege Gy., „Magánbiztonság II.," A kiadvány „A versenyképes közszolgálat személyzeti utánpótlásának stratégiai támogatása" elnevezésű projekt keretén belül készült. Budapest, Belügyminisztérium, 2018. p. 199. Elérhető: http://bmkszf.hu/dokumentum/2709/Maganbiztonsag_II.pdf (letöltés ideje: 2021.09.02.)
[57] Csege (2018) i.m. p. 200.
[58] Cserny–Christián (2020) i.m. p. 76.

COVID-19 AND LABOR SAFETY

QUANTITATIVE SURVEY OF THE PRACTICE OF PROTECTION AGAINST CORONA VIRUS EPIDEMIC OF COMPANIES OPERATING IN HUNGARY

COVID-19 ÉS MUNKAVÉDELEM

MAGYARORSZÁGON MŰKÖDŐ VÁLLALATOK KORONAVÍRUS-JÁRVÁNY ELLENI VÉDEKEZÉSI GYAKORLATÁNAK KVANTITATÍV FELMÉRÉSE

FARAGÓ Ferenc[1]

Abstract

Control of the coronavirus epidemic has become a priority for companies, posing a significant challenge for both company executives and occupational safety professionals. Eighteen months after the domestic release of COVID-19, we examined the company's systematic system for controlling the epidemic and its effectiveness. We conducted quantitative research involving 78 domestic companies using an online questionnaire survey. Our study points out that companies were not prepared for such a large-scale health emergency, but recognized their role and introduced technical, hygienic, organizational measures to protect the health of their employees. The control procedures used are not uniform, and in addition to the rules proposed by epidemiological organizations, efforts have been made to prevent the spread of the disease by developing and implementing additional measures.

Keywords

COVID-19, pandemic, occupational health and safety, health emergency, epidemic control, management system

Absztrakt

A koronavírus-járvány elleni védekezés a vállalatok egyik kiemelt feladatává vált, mely jelentős kihívást jelentett mind a cégvezetők, mind a munkavédelmi szakemberek számára. Tizennyolc hónappal a COVID-19 hazai megjelenése után megvizsgáltuk a járvány elleni védekezés vállalati módszereit és annak eredményességét. Kvantitatív kutatást végeztünk, 78 hazai vállalat bevonásával, online kérdőíves felméréssel. Tanulmányunk rámutat arra, hogy bár a vállalatok nem voltak felkészülve egy ilyen nagy mértékű egészségügyi vészhelyzetre, de felismerték szerepüket és műszaki, higiéniai, szervezési intézkedéseket vezettek be munkavállalóik egészségének megóvása érdekében. Az alkalmazott védekezési eljárások nem egységesek, a járványügyi szervezetek által javasolt szabályokon túl további intézkedések kidolgozása és bevezetése révén igyekeztek a betegség terjedését megakadályozni.

Kulcsszavak

COVID-19, pandémia, munkavédelem, munkahelyi egészségvédelem, egészségügyi vészhelyzet, járvány elleni védekezés, irányítási rendszer

[1] farago.ferenc@uni-obuda.hu | ORCID: 0000-0001-6627-9604 | PhD Student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonság-tudományi Doktori Iskola

BEVEZETÉS

A világméretűvé vált koronavírus-járvány az elmúlt időszak egyik legnagyobb kihívása lett. A társadalom minden szereplőjét komoly megpróbáltatás elé állította a járvány tovább terjedésének megfékezése és a megbetegedések számának visszaszorítása érdekében vívott harc. Gyors terjedése, a fertőzés- és hatásmechanizmusával, tüneteivel kapcsolatos információk hiánya, illetve a betegség súlyos és előre nem látható szimptómái rendkívül megnehezítették a védekezést. Természetesen a vállalatok működését is nagymértékben befolyásolta a pandémia, hiszen a munkahelyi közösségekben a fertőzések kockázata igen magas. A munkáltatók jogszabályban előírt felelőssége az egészséget nem veszélyeztető és biztonságos munkavégzés feltételeinek biztosítása. A COVID-19 elleni védekezés feladata tehát – szervezett munkavégzés esetén – részben a munkavédelmi szakemberek felelősségévé vált.

A koronavírus-járvány első magyarországi esetét 2020. márciusában regisztrálták, majd ezt követően folyamatosan nőtt az aktív esetszám és a vírus különböző variánsai újabb és újabb fertőzési hullámokat eredményeztek. A vállalatoknak válaszolniuk kellett a pandémiára, betartva azokat a szabályokat, amelyeket egyrészről a kormány, másrészről pedig a szakmai szervezetek javasoltak, szükség szerint kiegészítve az intézkedéseket a saját eljárásaikkal. Tizennyolc hónappal a COVID-19 hazai megjelenése után megvizsgáltuk a járvány elleni védekezés vállalati szisztematikus rendszerét és annak eredményességét. Kutatásunk célja a Magyarországon működő vállalatok koronavírus-járvány elleni védekezési gyakorlatának és módszereinek felmérése. 78 hazai vállalat bevonásával készült kvantitatív vizsgálat eredményei alapján arra adtunk választ, hogy a munkáltatók munkavédelmi szempontból milyen problémákkal küzdöttek meg a pandémia kapcsán, hogyan kezelték az előírt, illetve javasolt szabályokat, milyen intézkedéseket dolgoztak ki és ezeket hogyan építették be a vállalat szabályozási rendszerébe.

SZAKIRODALMI ÁTTEKINTÉS

A COVID-19 okozta pandémia viszonylag rövid idő alatt gyökeresen változtatta meg a társadalom mindennapi életét, merőben szokatlan, új helyzetet teremtve a gazdaság minden szereplője számára. Ebben a rendkívüli állapotban működésük biztonsága érdekében reagálniuk kellett a cégeknek is. Az üzletmenet folytonosságának biztosításához a vállalatoknak változtatni kellett szervezeti magatartásukon, üzleti stratégiájukon, hogy alkalmazkodni tudjanak a megváltozott körülményekhez. Számos tanulmány foglalkozott a vállalatok pandémiára adott válaszával hazánkban is, amelyek elsősorban a gazdaságra gyakorolt hatás, illetve az emberi erőforrás menedzsment (HR) oldaláról vizsgálták a változásokat és kihívásokat. Tanulmányában Kópházi [1] megemlíti, hogy a szervezetek többsége akkor vezet be alapvető változásokat, ha komoly külső hatások erre kényszerítik. A változások eredményességéhez azonban átgondolt, megalapozott lépések szükségesek. Kópházi megállapítja továbbá, hogy a szervezetek többsége nem készült fel a krízishelyzetek kezelésére. Emiatt, illetve a járvány első hulláma idején a kormány által bevezetett korlátozó intézkedések hatására nagymértékben változott a vállalatok gazdálkodása és a munkaerő piac. Csökkent az ipari termelés és foglalkoztatottság. [2] Más kutatók is megerősítik ezt a káros hatást, kiemelve, hogy nem minden szektort érintett egyformán a járvány. [3], [4] Pirohov

és Tóth rámutatnak, hogy a nagyvállalatok pénzügyileg stabilabb helyzete kedvezőbb feltételeket biztosított a krízis kezeléséhez, továbbá kisebb mértékű veszteséget szenvedtek azok a gazdasági szektorok, amelyek képesek voltak gyorsan alkalmazkodni a pandémia megjelenése után kialakult körülményekhez. [5] Nem vitatott a kényszerítő intézkedések szükségessége (karantén, üzletek, szolgáltató helyek bezárása), ugyanakkor látható a vállalatvezetéssel kapcsolatos prioritások átrendeződése. Rövid idő alatt kiemelkedő szerepet kapott a munkahelyi egészségvédelem és egészségmegőrzés, mely a pandémia okozta válság átvészelésének stratégiai kérdésévé vált. Felértékelődött a munkavállalók egészségének és biztonságának fontossága, mert ez a vállalatok fenntartható működésének egyik alappillére lett. Az egészséget nem veszélyeztető és biztonságos munkavégzés feltételeinek megteremtése a munkáltatók kötelezettsége, így a COVID-19 elleni védekezés feladatai – szervezett munkavégzés esetén – részben a munkavédelmi szakemberek felelősségévé váltak.

Henk de Vires, a szabványosítás-menedzsment kitüntetett professzora a COVID-19 vírus hatásmechanizmusán keresztül vizsgálta a különböző intézkedéseket. [6] Tanulmányában kiemeli, hogy a védekezési eljárások kidolgozása során a politikai döntéshozók, kormányok megpróbáltak olyan intézkedéseket hozni, amelyek védik a közegészséget, anélkül, hogy túlságosan akadályoznák a társadalom működését. A vállalatok célja hasonlóképpen az, hogy megvédjék munkavállalóik, ügyfeleik egészségét a működésük fenntartása mellett. Henk a vírus terjedésének módjait elemezte és kapcsolta össze az üzleti tevékenységekkel. Alapvetően ez a gyakorlati megközelítés működött hazánkban is, hiszen a járvány megfékezésének a legfontosabb tényezője az elkülönítés volt, vagyis a fertőzés lehetséges tovább terjedésének megakadályozása az emberi kapcsolatok csökkentése révén a terjedési mechanizmusok figyelembevételével. A vírus érintéssel (tárgyak vagy személyek), cseppfertőzéssel (más személyről cseppekkel közvetlenül, vagy a levegőn keresztül cseppek, illetve aeroszol formájában) terjed. A szakemberek véleménye eltér a különböző fertőzési utak hatékonyságát tekintve. Tanulmányában Goldman [7] rámutat például arra, hogy az élettelen felületeken keresztüli terjedés esélye rendkívül csekély, csak olyan esetekben fordulhat elő, amikor a fertőzött személy a felületre köhög vagy tüsszent, és valaki más nem sokkal a köhögés vagy tüsszentés után (1-2 órán belül) megérinti a felületet. Vizsgálatai szerint hosszabb távon a vírus nem marad életképes a felületeken. A legbiztonságosabb módszer mindazonáltal minden lehetséges fertőzési útvonal figyelembevétele a munkavállalók, az ügyfelek, valamint a munkavállalók és az ügyfelek közötti kapcsolatokban. Ez alapot adott a vállalatvezetők és a munkavédelmi szakemberek számára az intézkedések kialakításához.

A munkavédelem módszertana alapvetően kockázatszemléletű. Ahogy Szabó fogalmaz: „a munkahelyi balesetmegelőzés és egészségmegőrzés meghatározó eszköze a kockázatkezelés, és alapfogalma a kockázat.” [8] A kockázatok kezelésének alapelve az oksági összefüggések feltárása és értékelése, illetve az események bekövetkezési valószínűségének becslése. A munkavédelemben tehát általában a kockázatok értékelése jelenti az első lépcsőt a megalapozott megelőző intézkedések kidolgozásához. A kockázatértékeléshez viszont elengedhetetlen, hogy megfelelő információk álljanak a szakemberek rendelkezésére, amely alapján a kockázatok, az azokból származtatott veszélyek vagy esetek, illetve azok bekövetkezésének valószínűsége meghatározható. A pandémia alatt a kockázatértékeléseket megalapozó, elegendő információ hiánya megnehezítette a kockázatértékelési módszertan alkalmazását a járvány elleni védekezési stratégiák kialakításakor.

A vállalatok biztonsággal kapcsolatos eszközrendszerének a része a különböző veszélyhelyzetekre való felkészülés, az ezekre kidolgozott vészhelyzeti tervek. [9] A tömeges megbetegedések elkerülésére és a járványok hatásainak csökkentésére kidolgozott speciális cselekvési terv a pandémiás terv. Elkészítése állami intézmények számára kötelező, de gyakran vállalatok is készítenek a különböző járványok elleni védekezési intézkedéseket tartalmazó terveket. A pandémiás terv célja, hogy a tervben meghatározott intézkedések által biztosítható legyen (pandémiás időszakban) a vállalat folyamatos működése. [10] Alapot biztosít a pandémiás megbetegedések elleni felkészüléshez, a szükséges erőforrások meghatározásához. Előre kidolgozott intézkedési rendszert biztosít a pandémia megelőzésére, a járvány következményeinek csökkentésére.

Segítséget jelenthetnek a krízishelyzetek leküzdésében a különböző vállalatirányítási rendszerek. A vonatkozó szabványok követelményei között megtalálható a felkészülés és reagálás vészhelyzetre című szabvány fejezet, amely kifejezetten a szervezet működését befolyásoló kockázatok számbavételét és azok kezelését várja el a vállalatoktól. Az ISO 45001 szabványon alapuló Munkahelyi Egészségvédelem és Biztonság Irányítási rendszere (röviden: MEBIR) szintén megfogalmazza ezeket a követelményeket. Az itt említett szabványi elvárásoknak való megfelelés segítheti a vállalatokat a pandémia által okozott helyzetben, mert felkészíti a szervezetet a váratlan események kezelésére, illetve kialakítja a megelőzéshez, felkészüléshez szükséges szemléletet. Ugyanakkor a konkrét utasításokkal szemben lehet előnye a teljesítménykövetelményeket megfogalmazó szabályozóknak. Henk szabványosítási szakértőkre hivatkozva megemlíti, hogy a teljesítménykövetelményeket előíró szabályok általában jobbak, mint a bizonyos megoldásokat előíró szabályok, mert az előbbiek ösztönzik a kreativitást, hogy a vállalatok a követelményeknek leginkább megfelelő megoldással álljanak elő. [6]

Pandémiás helyzetben az információkat többnyire a járványügyi szervezetek biztosítják, amelyek a járvány kialakulásának, terjedésének nyomon követéséért felelősek. A különböző szakmai szervezetek, például az Egészségügyi Világszervezet (WHO), vagy hazánkban a Nemzeti Népegészségügyi Központ tájékoztatói fontos információkat biztosíthatnak a vállalatok járvány elleni védekezéséhez. Előfordul, hogy más szervezetek is közzétesznek olyan információkat, amelyek segítik a járvány elleni védekezést. Ilyen például a Nemzetközi Szabványügyi Testület, az ISO által kiadott "ISO/PAS 45005:2020 A munkahelyi egészségvédelem és biztonság irányítása. Általános útmutatók biztonságos munkavégzéshez a Covid19-járvány idején" című dokumentuma [11], amely összegyűjtve tartalmazza mindazokat a szükséges, illetve javasolt intézkedéseket, amelyeket a munkáltatók a betegség terjedésének megakadályozása érdekében megtehetnek. A PAS (Publicly Available Specifications, nyilvánosan elérhető specifikáció) egy szabványosítási dokumentum, amely szerkezetében és formátumában nagyban hasonlít egy adott szabványhoz, de eltérő fejlesztési modellel rendelkezik. A PAS-okat gyakran sürgős piaci igények alapján állítják elő, a szabványosítás felgyorsításának céljából. Az ISO arra törekedett, hogy a dokumentumban szereplő útmutatás végrehajtásával a szervezetek legyenek képesek hatékony intézkedéseket hozni a munkavállalók és más érdekelt felek védelme érdekében a COVID-19 kockázataival szemben és egyben igazolják, hogy a COVID-19-hez kapcsolódó kockázatokat kezelik, illetve olyan keretet hozzanak létre, amely lehetővé teszi a változó helyzethez való hatékony és időben történő alkalmazkodást.

MÓDSZERTAN

Kvantitatív kutatásunk a Magyarországon működő vállalatokra terjedt ki. Az adatgyűjtést online végeztük, kérdőív segítségével. A kérdőíven egy válaszos, több válaszos zárt kérdések, valamint nyitott kérdések, rövid szöveges válaszadási lehetőséggel szerepeltek. A kérdőívet kismintás, 15 fős kipróbálás és az érintettekkel való megbeszélés után véglegesítettük. A végleges kérdőív hivatkozását munkavédelmi szakemberek szakmai csoportjaihoz juttattuk el. A kvalitatív felmérés 2021. április 12. és május 31-e között történt és a következő hipotéziseken alapult:

H1: A vállalatok felismerték szerepüket és felelősségüket a COVID-19 járvány elleni védekezésben.

H2: A vállalatok tettek intézkedéseket a pandémia terjedésének megfékezésére és ezek az intézkedések lokális szinten eredményesek voltak.

H3: A kockázatértékelés módszertana az információk szűkössége miatt nem volt teljeskörűen alkalmazható, de képes volt alapot biztosítani a védekezési eljárások kialakításához.

H4: Az irányítási rendszerrel rendelkező vállalatok könnyebben építették be folyamataikba a védekezés érdekében hozott intézkedéseiket, a szabványosítás (pl. PAS) segít a hasonló esetek kezelésében.

A vizsgálatba bevont vállalatokat két platformon értük el:

- Online: Közösségi oldalon, Facebookon munkavédelmi szakmai csoportokban megosztottuk a Google-kérdőívet, és a bejegyzésben ismertettük a koronavírus-járvány elleni védekezésre vonatkozó felmérésünk célját.
- Szakmai szervezeten keresztül: Tanúsító cég Magyarországon működő szervezetét kértük meg, hogy juttassa el partnereihez a kutatásban való részvételre felkérő levelünket, mely tartalmazta a kérdőívre mutató hivatkozást.

Összesen 78 db értékelhető kérdőív képezi a mintát. A válaszadó cégek neve és működésük székhelye nem azonosítható, mert anonim módon végeztük a felmérést, de eredménye vélhetően mégis közelít egy országos lefedettségű, reprezentatív kutatás eredményéhez. A vállalatok nagyságrendjét az alkalmazotti létszám alapján határoztuk meg. A vizsgálati mintában a mikro vállalattól a nagyvállalati méretig minden vállalkozási nagyságrend megtalálható. A felmérésben részt vevő cégek létszám szerinti megoszlása az 1. táblázat szerint alakul.

Létszám kategória	Válaszadók száma (db)	Válaszadók aránya (%)
0-10 fő	13	16,7
11-50 fő	19	24,4
51-200 fő	23	29,6
201-500 fő	13	16,7
501-1000 fő	5	6,4
1000 fő fölött	5	6,4
Összesen	*78*	*100*

1. Táblázat: A kutatásban részt vevő vállalatok vállalati nagyságrend szerint, saját szerkesztés

A felmérésben részt vevő vállalatok tevékenységi köre a gazdasági tevékenységek ágazati osztályozásának széles körét lefedi, így a kutatás szempontjából reprezentatívnak tekinthető. Az adatfeldolgozást leíró statisztika segítségével és szövegelemzési módszerrel végeztük.

Tevékenység kör	Válaszadó (db)
Élelmiszeripar	18
Gép-, alkatrész gyártás	14
Szolgáltatás (tanácsadás, K+F, karbantartás stb.)	10
Kereskedelem	8
Nem jelölte meg	8
Mezőgazdaság	4
Építőipar	4
Vegyipar	4
Nyomdaipar, papírgyártás	4
Energiaipar	2
Gyógyszeripar	1
Szállítmányozás	1
Összesen	*78*

2. Táblázat: A kutatásban részt vevő vállalatok tevékenység szerint, saját szerkesztés

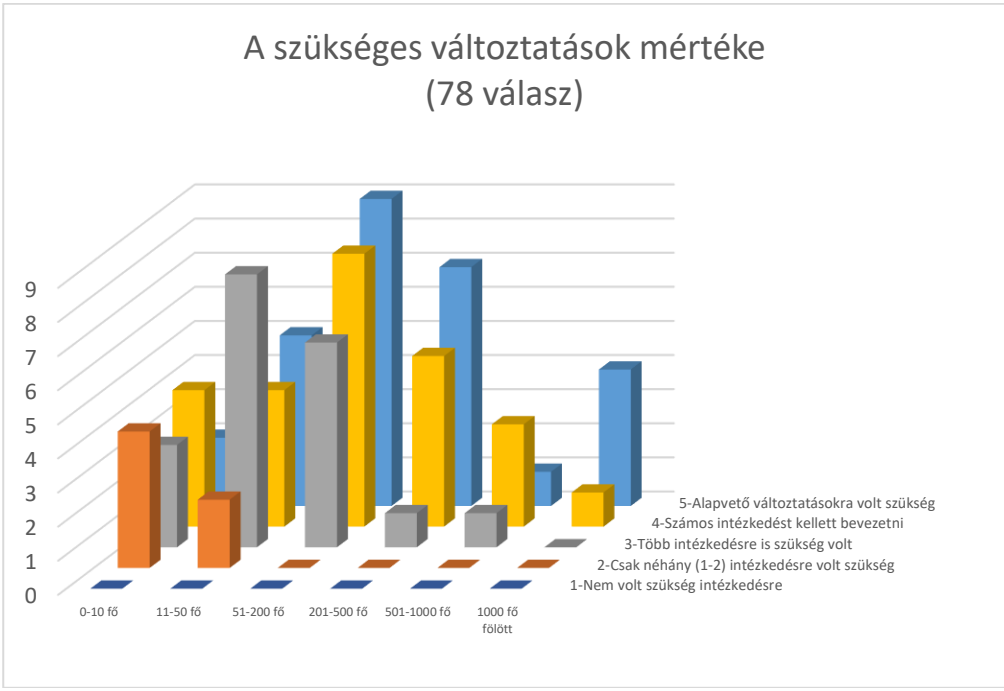
A KUTATÁS EREDMÉNYEI

Az első kérdéscsoporttal azt vizsgáltuk, hogy a vállalatok mennyire tartották szükségesnek működésük módosítását, illetve milyen információk alapján vezettek be intézkedéseket a koronavírus-járvány elleni védekezés érdekében.

Ebben a témakörben a felmérés első kérdése így szólt: „Az Ön vállalata vezetett be intézkedéseket a COVID-19 elleni védekezés céljából?" 5 pontos Likert-skálát alkalmaztunk, hogy megértsük a válaszadók preferenciáit. A skála szintjeihez az alábbi kódok tartoztak:

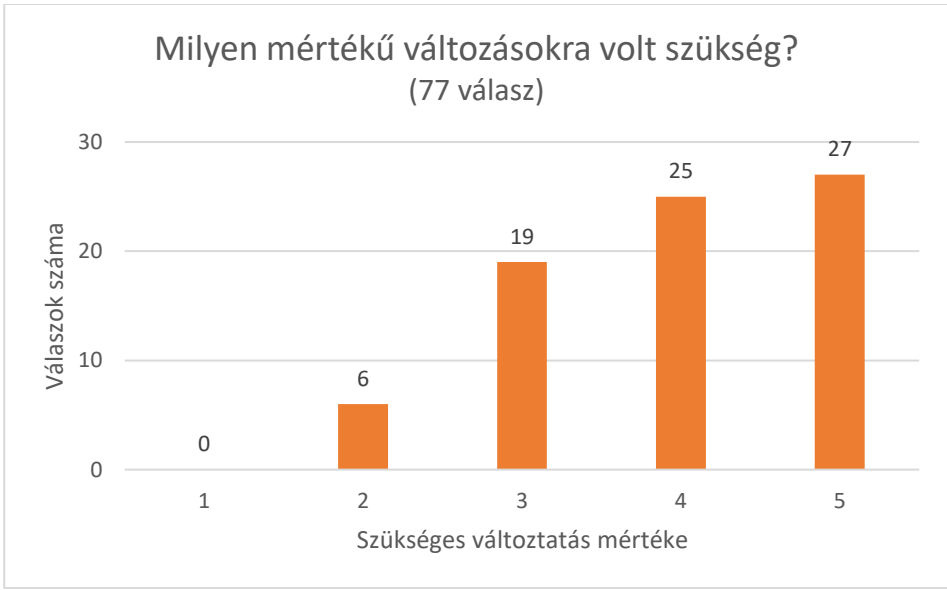
1 – Nem volt szükség intézkedésre
2 – Csak néhány (1-2) intézkedésre volt szükség
3 – Több intézkedésre is szükség volt
4 – Számos intézkedést kellett bevezetni
5 – Alapvető változtatásokra volt szükség

A kérdésre 78 válasz érkezett. A kapott eredményeket először a vállalati nagyságrend szerint rendeztük és átlagoltuk, hogy megvizsgáljuk a szervezet mérete és a szükségesnek ítélt változások mértéke közötti összefüggést.



1. Ábra: A vállalatok által szükségesnek ítélt változások mértéke, saját szerkesztés

Kódonként is összegeztük az érkezett válaszok számát.



2. Ábra: Az egyes kódokra érkezett válaszok, saját szerkesztés

A kérdéscsoport második kérdése a vállalatok által bevezetett konkrét intézkedési formákra vonatkozott. 15 előre meghatározott intézkedést (a koronavírus-járvány terjedésének megakadályozása érdekében leggyakrabban alkalmazott eljárásokat) tüntettünk fel a válaszok között, melyek együttes kiválasztására is lehetőség volt. Egyéni válaszadásra az „Egyéb" választási lehetőség megjelölésével és a válasz mező kitöltésével volt mód. A kérdésre 78 válasz érkezett.

Intézkedések	db
Védőeszköz (maszk) használat. A maszkot a vállalat biztosítja	70
Kézfertőtlenítő állomások elhelyezése	69
Munkavállalók oktatása, tájékoztató anyagok kihelyezése	61
Home office bevezetése	60
A munkahelyek rendszeres fertőtlenítése	59
Felfüggesztettük az üzleti utazásokat	53
Lázmérés a belépéskor	47
Áttértünk online kapcsolattartásra / értékesítésre	39
Távolságtartás (min 1,5 m) biztosítása a munkahelyeken és a közös helyiségekben (étkező stb.)	37
Rendszeres COVID tesztek a munkavállalók körében	29
Munkavállalók elkülönítése (védőfal stb.)	25
Ügyfelek elkülönítése (védőfal stb.)	15
Átmenetileg felfüggesztettük a tevékenységet, de a cégünk már ismét működik	7
Védőeszköz (maszk használat). A maszkot a vállalat nem biztosítja	2
Felfüggesztettük a működést, jelenleg sem működünk	1
Egyéb	18

3. Táblázat: A vállalatok által bevezetett intézkedések, saját szerkesztés

Az „Egyéb" kategóriára érkezett egyéni válaszokat módszerek szerint (elkülönítés, fertőtlenítés, védőeszközök használata, tesztelés stb.) csoportosítottuk és az eredmények értékelésénél figyelembe vettük.

A védekezési módszerekre vonatkozó kérdéscsoport harmadik pontjában megkértük a kutatásban részt vevőket, hogy osszák meg azon egyedi intézkedéseiket és eljárásaikat, amelyek az előző pont listájában nem szerepeltek. Erre az előző kérdés „Egyéb" pontjánál is lehetőség volt, de a vállalatok eljárásainak mélyebb megismerése érdekében külön kérdés segítségével is megpróbáltunk tájékozódni. Néhány pontban duplikált válaszokat kaptunk, de érkezett új információ is, amely tovább bővítette a kutatás eredményeit.

Tekintettel arra, hogy a koronavírus-járvány első szakaszában a COVID-19 vírus terjedési és hatásmechanizmusai nem voltak ismeretesek, illetve nem állt rendelkezésre elegendő információ a vírussal, valamint az általa okozott betegséggel kapcsolatban, megvizsgáltuk, hogy a döntéshozók milyen információkra alapozva dolgozták ki védekezési eljárásaikat. A kérdésre 77 válasz érkezett.

Válaszok	db
Kormányzati utasítások, szabályzók alapján	64
Szakmai szervezetek javaslatai alapján	40
Saját tapasztalatunk alapján	39
A cégközpont (HQ) utasításai alapján	25
Más cégek intézkedéseinek figyelembevételével	20
Fehér Könyv, anyavállalat intézkedései alapján, HR és munkavédelmis csoportokból szerzett infók alapján, fogl-eü orvos ajánlásai alapján	1
Munkabiztonsági kockázatértékelés figyelembevételével	1

4. Táblázat: A vállalatok intézkedéseit megalapozó információforrások, saját szerkesztés

A koronavírus-járvánnyal kapcsolatos információk forrására és az ismeretek megosztására vonatkozó további kérdés az együttműködő szervezetekre vonatkozott, vagyis azokra az érintettekre, akikkel a vállalatok a védekezési eljárások kialakítása során szakmai egyeztetést végeztek. A kérdőív ide vonatkozó pontja: „Jelölje meg, kiket vontak be a védekezési eljárások kialakításába!" öt előre megadott választ tartalmazott, illetve lehetőség volt egyéni válasz megadására is.

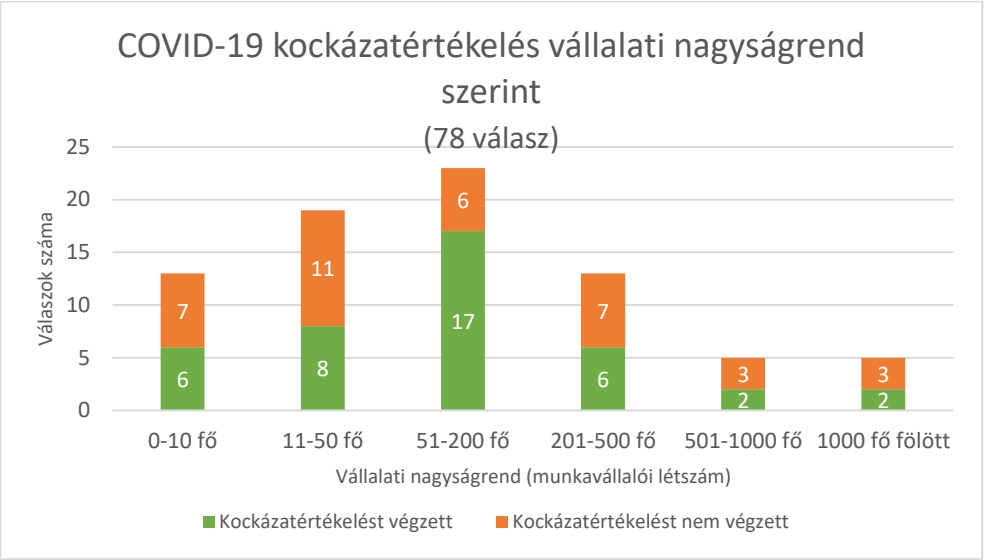
Válaszok	db
Egyeztettünk partnereinkkel és ügyfeleinkkel	42
Egyeztettünk a helyi hatósággal	16
Egyeztettünk a munkavállalókkal / munkavállalói képviselőkkel	58
Külső szakértőket kértünk az eljárások kidolgozására	7
Szakmai szervezetek, hálózatok tagjaiként kaptunk megoldásokat	13
Saját döntésünk alapján	1
Üzemorvos bevonása	2
Foglalkozás-egészségügyi szolgálat	1
Foglalkozás-egészségügyi szolgáltató, munkabiztonsági szakember	1
Foglalkozás-egészségügyi orvos	1
Saját hatáskörben alakítottuk ki az eljárásokat, a később elkészülő szakmai ajánlásokat utólag áttekintettük, de módosítás nem volt szükséges	1
NÉBIH dokumentációk, Vállalati Fehér könyv segítségével	1
Saját vezetőségünket vontuk be	1
Anyavállalat, takarító cég	1
Cégközpont utasítása alapján	1
Kormányzati intézkedéseket figyelve hoztuk meg saját, belső intézkedéseinket	1
Más cégekkel egyeztettünk	1

5. Táblázat: A vállalatok által a védekezési eljárásba bevont partnerek, saját szerkesztés

A kutatás során megvizsgáltuk, hogy a vállalatok végeztek-e a koronavírus-járvánnyal és annak lehetséges hatásaival kapcsolatos kockázatértékelést? Elemeztük továbbá, hogy a különböző vállalati nagyságrend szerint milyen arányban történt COVID-19 specifikus kockázatértékelés a vállalatoknál. A kérdésre 78 válasz érkezett.

Válaszok	db	%
Igen	41	52.6
Nem	37	47.4

6. Táblázat: COVID-19 kockázatértékelést végzett a vállalat?, saját szerkesztés



3. Ábra: COVID-19 kockzázatértékelések aránya vállalati nagyságrend szerint, saját szerkesztés

A következő kérdéscsoport annak megismerésére szolgált, hogy a koronavírus-járvány elleni védekezés érdekében hozott intézkedéseket a vállalatok milyen módon illesztették a szabályozási rendszerükbe? A kérdéscsoport első kérdése a belső szabályozás kialakítására vonatkozott: ”Hogyan történt az Ön cégénél a járvány elleni védekezésre vonatkozó belső szabályozás?” A kérdésre minden cég válaszolt, így 78 válasz érkezett.

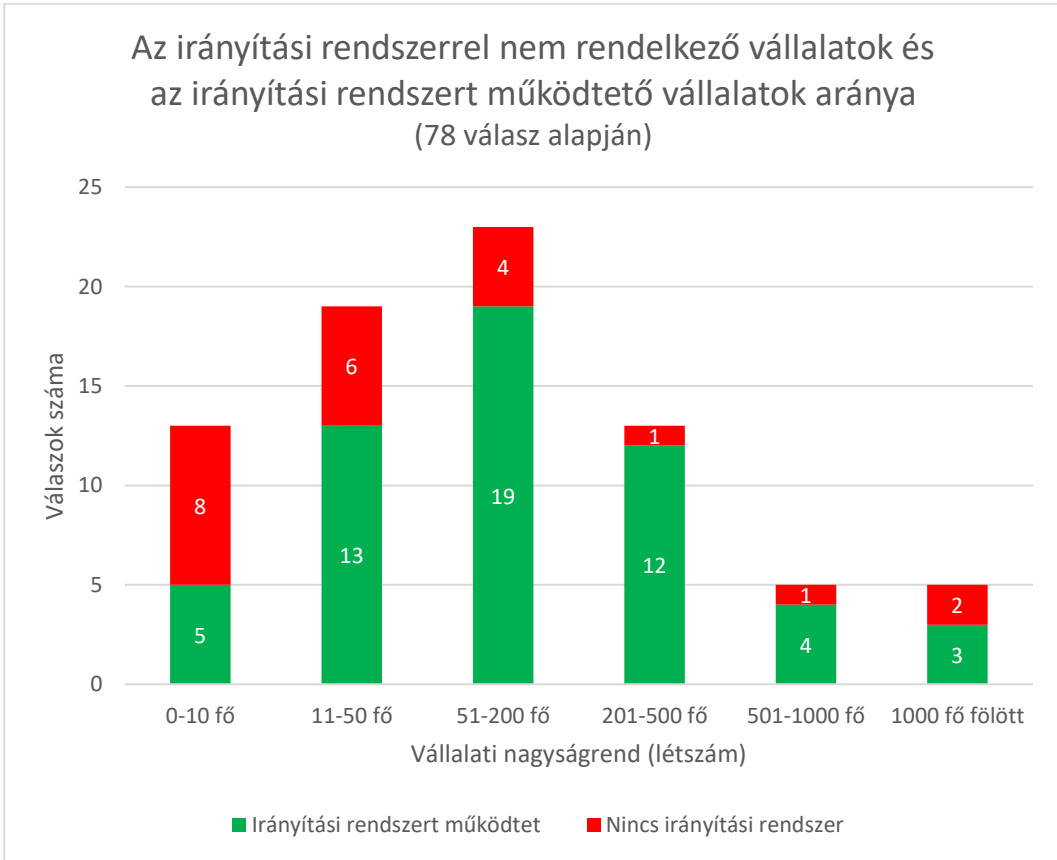
Válaszok	db
Belső utasítás készült	45
Önálló eljárás készült	19
Meglévő eljárást egészítettünk ki	15
A pandémiás tervet élesítettük	15
Máig nincs a járvány elleni védekezésre vonatkozó belső szabályozásunk	10
Az anyavállalat kiegészítette a már meglévő pandémiás tervét	1
Pandémiás terv átdolgozása a megváltozott körülményekhez	1
Kockázatértékelés	1
A kialakított szabályozás folyamatos aktualizálása, a hatályos jogszabályokhoz	1

7. Táblázat: A védekezési eljárások beépítése a vállalat szabályzói közé, saját szerkesztés

A kutatás során megvizsgáltuk a munkahelyi egészségvédelem és biztonság irányítási rendszert (OHSAS, vagy MEBIR) működtető vállalatok arányát, illetve a járványügyi intézkedések irányítási rendszerbe való integrálását.

Válaszok	db	%
Igen, az integrált irányítási rendszerünk része	16	20,5
Igen, és más független irányítási rendszerünk is van	2	2.6
Nincs MEBIR, bár van irányítási rendszerünk, pl. ISO 9000	34	43.6
Nincs irányítási rendszerünk	22	28.2
Cégünk fő tevékenysége az ilyen irányú szolgáltatás	1	1.3
Mi tanúsítunk kb. 500 MEBIR rendszert, Magyarországot én képviseltem az ISO-ban a 45001 szabvány kidolgozásában. Használjuk a 45005 szabványt is	1	1.3
IFS élelmiszerbiztonsági rendszer	1	1.3
Nincs OHSAS és MEBIR sem, IFS élelmiszer-biztonsági rendszerünk van	1	1.3

8. Táblázat: A MEBIR-t működtetésének aránya, saját szerkesztés



4. Ábra: Az irányítási rendszert működtető vállalatok aránya vállalati nagyságrend szerint, saját szerkesztés

Válaszok	db	%
Igen, eljárásainkat beépítettük a MEBIR-be	9	11.8
Eljárásainkat beépítettük az Integrált irányítási rendszerünkbe	26	34.2
Nem	41	53.9

9. Táblázat: Az eljárások MEBIR-be, vagyintegrált irányítási rendszerbe történő beépítése, saját szerkesztés

Tekintettel arra, hogy az ISO/PAS 45001:2020 a MEBIR-hez hasonló, ahhoz illeszthető, COVID-19 specifikus dokumentáció, így célszerű megvizsgálni, hogy a vállalatok ismerték-e és alkalmazták-e a PAS javaslatait?

Válaszok	db	%
Ismerjük, de nem alkalmazzuk	14	18.4
Ismerjük és alkalmazzuk	8	10.5
Nem ismertük még	54	71.1

10. Táblázat: Az ISO/PAS 45001:2020-t használata a vizsgált vállalatoknál, saját szerkesztés

Vizsgálatunk kiterjedt a COVID-19 pozitív fertőzések azonosítására, okainak vizsgálatára, illetve a betegségen átesett munkavállalók munkából való távolmaradásának időtartamára, valamint a kontaktkutatásokra.

Azonosítottak COVID-19 fertőzött munkavállalót?	db	%
Igen	70	89.7
Nem	8	10.3

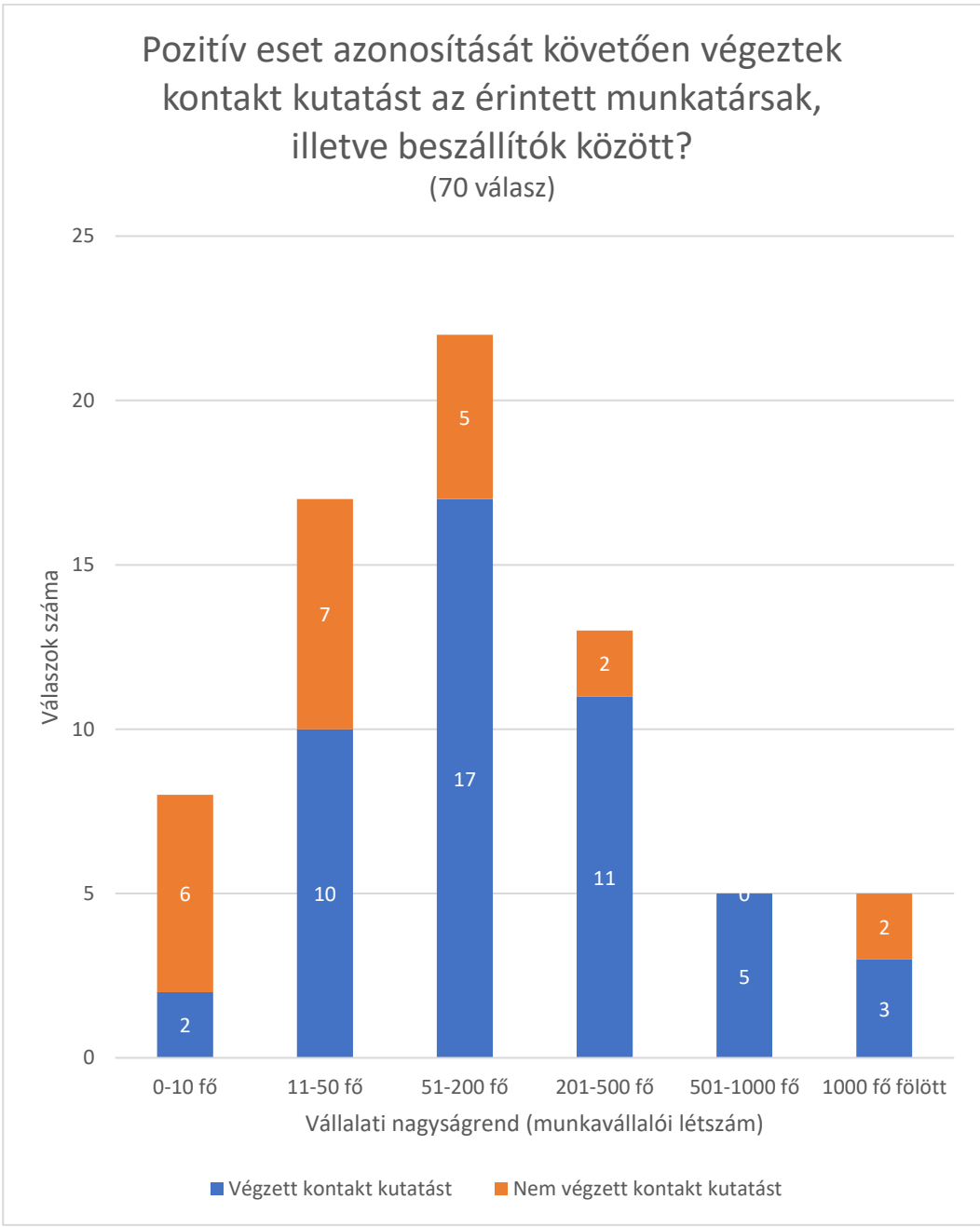
11. Táblázat: Koronavírus fertőzéses esetek előfordulása a vizsgált cégeknél, saját szerkesztés

Megállapították a betegségek lehetséges okait?	db	%
Igen, minden fertőzés esetén kivizsgáljuk a lehetséges okokat, hogy intézkedéseinket megfelelően módosíthassuk	40	57.1
Nem vizsgáltuk az okokat	30	42.9

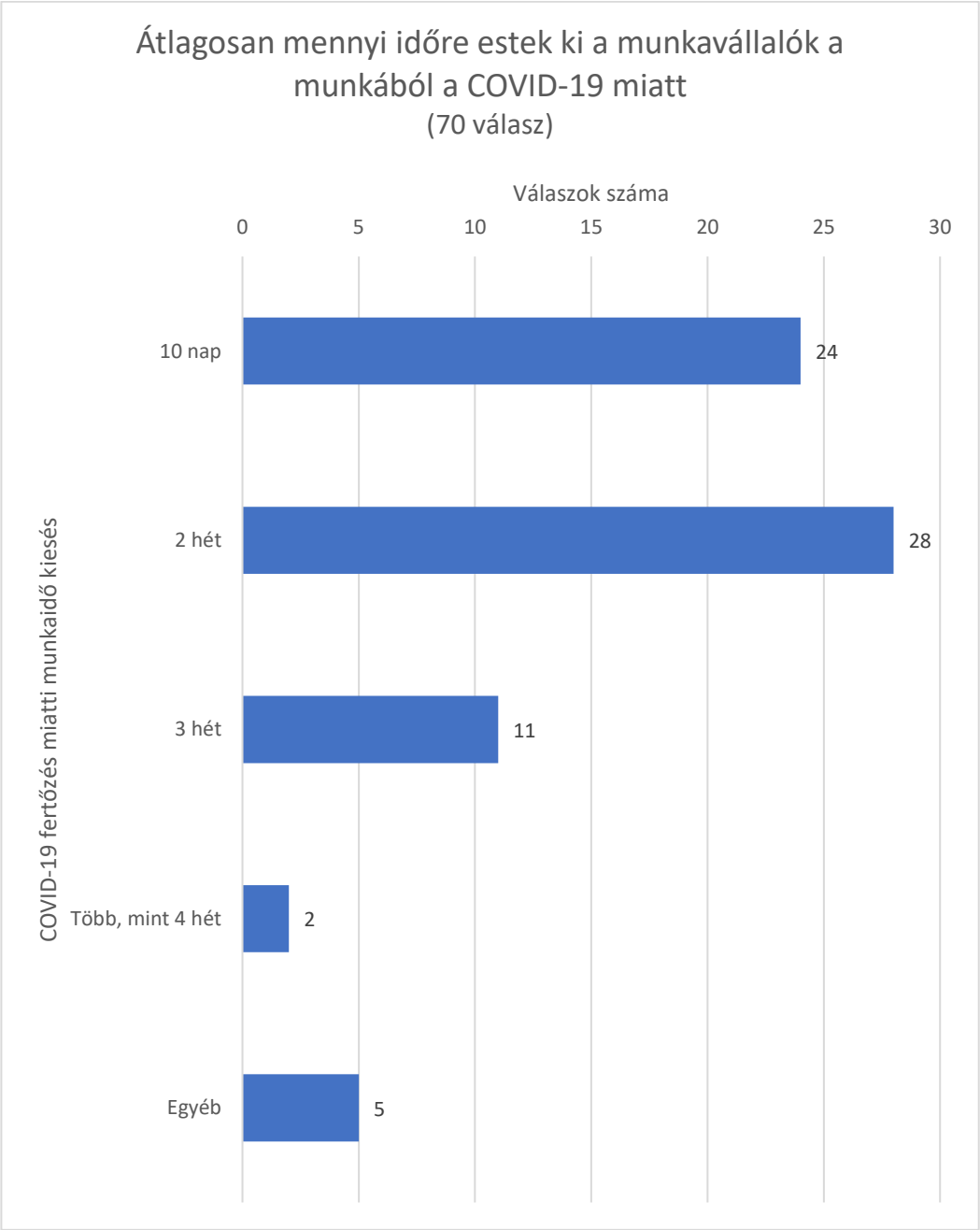
12. Táblázat: A betegségek lehetséges okainak vizsgálata, saját szerkesztés

Kontakt kutatás történt?	db	%
Igen, elvégeztük a kontakt kutatást	48	68.6
Nem	22	31.4

13. Táblázat: Kontakt kutatást végző cégek aránya, saját szerkesztés



5. Ábra: Kontakt kutatást végző vállalatok aránya vállalati nagyságrend szerint, saját szerkesztés



6. Ábra: A koronavírus fertőzés miatti munkaidő kiesés mértéke, saját szerkesztés

Záró kérdésként a kutatásban részt vevők egyéni válaszát kértük a koronavírus-járvány vállalatirányítással kapcsolatos legfontosabb benyomását illetően. 34 egyedi válasz érkezett. A válaszokat egyenként elemeztük és feldolgoztuk.

KÖVETKEZTETÉSEK, JAVASLATOK

A kutatás eredményei alapján megállapítottuk, hogy a munkáltatók jelentős erőfeszítéseket tettek munkavállalóik egészségének megóvása és a járvány terjedésének megakadályozása érdekében. Ehhez a vállalatok korábbi, járvány előtti működéséhez képest jelentős mértékű, alapvető változtatások bevezetésére volt szükség. A felmérésben e kérdés tekintetében a Likert-skálán érkezett válaszok között nagy mértékű eltérés nem mutatkozott (1. ábra). A kisebb létszámú vállalatok (0-10 fő és 11-50 fő) értékelése alacsonyabb volt, mint az átlagos (kb. 4-es) érték, a nagyobb létszámú cégek esetében átlag körüli, vagy az átlagérték feletti eredmények a jellemzőek. Kódonként összegeztük az érkezett válaszokat és meghatároztuk az egyes kódokra érkezett válaszok számát (2. ábra). A skála 1-es pontjához tartozó értékelés nem érkezett, tehát nem volt olyan válaszadó, aki nem tartott volna szükségesnek valamilyen intézkedést. A 4-es és 5-ös pont került kiválasztva a legnagyobb számban, vagyis a válaszadók többsége nagymértékű, vagy alapvető változásokat tartott szükségesnek a járvány tovább terjedésének megakadályozása érdekében.

A vállalatok felismerték tehát felelősségüket a pandémia tovább terjedésének megakadályozása és a munkavállalóik egészségének megóvása kapcsán és megelőző intézkedéseket vezettek be a fertőzés tovább terjedésének megakadályozása érdekében (3. táblázat). Alapvetően a csepp- és aeroszol terjedés megakadályozása (maszk használat, arcvédő használat), az elkülönítés (home office, online kapcsolattartás, védőfal, távolságtartás bevezetése), a helyiségek rendszeres fertőtlenítése, illetve a higiéniai intézkedések bevezetése volt a legjellemzőbb. Ezek az intézkedések egyrészről a munkafolyamatok és eljárások átszervezésével jártak (szakok átszervezése, elkülönítése, folyamatok átszervezése stb.), másrészről pedig a munkavállalók egyéni védelmére is kiterjedt (egyéni védőeszközök biztosítása otthoni használatra, fertőtlenítő eszközök biztosítása stb.). Tevékenységi formától és a működés sajátosságaitól függően alakult a munkaszervezés kidolgozása, a kollektív és egyéni védelem kialakítása. Néhány esetben egyedi megoldást is alkalmaztak a kutatásban részt vevő vállalatok (pl. COVID-19 politika és folyamatos nyomon követés, professzionális mentális támogatás biztosítása a munkavállalóknak), de alapvetően az alábbi főbb intézkedéscsoportok voltak a jellemzőek:

1. Elkülönítés
   a. Időben (műszakok időbeni elhatárolása)
   b. Térben (home office, online ügyfélkapcsolatok, személyes távolságtartás a vállalaton belül)
2. Higiéniai intézkedések (fertőtlenítés, kézfertőtlenítő állomások stb.)
3. Információ gyűjtés (lázmérés, COVID-19 teszt, munkavállalók kapcsolati rendszerében történt fertőzéses esetek jelentése)
4. Gyanús esetek elkülönítése (felsőlégúti betegség tünetei, vagy láz esetén kötelező otthon tartózkodás)
5. Egyéni védőeszközök biztosítása (maszk, arcplexi, gumikesztyű stb.)

A kutatás során a H1 hipotézist tehát igazoltuk, a H2 hipotézist pedig részben igazoltuk. A vállalatok felismerték szerepüket és felelősségüket a COVID-19 járvány elleni védekezésben és ennek megfelelően intézkedéseket dolgoztak ki és léptettek életbe a betegség tovább terjedésének megakadályozására. Az intézkedések eredményességét nem tudtuk megállapítani, mert a kutatás nem terjedt ki annak vizsgálatára, hogy a megbetegedett dolgozók a munkahelyen kapták-e el a fertőzést, vagy munkahelyen kívül.

A védekezési eljárások kidolgozásához elsősorban a kormányzati utasításokat és szabályokat vették figyelembe a vállalatok, mert a járvány kezdeti szakaszában főként a kormányzati kommunikáció, a Magyar Kormány által létrehozott Operatív Törzs tájékoztatói voltak a széles körben elérhető információforrások (4. táblázat). A vállalatok emellett kikérték a szakmai szervezetek (Népegészségügyi Szakigazgatási Szerv stb.) javaslatait is. Ugyanilyen arányban voltak azok a válaszadók, akik a saját tapasztalataikra támaszkodtak az eljárások kialakításánál. Multinacionális vállalatok esetében jellemző volt, hogy a cégközpont utasításait követve kellett az eljárásokat kialakítani, amely könnyebbséget jelent a leányvállalatnak, hiszen a vállalat más országban működő telephelyén már kidolgozott, bevezetett eljárásokat kellett a hazai gyakorlatba átültetni.

A járvány elleni intézkedések kialakítása és bevezetése során a munkáltatók legnagyobb arányban a közvetlen érintettjeikkel, vagyis a munkavállalóikkal, partnereikkel és ügyfeleikkel egyeztettek (5. táblázat). Ezen túl a helyi hatóságokkal, illetve a szakmai szervezetekkel egyeztetve próbáltak az intézkedéseket megalapozó információhoz jutni. A vizsgált vállalatoknál elenyésző alkalommal kerültek bevonásra a foglalkozás-egészségügyi szakorvosok, illetve szakszolgálatok.

A koronavírus-járvány hatásaival kapcsolatos kockázatértékelést a vállalatok fele (52,6%-a) végzett (6. táblázat és 3. ábra). A járvány kezdeti időszakára jellemző információhiány nagymértékben megnehezítette a megfelelő védekezési eljárások kialakítását, ez részben lehetett akadálya a kockázatértékelések elvégzésének is. A kutatás a kockázatértékelés elmaradásának okát nem tárta fel, így a H3 feltételezésünket nem igazoltuk.

A koronavírus-járvány elleni védekezés érdekében hozott intézkedéseket a vállalatok többsége (58%) belső utasítás formájában építette be a szabályozási rendszerébe, volt, ahol meglévő eljárást egészítettek ki (19%) és volt, ahol önálló eljárásként került be a vállalat szabályzói rendszerébe (24%) (7. táblázat). A belső utasítás a vállalatok szabályozásának egy formája, tulajdonképpen valamely szabályozni kívánt folyamatra vonatkozó önálló rendszabály, amely a vállalat többi szabályától függetlenül kerül bevezetésre. Az eljárás az irányítási rendszerbe integrált belső szabályozási forma. Önálló eljárásként egy bizonyos probléma egyedi szabályozására szolgál, meglévő eljárásba illesztve egy probléma csoport szabályozását teszi lehetővé. Volt olyan vállalat, ahol a pandémiás terv frissítése és végrehajtása révén történt a szabályozás (19%). A válaszadók egy részénél (10%) egyáltalán nem készült a járvány elleni védekezésre vonatkozó belső szabályzat.

A felmérésben részt vevő vállalatok mintegy harmada (22 db, 28,2%) nem rendelkezett irányítási rendszerrel (8. táblázat). A többi vállalat (56 db, 72%) működtet valamilyen irányítási rendszert. Közülük 19 rendelkezik MEBIR-rel, a többi vállalkozás MEBIR-t nem üzemeltet, de más típusú irányítási rendszert (minőségirányítási rendszert, élelmiszerbiztonsági rendszert) igen. Az irányítási rendszer szemlélete tehát a vállalkozások nagy részénél adott. Az irányítási rendszert nem működtető cégek aránya a vállalati nagyságrend növekedésével csökken (4. ábra). Ez alól kivétel a felmérésben részt vevő ezer fő feletti vállalati kategória, ahol a mintában szereplő 5 nagyvállalat közül kettő azt a választ adta, hogy nem működtet irányítási rendszert. A védekezési eljárásokat az irányítási rendszerrel rendelkező cégek többsége beintegrálta az irányítási rendszerébe (9. táblázat). Így a COVID-19 miatt létrehozott folyamatok a vállalati irányítási rendszer részévé váltak és nem önálló szabályzatként léteznek. A H4 hipotézist a kutatás során igazoltuk. Az irányítási rendszerrel

rendelkező vállalatok könnyebben építették be folyamataikba a védekezés érdekében hozott intézkedéseiket.

Az „ISO/PAS 45005:2020 Általános irányelvek a biztonságos munkavégzéshez a COVID-19 járvány idején" című dokumentumot a vállalatok döntő többsége (71%) nem ismerte (10. táblázat). A PAS-t ismerő vállalatok közül is csak alacsony számban vannak azok a cégek, amelyek alkalmazták annak ajánlott intézkedéseit. Ez a felmérésben részt vevő cégek mindössze 10%-át jelenti, ami igen alacsony aránynak tekinthető. Hasonló esetekben célszerű lenne az átfogó intézkedési javaslatokat tartalmazó ajánlások szélesebb körben történő népszerűsítése, megismertetése az érintett felekkel.

A megbetegedéses esetek kezelése sajátos feladatot és jelentős nehézséget jelentett a vállalatok számára. Korábban ehhez hasonló problémával nem kellett még megküzdenie a munkáltatóknak, a COVID-19 járvány ebben a tekintetben is komoly kihívások elé állította a vezetőket. A vállalatok döntő többségénél, mintegy 90%-nál azonosítottak COVID-19 pozitív munkavállalót (11. táblázat). A védekezésre kialakított eljárások ellenére magas arányú volt a megbetegedések száma. Pusztán a megbetegedések számának alapján azonban nem lehet egyértelműen a vállalatok védekezési gyakorlatának eredményességét megítélni, tekintettel arra, hogy a munkavállalók munkaidőn túli biztonságáról a munkáltató nem tud minden határon túl gondoskodni. A biztonságra való törekvés a munkavállaló saját attitűdje szerinti mértében történik, a munkáltatónak erre gyakorolt hatása elenyésző. Így nem lehetséges egyértelműen megállapítani azt, hogy a fertőzések a vállalaton belül, vagy kívül történtek? A felmérés rámutatott arra, hogy a munkáltatók többsége (kb. 60%-a) igyekezett a megbetegedések lehetséges okait kivizsgálni és erőfeszítéseket tenni annak érdekében, hogy a saját folyamataik gyenge pontjait azonosíthassák és intézkedéseiket megfelelőképpen módosítsák (12. táblázat).

Az országos tisztifőorvos által a koronavírus-járvány miatt kiadott eljárásrend előírta, hogy kötelező felderíteni minden olyan személyt, aki valószínűsíthetően vagy igazoltan kapcsolatba került a koronavírussal fertőzött személlyel. A járványügyi kivizsgálás jogszabályban meghatározott módon, a szakma szabályai szerint történik, végrehajtásában járványügyi szakemberek vesznek részt [12]. A vállalatok közel 70%-a szintén követte ezt az eljárást és pozitív eset azonosítását követően végzett valamilyen módon kontakt kutatást (13. táblázat). Nagyobb létszámú vállalatok esetén volt jellemzőbb a kontakt kutatás, vélhetően a munkavállalók magasabb létszáma, illetve a távoli munka lehetőségének korlátozottsága miatt (5. ábra). A munkavállalók a fertőzés miatti munkából való távolmaradása leggyakrabban 10 nap és 2 hét közti időtartamra esett. Kisebb arányban előfordult 3 heti, illetve 4 héten túli munkaidő kiesés is (6. ábra).

A munkáltatók a koronavírus-járvány miatt az irányítási rendszert, illetve a vállalat egészét érintő változások közül elsősorban a vállalatvezetési és -szervezési feladatok átalakulását emelték ki. A korábbiakban megszokott munkarend, illetve munkabeosztások átszervezése, a vállalati folyamatok átstrukturálása jelentette az egyik legnagyobb változást. Új kihívást jelentett a pandémia terjedése és az egyre bővülő ismeretek miatti folyamatos változásokhoz való gyors alkalmazkodás kényszere is. A rugalmasság, a külső változásokhoz való rendkívül gyors adaptálódás szerepe jelentős mértékben megnőtt a pandémia alatt. Hangsúlyosabbá vált a munkavállalók magasabb szintű védelmének biztosítása a munkáltató részéről. A bevezetett higiéniai intézkedések előnyeinek felismerése miatt azok hosszú

távú fenntartásának szándéka is kialakult. Egyes esetekben a munkafolyamatokat hatékonyabbá tette az, hogy a vállalatoknak alkalmazkodni kellett a változásokhoz. A távoli, otthoni, online munka, a home office előnyeinek megismerése és kihasználása hasonlóan eredményesnek bizonyult, így több vállalat részéről felmerült annak hosszabb távon történő alkalmazása is.

Problémaként említették a munkáltatók, hogy az elkülönítés, a távmunka és az online kapcsolattartás, bár tagadhatatlanul eredményes a betegség tovább terjedésének csökkentése szempontjából, de ugyanakkor a személyes munkakapcsolatok átalakulását is jelentette. Ez sok esetben nehézséget, növekvő pszichoszociális terhet jelentett a munkavállalók számára. A vírussal kapcsolatos információk kezdeti bizonytalansága, hiányossága alapvetően befolyásolta, illetve késleltette a védekezési intézkedések kidolgozását és bevezetését.

ÖSSZEFOGLALÁS

A koronavírus-járvány jelentős kihívás elé állította a vállalatokat és a munkavédelmi szakembereket is. Kezdetben kevés érdemi információra támaszkodva, az egyre gyarapodó ismeretekhez folyamatosan alkalmazkodva dolgozták ki és vezették be eljárásaikat a munkavállalók egészségének megőrzése érdekében. A járvány terjedésének sebessége és a betegség súlyossága sokkszerűen érte a közösségeket, így a vállalatokat is, ezért a pandémia terjedését megakadályozó védekezési eljárások kidolgozása sürgető kényszerként lépett fel. A hagyományos munkavédelmi módszertanok alkalmazására ilyen feltételek mellett nem minden esetben volt lehetőség. A kezdeti bizonytalanság után a vállalatok belátták a pandémia terjedése elleni eljárások jelentőségét, illetve saját szerepüket a vírus elleni harcban, így a munkahelyi biztonság és egészségvédelem rövid idő alatt jelentősen felértékelődött.

A koronavírus-járvány okozta probléma még nem szűnt meg. A szárazabb, melegebb nyári időszakban mérséklődött a fenyegetés. A vakcinák megjelenését követően, a beoltottak számának növekedésével tovább csökkent a fertőzés üteme, de 2021-ben sajnos korántsem beszélhetünk még a járvány végéről. Az őszi és téli időszakban ismét megnövekszik a felsőlégúti megbetegedések száma, és vele a COVID-19 terjedésének kockázata is. Emiatt a munkáltatóknál továbbra is hangsúlyos feladatként jelentkezik a munkavállalók egészségének megőrzése érdekében folytatott küzdelem. Javasolt tehát a munkavédelmi módszerek eredményességének vizsgálata és a védekezést hatékonyan segítő eljárások kidolgozása. Kvalitatív eljárásokkal célszerű a COVID-19 kockázatértékelések eredményességét megvizsgálni és meghatározni azokat a kockázatelemzési módszereket, amelyek ezen a területen eredményesnek bizonyultak. Javasolt a szisztematikus módszertani eljárásokat összefoglaló kiadványok, mint például az Általános irányelvek a biztonságos munkavégzéshez a COVID-19 járvány idején című PAS szélesebb körben történő megismertetése, hatékonyabb kommunikációja a vállalatok felé. A járvány további hullámai előtt fontos lenne a vállalati beavatkozások sikerességét megvizsgálni és az eredményes eljárásokat, módszereket megosztani a vállalatvezetőkkel, munkavédelmi szakemberekkel elősegítve ezzel a szélesebb körű hatékony védekezést. A pandémiával kapcsolatban rendelkezésre álló információk, illetve a védekezés során szerzett tapasztalatok folyamatos bővülése lehetőséget biztosít a munkavédelmi szakemberek számára a szisztematikus, átgondolt, rendszerszintű védekezési eljárások kidolgozására.

IRODALOMJEGYZÉK

[1] A. Kópházi, "A COVID-19 szervezetekre gyakorolt hatásának HR apsektusai és szervezetfejlesztési lehetőségei," in *„Gazdaságvédelem és pénzügyi kiutak" pénzügyi, adózási és számviteli szakmai és tudományos konferencia*, pp. 98–103.

[2] J. Köllő and B. Reizer, "A koronavírus-járvány első hullámának hatása a foglalkoztatásra és a vállalatok árbevételére," *Közgazdasági Szle.*, vol. LXCIII., pp. 345–374, 2021.

[3] P. J. Tóth Arnold, Szabó Szilvia, Kálmán Botond, "A foglalkoztatottság alakulása a magyar gazdaság szektoraiban a Covid-19 járvány következtében," *Új munkaügyi Szle.*, vol. 2, no. 1, pp. 2–23, 2021.

[4] J. Poór, K. Dajnoki, G. Pató, S. Beáta, and S. Szabó, Eds., "Koronavírus-válság kihívások és HR válaszok: Első és második fázis összehasonlítása," Magyar Agrár és Élettudományi Egyetem 2100 Gödöllő Páter Károly u. 1., 2021.

[5] T. B. Pirohov, "COVID-19 vírus második hullámában tapasztalható foglálkoztatási kihívások a vállalatok szemszögéből," *Int. J. Eng. Manag. Sci.*, vol. 6, no. 2, 2021, doi: 10.21791/IJEMS.2021.2.13.A.

[6] Henk de Vries, "Samen tegen corona - Dynamiek tussen regels en innovaties (long-read)," 2020. https://www.nnk.nl/show/pub/47/samen-tegen-corona-dynamiek-tussen-regels-en-innovaties.

[7] E. Goldman, "Exaggerated risk of transmission of COVID-19 by fomites," *Lancet Infect. Dis.*, vol. 20, no. 8, pp. 892–893, 2020, doi: 10.1016/S1473-3099(20)30561-2.

[8] Szabó Gyula, "A munkavédelemi kockázatkezelés sajátosságai," *Bánki Közlemények*, vol. 3, no. 1, pp. 5–12, 2020.

[9] K. Lazányi, "A biztonsági kultúra," *Taylor*, vol. 7., no. 1–2, pp. 398–405, 2015, [Online]. Available: https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12936.

[10] B. Bognár *et al.*, *Vállalati Fehér Könyv - Gyakorlati útmutató a vállalati pandémiás terv elkészítéséhez és végrehajtásához*. Budapest: Innovációs és Technológiai Minisztérium Járványmatematikai modellező és epidemiológiai projektje, 2020.

[11] ISO, "ISO/PAS 45005:2020 Occupational health and safety management — General guidelines for safe working during the COVID-19 pandemic." https://www.iso.org/standard/64286.html (accessed Oct. 01, 2021)

[12] "Így zajlik a kontaktvizsgálat." https://koronavirus.gov.hu/cikkek/nnk-igy-zajlik-kontaktvizsgalat (accessed Oct. 01, 2021).

REVIEW ABOUT THE BOOK JOSÉ E. ALVAREZ: THE SPANISH FOREIGN LEGION IN THE CIVIL WAR 1936

RECENZIÓ JOSÉ E. ALVAREZ: THE SPANISH FOREIGN LEGION IN THE CIVIL WAR 1936 KÖNYVÉRŐL

BESENYŐ János[1]

Az elmúlt időszakban egyre több a XIX-XX. század hadtörténeleméhez kapcsolódó esemény kutatását, feldolgozását végezték el hadtörténészek, amelyek közé szervesen illeszkedik José E. Alverez[2] könyve is, amely a Légiónak a Spanyol Polgárháború első hat hónapjában történt tevékenységét veszi górcső alá. A kevésbé kutatott Spanyol Légió egyik különlegesen jó ismerője a szerző, aki évek óta kutatja és publikálja a szervezet tevékenységével kapcsolatos könyveit, cikkeit. Már csak azért is fontos a szerző tevékenysége mivel a Légióról és annak tevékenységéről leginkább spanyol nyelvű anyagokhoz lehet hozzáférni, angol nyelvűhöz azonban csak igen korlátozottan. Ezt magam is tapasztaltam, amikor a Légió nyugat-szaharai tevékenységét, valamint a Légióban szolgáló magyarok után kutattam.[3]

1936 júliusában a spanyol hadsereg egyik legjobban kiképzett, felkészített egysége volt az akkor hat zászlóaljból álló, alig 4000 fős Légió, amelynek a támogatása elengedhetetlen volt a köztársasági kormány ellen felkelést indító tábornokoknak. Ezért annak megnyeréséért mindent megtettek és jelentős részben nekik volt köszönhető, hogy a felkelést sikerre tudták vinni és az nem fojtotta el a kormányzat már a kezdetén a csírájában. De Franco is főként nekik köszönhette, hogy több más jelölt és önjelölt közül, végül ő szerezhette meg az ország feletti uralmat. A Légiót 1934-ig csak az afrikai gyarmatokon - főként Marokkóban - vetették be, ahol igen komoly harci tapasztalatokat szerzett, így mikor a spanyol hadsereg más egységei nem voltak képesek kezelni az Asturiai felkelést, őket hívta segítségül a kormányzat. A felkelést igen hatékonyan, minimális veszteségekkel tudták felszámolni, bár a baloldali, és később az őket kivezénylő erők is bírálták a felkelőkkel és a civil lakossággal szembeni fellépésüket.[4] A szerző által leírtakból úgy tűnik, hogy a Légió egyáltalán nem akart aktívan részt venni a politikában, egyszerűen katonák akartak lenni és tenni azt, ami a feladatuk volt, megvédelmezni az afrikai területeket. Ezt sikeresen meg is tették. Ők voltak az akkori spanyol hadsereg elitje, akik a legkeményebb

[1] besenyo.janos@uni-obuda.hu | ORCID: 0000-0001-7198-9328 | habilitated associate professor, Óbuda University, Doctoral School for Safety and Security Sciences, Africa Research Center | habilitált egyetemi docens, Óbudai Egyetem Biztonságtudományi Doktori Iskola, Afrika Kutatóközpont

[2] Professzor Dr. José E. Alvarez történész 1996-ban kezdte az oktatási tevékenységet a Houston Downton Egyetemen. Hadtörténész diplomát szerzett a West Point-i Katonai Akadémián és több hadtörténeti társaság tagja. Alvarez professzor által tanított tárgyak: Világtörténelem, XX. századi Európai Történelem, Közel-Kelet történelme, valamint az USA történelme. Szinte egyedüliként kutatja a Spanyol Idegenlégió történelmét, amelyből több cikket, könyvet publikált. Elérhetősége: alvarezj@uhd.edu

[3] Besenyő János: Hungarians in the Spanish Legion? Węgrzy w Legionie Hiszpańskim? Studia Politicae Universitatis Silesiensis 2019, 26, 25—44, DOI: http://doi.org/10.31261/SPUS.2019.26.02 https://www.journals.us.edu.pl/index.php/SPUS/article/view/8288

[4] Erről bővebben: James Matthews: Reluctant Warriors: Republican Popular Army and Nationalist Army Conscripts in the Spanish Civil War, 1936-1939, OUP Oxford, 2012; Francisco J. Romero Salvadó: Historical Dictionary of the Spanish Civil War, Rowman & Littlefield, 2013; Paul Preston: The Spanish Civil War: Reaction, Revolution and Revenge, W.W. Norton & Company, 2007; Antony Beevor: The Spanish Civil War, Cassell, 2001; Antony Beevor: The Battle for Spain: The Spanish Civil War, 1936-1939, Penguin Books, 2006; Stanley G Payne: The Spanish Civil War, Cambridge University Press, 2012;

kiképzést kapták, hihetetlenül fegyelmezettek és bajtársiasok voltak, illetve jelentős harci tapasztalattal rendelkeztek. Egyfajta „elitista szubkultúrát" hoztak létre, ahol az akkori spanyol hadsereggel ellentétben nem a mindennapi túlélés és a ranglétrán való araszolgatás, hanem a kiadott parancsok azonnali és hatékony teljesítése, sőt a katonához méltó halál elérése volt. Ezzel ellentétben a spanyol katonai és rendőri erőket mélyen átszőtte a politika, a nepotizmus, korrupció, sőt a vezetőik politikai és ideológiai megosztottsága miatt ezek a szervezetek a működőképtelenség határán táncoltak. Nagy részt ezért sem voltak képesek az 1936 nyarán kirobbant puccsal szemben hatékonyan fellépni. Ezzel szemben a Légió vezetése igyekezett távoltartani a szervezetet a politikától, annak ellenére, hogy a vezetők egy része a jobboldali erőkkel szimpatizált. Végül olyan helyzetbe kerültek, hogy úgy érezték, hogy nincs más választásuk, mint támogatni a puccsistákat és részt venni az ország törvényes kormányának megdöntésében. Ez ugyan elfogadhatatlan egy demokratikus berendezkedésű államban, de az akkori időszakban Spanyolországban többször került vértelen, vagy minimális áldozattal járó katonai puccsra, így a legtöbben úgy gondolták, hogy ebben az esetben sem lesz másképp. Erre azonban rácáfolt az élet, ugyanis a köztársasági vezetők nem voltak hajlandóak „csendben visszavonulni," és támogatták őket a nagyvárosokban élő munkások és kereskedők is, így egy három éven keresztül tartó brutális polgárháború kezdődött, amelynek az egyik főszereplője volt a Légió, valamint a marokkói és szaharávi törzsek tagjaiból toborzott Regulares alakulatok.[5] A szerző szerint egyébként a puccsisták célja nem a Köztársaság felszámolása, hanem bizonyos módon a „megreformálása" volt. Ezt bizonyítja, hogy a felkelést kirobbantó katonai vezetők egyike, Emilio Mola Vidal tábornok a kormányzatot ugyan megkívánta dönteni, de a köztársasági formát meg akarta őrizni, sőt annak a nevében tervezte működtetni a katonai kormányzatot.[6] De nem csak ő, hanem a puccsisták többsége is így gondolta. Badajoz elfoglalása után a Légió parancsnoka, Yagüe alezredes a győzelmi beszédét így fejezte be: „Kiáltsátok velem: Hosszú életet Spanyolországnak! Hosszú életet a Köztársaságnak! Hosszú életet a hadseregnek!"[7]

A szerző külön kiemelte, hogy a magas szintű szervezettség és a professzionalitás mellett a Légióban a brutalitás és az erőszak a mindennapok része volt, hiszen ezek nélkül nem is győzhettek volna a marokkói hadszíntéren, ahol rajtuk kívül szinte minden spanyol egység kudarcot vallott. Ezeket a tulajdonságokat a „fehér terror" keretében hatékonyan használták fel a nacionalistákkal szembenálló erőkkel, valamint az őket támogató polgári lakossággal szemben. Nem csak ezeknek voltak köszönhető a pacifikáció keretében végrehajtott atrocitásoknak, hanem azoknak a történelmi tapasztalatoknak is, amit Franco fiatal tisztként még a marokkói harcok idején szerzett, amikor a stratégiai fontosságú Annual elfoglalását nem megfelelően készítették elő, aminek következtében a spanyolok egyik legnagyobb afrikai veszteségüket szenvedték el. Éppen ezért Franco, az őt támogató németek sürgetése ellenére sem sietett Madrid elfoglalására, hanem szisztematikusan szállta meg az útjába kerülő területeket és számolt fel minden lehetséges ellenállást és csak akkor indult tovább amikor úgy érezte, hogy nem marad mögötte olyan erő, amely hátba támadhatná. Ezért a katonái minden fegyvert begyűjtöttek, letartoztatták és/vagy kivégezték

[5] Besenyő János: Western Sahara, Publikon Publisher, Pécs, 2009, p. 59.
[6] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. p. 10.
[7] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. p. 74

azokat, akik fegyveresen harcoltak a nacionalisták ellen, esetleg veszélyeztethették azok céljait. Ez volt a strategy of limpiar (cleanse) and castigar (punish).[8] Azt azért látni kell, hogy a köztársaságiak oldalán harcolók sem voltak Grál lovagok, amelyre bizonyítékok azok a kegyetlenségek és atrocitások, amelyeket ők is elkövettek a velük nem szimpatizáló polgári lakosok vagy a fogságukba került, korábban velük szemben harcolók ellen.[9] Persze a Légió sikereihez – az előzőleg említettek mellett - főleg a kezdeti időszakban elengedhetetlen volt a kormányzat tehetetlensége, a spanyol hadsereg szégyenletes állapota, az ország megosztottsága és a puccsisták szerencséje, valamint a külföldről, a náci Németországtól és a fasiszta Olaszországtól kapott sokrétű – katonai, logisztikai, szállítási, stb. - támogatás is. A német és olasz szállítóeszközök nélkül ugyanis az afrikai bázisokon állomásozó alakulatok, nem lettek volna képesek átjutni a köztársasági erők által ellenőrzött Gibraltári szoroson át a kontinensre, így a felkelést a köztársaságiak – ha képesek lettek volna rá – könnyen felszámolhatták volna. Azonban a külföldi támogatással a lázadó tábornokok átléptek egy határt, ahonnan nem volt visszatérés és „egy bukásra ítélt puccsból egy három évig tartó véres polgárháború lett", amelyben német és olasz katonák is részt vettek Franco oldalán.[10] Míg a kormányzat a Szovjetunióhoz fordult, amely a saját politikai érdekében és Spanyolország aranykészletéért cserében fegyvereket és tanácsadókat küldött a köztársaságiak támogatására.[11] Így a polgárháború gyorsan nemzetközivé vált, ahol a baloldali és jobboldali eszmék fegyveres ütköztetése folyt.

A könyvben végig követhetjük a polgárháború első hónapjaiban a Légió tevékenységét Seville, Almendralejo, Merida, Badajoz, Santa Amalia, Talavera de la Reina, Santa Olalla, Maqueda, Toledó, Illescas, Oviedo és sok más településen, amelyeket nem csak elfoglalniuk kellett, hanem meg is védelmezni a kemény ellentámadásoktól. Az összecsapások folyamán voltak hősies és kevésbé hősies események, de az egyértelmű, hogy a légionáriusok keményen kivették a részüket a harcokból, amely jól látható volt a veszteséglistájukból is.[12] A könyv értékét növeli, hogy a szerző nem csak „távolságtartó" történészként, levéltári forrásokból dolgozott, hanem az események aktív résztvevőivel készített interjúkat is felhasznált, sőt személyesen is felkereste az események helyszíneit. Külön tetszett, hogy a könyvben több légionáriust vagy a Légióhoz köthető személyt is bemutatott az „emberi" oldaláról, nem titkolván el azok pozitív, de negatív tulajdonságait sem. Közéjük tartozott a 8. zászlóalj állományában szolgáló magyar származású Inocencio Kadar Szass (eredeti neve: Nagy Károly), hadnagy, aki néhány légionáriussal sikeresen állította meg egy négy szovjet tankból és 400 gyalogosból álló egység támadását, amiért külön kitüntetést kapott.[13] Szintén érdekes, hogy olyan információkat lehet megtudni a

[8] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. pp. 52-53.
[9] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. pp. 66, 76, 215, 237, 266.
[10] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. pp. 22, 143-144.
[11] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. p. 217
[12] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. pp. 85, 205, 208
[13] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. pp. 177, 269. and Besenyő János: Hungarians in the Spanish Legion? Węgrzy w Legionie Hiszpańskim? Studia Politicae Universitatis Silesiensis 2019, 26, 25—44, DOI: http://doi.org/10.31261/SPUS.2019.26.02
https://www.journals.us.edu.pl/index.php/SPUS/article/view/8288

polgárháborúban résztvevőkről és az általuk használt fegyverekről, eszközökről, amelyekről nem hogy egy átlagos olvasó, de sok történész sem rendelkezik.

A könyv elolvasása után az olvasó leszámol azzal a közkeletű vélekedéssel, hogy a Légió idegen egységként, kvázi zsoldosokként harcolt volna a spanyol hazafiak ellen, sőt egyértelműen látható, hogy a légió állományának 80%-a nem külföldi, hanem spanyol volt és az ő felfogásuk szerint a hazájukért harcoltak. Furcsa, hogy korábban a köztársasági erők oldalán harcoló nemzetközi brigádokban szolgáló külföldieket szabadságharcosnak tekintették, annak ellenére, hogy a Sztálin által vezetett Szovjetunió birodalmi céljait szolgálták és nem a törvényes spanyol kormányét. Sőt azok közül többen hasonló, vagy brutálisabb cselekedeteket követtek el a velük szembenállók (katonák, civilek, egyházi személyek, stb.) ellen, mint a légionáriusok. Ennek ellenére, a megítélésük mégis pozitívabb volt az elmúlt évtizedekben.

A szerző ugyancsak cáfolja, hogy a 10 napon keresztül tartó badajozi mészárlást a légionáriusok követték volna el, mint ahogy azt korábban több forrás is állította. Ugyanis az elfogott köztársaságiak kivégzését a Falangisták és a Polgárőrség tagjai hajtották végre, nem pedig a légionáriusok, akik addigra már elhagyták a várost.[14] Ezzel a könyvvel sokkal árnyaltabban lehet szemlélni az akkori eseményeket, amelyek Spanyolországban még érzékeny kérdésnek számítanak, ezért nem is kutatható nagyon sok levéltári anyag a Polgárháborúval kapcsolatosan. Remélhetőleg ez változni fog és egyre több levéltári anyagot szabadítanak fel a kutatók számára és készülnek Alvarezéhez hasonló könyvek. Remélem, hogy a szerző nem áll meg az 1936-os évnél, hanem a Légió teljes polgárháborús tevékenységét fel fogja dolgozni, amit már most várok.

A könyv elolvasását mindazoknak javaslom, akik kíváncsiak az 1936-os év viszonyaira, a Spanyol Polgárháború kirobbanásának körülményeire, valamint a szembenálló felek – közülük is kiemelkedően a Légió – tevékenységére.

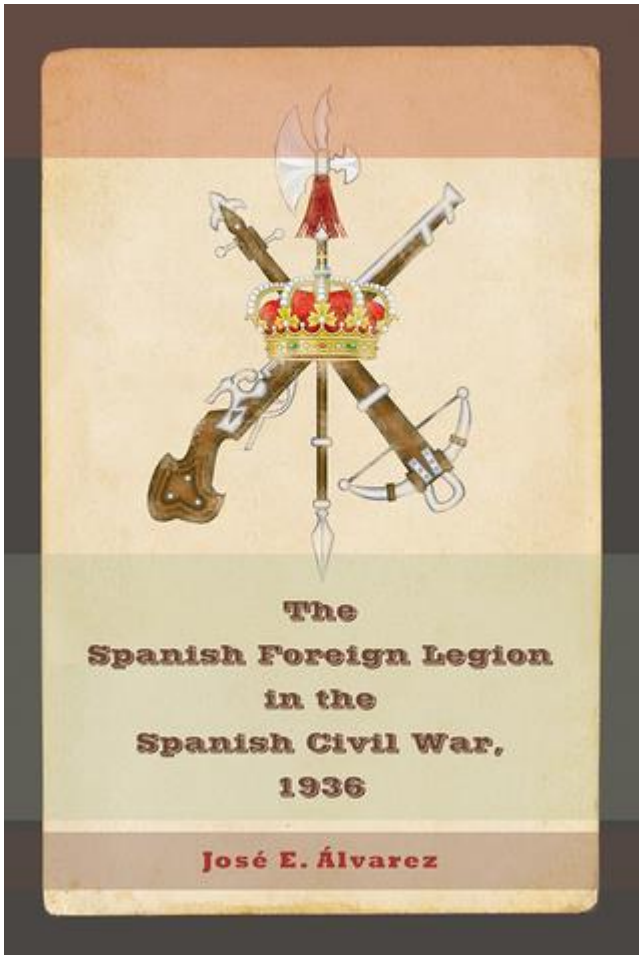
José E. Alverez: The Spanish Foreign legion in the Civil War 1936, University of Missouri Press, 2018, 313 oldal

FELHASZNÁLT IRODALOM

Antony Beevor: The Battle for Spain: The Spanish Civil War, 1936-1939, Penguin Books, 2006.
Antony Beevor: The Spanish Civil War, Cassell, 2001.
Besenyő János: Hungarians in the Spanish Legion? Węgrzy w Legionie Hiszpańskim? Studia Politicae Universitatis Silesiensis 2019, 26, 25—44, DOI: http://doi.org/10.31261/SPUS.2019.26.02
https://www.journals.us.edu.pl/index.php/SPUS/article/view/8288
Besenyő János: Western Sahara, Publikon Publisher, Pécs, 2009.
Francisco J. Romero Salvadó: Historical Dictionary of the Spanish Civil War, Rowman & Littlefield, 2013.
James Matthews: Reluctant Warriors: Republican Popular Army and Nationalist Army Conscripts in the Spanish Civil War, 1936-1939, OUP Oxford, 2012.

[14] José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018. p. 75, 244.

José E. Alvarez: The Spanish Foreign Legion in the Spanish Civil War, 1936, University of Missouri Press, 2018.
Paul Preston: The Spanish Civil War: Reaction, Revolution and Revenge, W.W. Norton & Company, 2007.
Stanley G Payne: The Spanish Civil War, Cambridge University Press, 2012.



1. ábra: A könyv borítója
(forrás: https://www.goodreads.com/book/show/27409653-the-spanish-foreign-legion-in-the-spanish-civil-war-1936)

Follow, like, post, publish! | Kövess, lájkolj, posztolj, publikálj!

https://biztonsagtudomanyi.szemle.uni-obuda.hu

https://www.linkedin.com/company/safety-and-security-sciences-review

https://www.facebook.com/biztonsagtudomanyi.szemle