ISSN 2676-9042

Vol 8, No 2, 2026.

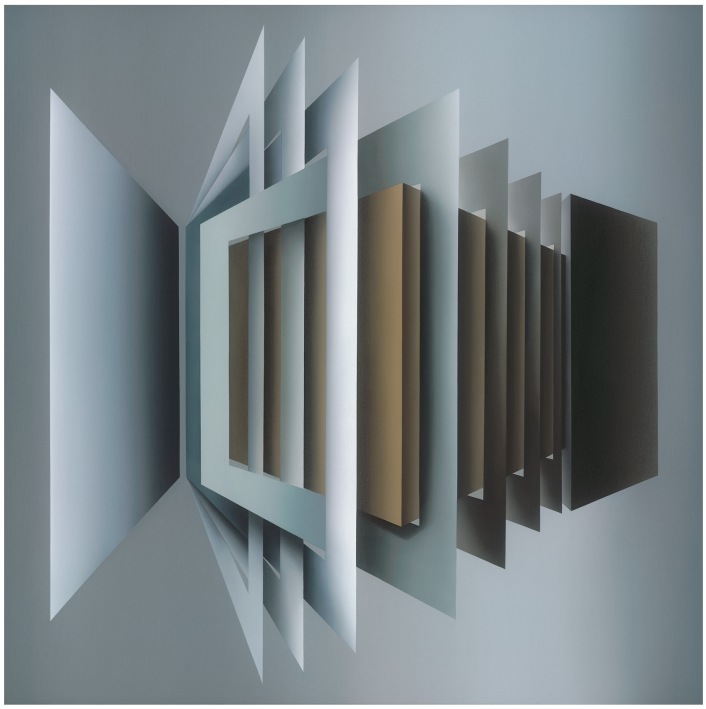
2026, VIII. évf. 2. szám

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
BORS Györgyi
painter/festőművész
Cube peeling II. painting | **Kockahámozás II.** című festménye látható

The Military Science Committee of the 9th Department of Economics and Law of the Hungarian Academy of Sciences classified our journal as a "C" category.	Folyóiratunkat a Magyar Tudományos Akadémia IX. Gazdaság- és Jogtudományok Osztályának Hadtudományi Bizottsága „C" kategóriás folyóiratnak minősítette.
The Safety and Security Sciences Review is a classified journal by Hungarian Science Bibliography.	A Biztonságtudományi Szemle a Magyar Tudományos Művek Tára (MTMT) által minősített folyóirat.
Our journal is indexed by the following databases	**Folyóiratunkat a következő adatbázisok indexelik**

EBSCO

epa.oszk.hu

Electronic Periodicals Archive & Database | Elektronikus Periodika Adatbázis
https://epa.oszk.hu/04100/04186

MATARKA

Hungarian Periodicals Table of Contents Database | Magyar folyóiratok tartalomjegyzékeinek kereshető adatbázisa
https://matarka.hu/szam_list.php?fsz=2267&nyelv=hun

ÓDA Óbudai Egyetem Digitális Archívum

Digital Archives of Óbuda University | Óbudai Egyetem Digitális Archívum

dk Országos Széchényi Könyvtár - Digitális Könyvtár

National Széchenyi Library Digital Library | OSZK Digitális Könyvtár
https://oszkdk.oszk.hu/DRJ/39186

ULRICHSWEB™ GLOBAL SERIALS DIRECTORY

Global Serials Directory | Globális Sorozatok Könyvtára
http://ulrichsweb.serialssolutions.com/title/1678275514425/863974

doi Foundation

Digital Object Identifier | Digitális ObjektumAzonosító
https://www.doi.org

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	Élelmiszer-biztonság
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
Fire Safety and Disaster Management	Tűzbiztonság és katasztrófavédelem

The **aim** of the journal is to publish studies, research reports, book reviews for professionals working in the field of security science or related scinces, or for those interested in the subject of the broadly disciplinary framework of military technical sciences, and for security awareness and developing a safety culture. We know that the cultivation of security sciences includes the study of the history of military and law enforcement security, as well as the knowledge of the historical aspects of our field of science, and its development. We are working towards to present the latest theoretical models and empirical research findings in our journal. We believe that our Journal and our authors can contribute to the creation of a world that enables a (more) secure life for all the inhabitants of the Earth by knowing the historical past and examining the events of the present with precision and accuracy.

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.

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, vagy a téma iránt érdeklődők számára a katonai műszaki tudományok, s így a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése. Tudjuk, hogy a biztonságtudományok művelésébe beletartozik a had-, rendészet- és biztonságtörténet vizsgálata, tudományterületünk történeti és történelmi vetületeinek, s így fejlődésének megismerése. Azon dolgozunk, hogy Folyóiratunkban bemutassuk jelenkorunk legújabb teoretikus modelljeit és empirikus kutatási eredményeit. Hiszünk benne, hogy Folyóiratunk és szerzőink a történelmi múlt ismeretével, a jelenkor eseményeinek precíz és akkurátus vizsgálatával hozzá tudunk járulni egy olyan világ megteremtéséhez, amelyik lehetővé teszi a Föld minden lakója számára a biztonságos(abb) életet.

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.

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

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 8, No 2, 2026. | **2026. VIII. évf. 2. szám**

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

BEREK László

berek.laszlo@uni-obuda.hu

László BEREK graduated as an information specialist–librarian from Eötvös Loránd University, after which he obtained qualifications as a system informatics specialist and library expert. He defended his doctoral dissertation at the Doctoral School of Safety and Security Sciences of Óbuda University in 2024. Over the past twenty years, he has gained extensive professional experience in scientific and academic libraries, and since 2015 he has served as Director of the University Library of Obuda University. His research interests include the security of online scholarly communication, research ethics, plagiarism detection and the identification of AI-generated texts, as well as university rankings and related scientometric issues. He is the author of four university textbooks used in the doctoral programmes of two doctoral schools at Óbuda University, and he teaches the course "Research Publication Skills" at the Doctoral School of Innovation Management. In recent years, he has developed several e-learning materials. He is a member of five committees at Obuda University, including the Scientific Council, the Ranking Committee, the Greenmetric Committee, the IT Committee, and the Artificial Intelligence Transition Committee. He also serves as a board member of the Technical Librarians' Section of the Association of Hungarian Librarians.

BEREK László az Eötvös Loránd Tudományegyetemen végzett informatikus könyvtárosként, ezt követően rendszerinformatikusi és könyvtári szakértői képesítést szerzett. Doktori értekezését az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában védte meg 2024-ben. Az elmúlt húsz évben tudományos és egyetemi könyvtárakban szerzett szakmai tapasztalatot, 2015 óta az Óbudai Egyetem Egyetemi Könyvtárának igazgatója. Kutatási területei közé tartozik az online tudományos kommunikáció biztonsága, a tudományetika, a plágiumellenőrzés és a mesterséges intelligencia által generált szövegek detektálása, továbbá az egyetemi rangsorok és a kapcsolódó tudománymetriai kérdések. Négy egyetemi tankönyv szerzője, amelyeket az Óbudai Egyetem két doktori iskolájának programjaiban használnak, emellett az Innovációmenedzsment Doktori Iskola „Kutatási publikációs ismeretek" című kurzusának oktatója. Az elmúlt években több e-learning tananyagot is kidolgozott. Az Óbudai Egyetem öt bizottságának tagja, köztük a Tudományos Tanácsé, a Ranking Bizottságé, a Greenmetric Bizottságé, az Informatikai Bizottságé és a Mesterséges Intelligencia Átállási Bizottságé. Emellett a Magyar Könyvtárosok Egyesülete Műszaki Könyvtáros Szekciójának elnökségi tagja.

BOKROS Anna Dóra

bokrosdora@gmail.com

She graduated from ÓE BGK with a BSc in Military and Safety Engineering specializing in information security, followed by an MSc in Safety Engineering. During her work at multinational companies, she gained practical experience in physical and human security, asset protection project implementation, and multicultural work environments. She currently works in the banking sector in information security, focusing primarily on ICT risk analysis and compliance with NIS2, DORA, and critical infrastructure regulations. Her academic interests examine the intersection of rapidly evolving technology and human factors, including social engineering techniques, behavioral biometrics, and the impact of algorithms on decision-

Az ÓE BGK karán végzett biztonságtechnikai mérnök, információbiztonság szakirányon, majd vagyonvédelmi rendszer tervező mesterképzésen. Multinacionális vállalatoknál végzett munkája során gyakorlati tapasztalatot szerzett fizikai- és humánbiztonság, valamint vagyonvédelmi projektek megvalósítása terén, emellett számos különböző nemzetiség munkakultúrájával megismerkedett. Jelenleg a bankszektorban dolgozik információbiztonsági területen, fő fókusza az IKT kockázatelemzés mellett a NIS2, DORA és kritikus infrastruktúra megfelelés. Jelenlegi tudományos érdeklődése középpontjában a rohamosan fejlődő technológia és az emberi tényezők találkozásánál felmerülő kérdések állnak, mint a social engineering technikák fejlődése, a felhasználói viselkedésminták biometrikus azonosításként

making. Beyond their technological dimensions, she also explores these topics from political-strategic and philosophical perspectives.

való alkalmazása, valamint az algoritmusok döntéshozatalra gyakorolt hatása. Ezen kérdések a technológiai aspektusai mellett kiemelten foglalkoztatják politikai stratégiai, filozófiai megközelítésből is.

BOROSS Zsigmond Attila

attila.zsigmond.boross@vih.gov.hu

I was born in 1971 in Szeghalom, Békés County, where I completed both my primary and secondary education. After fulfilling my compulsory military service, I studied History and Geography at the Teacher Training Faculty of Eötvös Loránd University. I spent one year teaching at a primary school before beginning my career in the field of national security, where I worked on countering extremism. Later, also at Eötvös Loránd University, I graduated as a political scientist. This allowed me to combine the academic study of extremist political theory with the practical analysis of its real-world manifestations. After more than fifteen years, I continued my professional career at the National Police Headquarters, where I was responsible for establishing and leading the professional framework for combating hate crimes. As a national law enforcement partner in international projects, I had the opportunity to publish on the experiences gained in this field, and to introduce students of the Counter-Terrorism Department at the University of Public Service to the issues of radicalisation, extremism, and fanaticisation. Subsequently, as a member of the National Protective Service, I was able to monitor and analyse undesirable processes occurring within the closed world of the prison system. I conducted months-long interviews with several high-profile inmates, providing valuable material for later analytical work.

1971-ben születtem Békés megyében, Szeghalmon, ahol az általános és középiskolát is végeztem. A sorkatonai szolgálat letöltését követően az Eötvös Loránd Tudományegyetem Tanárképző Főiskolai karára jártam történelem - földrajz szakra. Egy évig tanítottam általános iskolában, majd nemzetbiztonsági területen helyezkedtem el, ahol extrémizmus-elhárítással foglalkoztam. Szintén az ELTE-n, politológusként végezve tudtam hasznosítani a szélsőséges politikaelmélet tanulmányozásának és a gyakorlati megvalósulás vizsgálatának egyidejű megélését. Másfél évtizedet követően az Országos Rendőr-főkapitányságon folytattam a pályafutásomat, a gyűlölet-bűncselekményekkel szembeni szakvonal kiépítésével és vezetésével. Nemzetközi projektek hazai rendvédelmi együttműködőjeként a szakvonalon szerzett tapasztalatokról publikálhattam, illetve a radikalizáció, extrémizmus, fanatizálódás kérdéskörét az NKE Terrorelhárítási tanszékének hallgatóival igyekeztem megismertetni. Ezután a Nemzeti Védelmi Szolgálat munkatársaként a büntetés-végrehajtás zárt világában zajló nemkívánatos folyamatokat kontrollálhattam. Több kiemelt fogvatartottal hónapon átívelő interjút készíthettem, későbbi elemzések számára.

BRAUN András

braun.andras92@stud.uni-obuda.hu

András BRAUN graduated from the Faculty of Military and Security Engineering of the National University of Public Service in 2016 with a specialization in radar engineering. In 2022, he graduated from Óbuda University with an MSc in Security Engineering. He participated in the operation of military radars in service in Hungary for nearly 7 years. He is currently a doctoral student at the Doctoral School on Safety and Security Sciences; his field of research is the safety assessment of the operation of radar systems.

BRAUN András 2016-ban a Nemzeti Közszolgálati Egyetem Had- és Biztonságtechnikai mérnöki Karán végzett radar mérnök specializáción. 2022-ben az Óbudai Egyetem Biztonságtechnikai mérnöki MSc szakon szerzett diplomát. Közel 7 éven keresztül vett részt a Magyarországon hadrendben álló katonai radarok üzemeltetésében, működtetésében. Jelenleg a Biztonságtudományi Doktori Iskola doktorandusz hallgatója, kutatási területe, tanulmányain belül, a radarok alkalmazásának biztonságtechnikai vizsgálata.

ELEK Barbara

elek.barbara@bgk.uni-obuda.hu

Barbara ELEK is a habilitated associate professor, geophysical environmental engineer and fire protection engineer. She is a faculty member of the Institute of Safety Science and Cybersecurity at the Donát Bánki Faculty of Mechanical and Safety Engineering of Óbuda University, and serves as head of the EHS postgraduate engineering and specialist training programmes. She is a lecturer and supervisor at the Doctoral School of Safety and Security Sciences of Óbuda University. Her research interests include fire and explosion protection, safety issues of critical energy systems and facilities, and environmental safety.

ELEK Barbara habilitált egyetemi docens, okl. környezet-geofizikus mérnök, tűzvédelmi szakmérnök. Jelenleg az Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar Biztonságtudományi és Kibervédelmi Intézetének oktatója, valamint az EHS szakmérnök és szakember képzés képzésvezetője. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának oktatója és témavezetője. Kutatási területei a tűz- és robbanásvédelem, az energetikai létfontosságú rendszerek és létesítmények biztonsági kérdései, valamint a környezetbiztonság.

GÁBOR Edina

gabor.edina@phd.uni-obuda.hu

Edina GABOR is a health promotion psychologist and a PhD student at the Doctoral School of Safety and Security Sciences of Óbuda University. She was formerly the Director General of the National Institute for Health Development, and is currently a board member of the Association for Healthier Workplaces. Her scientific interest focuses on workplace health promotion, the organizational-level management of psychosocial risks, and leadership commitment. In her recent research, she also examines the impacts of artificial intelligence on work processes, occupational safety, and workplace psychosocial risks. She provides educational and consulting services at several universities, primarily in the areas of workplace health promotion, stress management, occupational safety, and psychosocial risks. Her scientific publications have appeared in the related fields of health promotion, psychology, mental health care, and safety and security sciences. Her Hirsch index is 5.

GÁBOR Edina egészségfejlesztő szakpszichológus, az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorandusza. Korábban az Országos Egészségfejlesztési Intézet főigazgatója volt, jelenleg az Egészségesebb Munkahelyekért Egyesület elnökségi tagja. Tudományos érdeklődése a munkahelyi egészségfejlesztésre, a pszichoszociális kockázatok szervezeti szintű kezelésére és a vezetői elköteleződésre irányul. Újabb kutatásaiban a mesterséges intelligencia munkavégzésre, munkavédelemre és munkahelyi pszichoszociális kockázatokra gyakorolt hatásait is vizsgálja. Oktatási és konzultációs tevékenységet több egyetemen és szakmai képzésben végez, elsősorban a munkahelyi egészségfejlesztés, a stresszkezelés, a munkavédelem és a pszichoszociális kockázatok témakörében. Tudományos publikációi az egészségfejlesztés, a pszichológia, a mentális egészségügyi ellátás és a biztonságtudomány kapcsolódó területein jelentek meg. Hirsch-indexe: 5.

KELEMEN László

kelemenl@cyberexpert.hu

As a computer engineer, certified engineering instructor, and forensic IT expert, I prepare expert opinions for government agencies and private clients, primarily in the fields of IT, cybersecurity, digital forensics, and blockchain technology. I have several years of experience as an ethical hacker, penetration tester, and vulnerability researcher, including vulnerability testing of OT/industrial control systems.I am actively involved in researching and developing Web3, smart contract,

Mérnök informatikusként, okleveles mérnöktanárként és igazságügyi informatikai szakértőként hatósági kirendelésekre és magánmegbízásokra készítek szakértői véleményeket, elsősorban informatikai, kiberbiztonsági, digitális forenzikus és blokklánc-technológiai területeken. Többéves gyakorlattal rendelkezem etikus hackerként, penetration testerként és vulnerability researcherként, beleértve az OT/ipari vezérlő rendszerek sérülékenység vizsgálatot is. Aktívan foglalkozom Web3-, smart contract-, DeFi-, NFT- és blockchain se-

DeFi, NFT, and blockchain security solutions. As a developer, I build applications, scripts, and data analysis systems using Python, PHP, Java, JavaScript, and Solidity. My specific research areas include blockchain-based tracking, wallet tagging, and the application of machine learning and artificial intelligence for forensic and cybersecurity purposes. My previous professional experience includes cyber intelligence gathering, telecommunications and data analysis, as well as custom development projects. I have achieved finalist and top 10 finishes in CTF and international blockchain competitions.

curity megoldások vizsgálatával és fejlesztésével. Fejlesztőként Python, PHP, Java, JavaScript és Solidity nyelveken készítek alkalmazásokat, scripteket és adatelemző rendszereket. Speciális kutatási területeim közé tartozik a blockchain-alapú nyomkövetés, a wallet-címkézés, valamint a gépi tanulás és a mesterséges intelligencia forenzikus s kiberbiztonsági célú alkalmazása. Korábbi szakmai tapasztalataim kiberinformáció-gyűjtési, táv- és hírközlési adatelemzési, valamint egyedi fejlesztési feladatokra is kiterjednek. CTF- és nemzetközi blockchain versenyeken döntős, illetve TOP 10-es eredményeket értem el.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Csaba KOLLÁR is a communications engineer, certified communications specialist, electronic information security manager, doctor of economics (PhD), and doctor (PhD) and habilitated doctor (Dr. habil.) in military engineering. He is also a cybernetics consultant, coach, and mediator. His research interests include the social aspects and economic impacts of the digital age, with a particular focus on the human aspects of information security, information security awareness, human-robot interaction, smart cities, artificial intelligence, social credit systems, and domotics. He is a senior research fellow at Óbuda University, where he leads the specialized courses for Domotics Engineer/Consultant and Facility and Property Professional Engineer/Manager. He is also the head of the Artificial Intelligence Workshop and serves as the scientific secretary of the Editorial Board of the Safety and Security Sciences Review, which is classified by the Military Science Committee of the 9th Department of Economics and Law of the Hungarian Academy of Sciences. Csaba Kollár is an expert with the Hungarian Society of Military Science and the National Association of Human Professionals, and has been a member of the Artificial Intelligence Consortium since Q4 2018.

KOLLÁR Csaba kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), a katonai műszaki tudományok doktora (PhD) és habilitált doktora (Dr. habil.), kibernetikus, tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa, az információbiztonság-tudatosság fejlesztése, az ember-robot interakció, az okosváros, a mesterséges intelligencia, a társadalmi kredit rendszere, az intelligens épületek (domotika rendszerek) üzemeltetése és gazdálkodása. Az Óbudai Egyetem tudományos főmunkatársa, a domotika szakmérnök/szaktanácsadó és a létesítménygazdálkodó és -üzemeltető szakmérnök/szakmenedzser továbbképzési szakok képzésvezetője, a Mesterséges Intelligencia Műhely vezetője, az MTA IX. Osztály Hadtudományi Bizottsága által minősített Biztonságtudományi Szemle szerkesztőbizottságának tudományos titkára, az Egyetem Biztonságtudományi Doktori Iskolájának és a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának az oktatója, témavezetője. A Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

LEISZTNER Péter

leisztner.peter@uni-obuda.hu

Peter LEISZTNER is a certified environmental engineer, occupational safety engineer, and industrial installation engineer, and a Ph.D. student at the Doctoral School of Safety and Security Sciences at Óbuda University. With over ten years of experience in occupational safety, he is dedicated to developing businesses built around safety. His research focuses

LEISZTNER Péter okleveles környezetmérnök, munkavédelmi mérnök és gyárszerelő üzemmérnök, valamint PhD hallgató az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában. Több mint tíz éves munkavédelmi tapasztalattal, elkötelezett a biztonság köré épülő vállalkozások fejlesztése iránt. Kutatásai a munkavédelmi képviseletre, a munkavédelmi

on occupational safety representation, measuring the performance of workers' representatives in the field of occupational safety, defining their tasks and roles within companies' occupational safety organizations, and assessing and determining the level of their occupational safety knowledge.

képviselők munkavédelmi teljesítményének mérésére, feladataik és szerepük meghatározására a vállalatok munkavédelmi szervezetein belül, valamint munkavédelmi ismereteik szintjének felmérésére és meghatározására összpontosítanak.

LŐCSEI Anikó

locsei.aniko@bparchiv.hu

Aniko LOCSEI received an MA degree in History (EKF-BTK) and archival appointment, followed by participation in several professional archival conferences (2012, 2014, 2016, 2019). Early research focused on the processing and analysis of judicial records and statistical data related to prosecuted individuals from different historical periods. In 2017, she was appointed chief archivist and later senior counsellor. Professional activities include the development of registration systems, databases and archival finding aids, as well as supporting scientific research groups. The primary field of research focuses on digital data protection and cybersecurity, with particular attention to the protection and authenticity of digital documents. In addition, research interests extend to the historical development of disaster management systems and the examination of modern situational assessment and protection systems, especially digital decision-support and information management solutions. Research also includes the application possibilities of blockchain technology, which may contribute to strengthening data integrity and ensuring the authenticity of digital documents.

LŐCSEI Anikó történettudományi MA diploma (EKF-BTK) és levéltárosi kinevezés megszerzését követően több szakmai konferencián vett részt levéltári területen (2012, 2014, 2016, 2019). Kutatásai kezdetben különböző korszakok jogszolgáltatási iratainak, valamint perbe vont személyek statisztikai adatainak feldolgozására és elemzésére irányultak. 2017-ben főlevéltárosi, később tanácsosi kinevezésben részesült. Munkája során nyilvántartási rendszerek, adatbázisok és segédletek készítésével, valamint tudományos kutatócsoportok támogatásával foglalkozik. Fő kutatási területe a digitális adatvédelem és adatbiztonság, különös tekintettel a digitális dokumentumok védelmére és hitelességének biztosítására. Emellett érdeklődése kiterjed a katasztrófavédelmi rendszerek történeti fejlődésére, valamint a modern helyzetértékelési és védelmi rendszerek vizsgálatára, különös figyelemmel a digitális döntéstámogatási és információkezelési megoldásokra. Kutatásaiban a blokklánc-technológia alkalmazási lehetőségeivel is foglalkozik, amely hozzájárulhat az adatintegritás növeléséhez és a digitális dokumentumok hitelességének biztosításához.

MAREK Bence Attila

redder.mb@gmail.com

Bence Attila MAREK graduated in 2019 from the Donát Bánki Faculty of Mechanical and Safety Engineering at Óbuda University, specializing in Military and Safety Engineering. In 2022, he obtained his Master's degree in Safety Engineering at Óbuda University, with a specialization in Security Organization. Following this, he completed the Occupational Safety Engineering postgraduate program at the same institution. He first worked in the field of property protection before transitioning to occupational safety. He is currently employed as an Occupational Safety Engineer at Opella Healthcare Hungary Ltd. Within the framework of his doctoral studies, he plans to research the application of Artificial Intelligence (AI) in the field of occupational safety.

MAREK Bence Attila 2019-ben az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai mérnöki Karán végzett had- és biztonságtechnikai mérnök specializáción. 2022-ben az Óbudai Egyetem Biztonságtechnikai mérnöki MSc szakon okleveles biztonságtechnikai mérnök diplomát szerzett vagyonvédelmi szervező szakirányon. Ezt követően ugyanebben az intézményben végezte el a munkavédelmi szakmérnöki képzést. Először a vagyonvédelem területén dolgozott, mely után a munkavédelem területére váltott. Jelenleg az Opella Healthcare Hungary Kft.-nél dolgozik munkavédelmi mérnökként. Doktori tanulmányain belül a mesterséges intelligencia (AI) felhasználását tervezi kutatni a munkavédelmen belül.

MÁRKOS Szilárd Attila

markos.szilard@bgk.uni-obuda.hu

I completed my higher education studies at the Bánki Donát Faculty of Mechanical and Safety Engineering at Óbuda University. I obtained my bachelor's degree (BSc) in 2011, specializing in mechanical engineering and machine design, and then in 2015 I completed my master's degree (MSc) in mechatronics engineering, specializing in intelligent equipment. During my professional career, I have worked on numerous industrial projects as a mechanical designer, regularly consulting with electrical engineers and automation specialists during their operation. As a result, I have gained an increasingly deeper insight into the design of complex, multidisciplinary systems. After that, my interest turned to modern building engineering, in the context of which I designed several systems related to the topic. Nowadays, hot and cold water networks and artificial ventilation require a number of auxiliary devices, and electrical networks are becoming increasingly complex. Control is essential for the coordinated operation of all these systems. Home automation offers a solution to these tasks, which is how I came into contact with this field of science.

Felsőfokú tanulmányaimat az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán végeztem. Alapszakos (BSc) diplomámat 2011-ben szereztem meg Gépészmérnök Gépszerkesztő tervező szakirányon, majd 2015-ben Mechatronikai mérnökként végeztem el a mesterképzést (MSc) az Intelligens berendezések szakirányon. Szakmai pályám során számos ipari projektben dolgoztam gépészeti tervezőként, amelyek működtetése közben rendszeresen egyeztettem villamosmérnök és automatizálási szakemberekkel. Ennek köszönhetően egyre mélyebb rálátásom alakult ki a komplex, több szakterületet átfogó rendszerek tervezésére. Ezek után az érdeklődésem a modern épületgépészet felé fordult, melynek keretében több a témához kapcsolódó rendszert is terveztem. Napjainkban már a hideg-meleg vízhálózatok és a mesterséges szellőztetés is számos segéd berendezést igényel, a villamos hálózatok pedig egyre összetettebbé válnak. Mindezek összehangolt működéséhez elengedhetetlen a vezérlés. Ezen feladatok megoldására kínál megoldást a domotika, így kerültem kapcsolatba ezzel a tudományággal.

MORVAY László

morvay.laszlo@phd.uni-obuda.hu

László MORVAY (1967) electrical operating engineer in the medical technology sector (KKVMF, 1989) and MSc in safety engineering (ÓE-BGK, 2023). He is currently the managing director of HOLL & MOOR Health Service and Consulting Ltd. He specializes in soft laser therapy, as well as compiling professional material for research and development projects supported from EU and domestic funds, and monitoring and documenting the professional progress of projects. Contract tender assessor of the National Research, Development and Innovation Office. Continuous learning is the key to professional development, so he is currently a doctoral student at Óbuda University's Doctoral School on Safety and Security Sciences. His field of research is the investigation of medical devices used in musculoskeletal disorders, which covers the safety issues of soft laser therapy (light), ultrasound therapy (mechanical) and electrotherapy (electric current).

MORVAY László (1967) villamos-üzemmérnök orvostechnikai ágazaton (KKVMF, 1989) és biztonságtechnikai mérnök-tervező MSc (ÓE-BGK, 2023). Jelenleg a HOLL & MOOR Egészségügyi Szolgáltató és Tanácsadó Kft ügyvezetője. Szakterülete a lágylézer terápia, valamint uniós és hazai forrásból támogatott kutatás-fejlesztési projektek szakmai anyagának összeállítása, a projektek szakmai előrehaladásának ellenőrzése, dokumentálása. A Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal szerződéses pályázati bírálója. A szakmai fejlődés kulcsa a folyamatos tanulás, ezért jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza. Kutatási területe a mozgásszervi megbetegedések során alkalmazott orvostechnikai eszközök vizsgálata, amely a lágylézer terápia (fény), az ultrahang terápia (mechanikai) és az elektroterápia (elektromos áram) biztonsági kérdéseire terjed ki.

NAGY Rudolf

nagy.rudolf@uni-obuda.hu

Dr. habil. Rudolf NAGY, retaired firefighter Colonel, is currently associate professor at Óbuda University. He studied in foreign educational institutions. He served as a CBRN defence officer, and took part in industrial safety tasks. He gained experience as an operations officer in the NATO SFOR mission. After that he became Deputy Head of the Emergency Management Department of Hungarian National Directorate General for Disaster Management. Summa cum laude earned a PhD degree in field of Critical Infrastructure Protection. Later he was appointed Deputy Head of the Disaster Management Training Centre. In civilian life, he worked as an EHS manager. He has been teaching subjects of safety and security sciences since 2015, and is responsible for the fire protection engineering specialization. He obtained a habilitated doctorate in the scientific study of self-ignition.

Dr. habil. NAGY Rudolf nyugalmazott tűzoltó ezredes, jelenleg az Óbudai Egyetem docense. Külföldi oktatási intézményekben tanult. Vegyivédelmi tisztként szolgált, és részt vett iparbiztonsági feladatokban. A NATO SFOR misszióban műveleti tisztként szerzett tapasztalatokat. Ezt követően az Országos Katasztrófavédelmi Főigazgatóság Veszélyhelyzetkezelési Főosztályának helyettes vezetője lett. Summa cum laude minősítéssel szerzett PhD fokozatot a kritikus infrastruktúrák védelme területén. Később a Katasztrófavédelmi Oktatási Központ vezetőjének helyettesévé nevezték ki. A polgári életben EHS vezetőként dolgozott. 2015 óta oktatja a biztonságtudományok tantárgyakat, a tűzvédelmi mérnöki specializáció felelőse. Habilitált doktori címet szerzett az öngyulladások tudományos vizsgálatából.

NÉGYESI Imre

negyesi.imre@uni-nke.hu

Dr. habil. Colonel Imre Négyesi, associate professor, PhD, National University of Public Service, Faculty of Military Science and Defence Officer Training, Military Infocommunication Institute and Head of the Department of Informatics. Civilian qualification: Radiochemical engineer. Scientific interest: Research into the military applications of artificial intelligence. Scientific board memberships: Doctoral School of Military Science, supervisor and lecturer of the Doctoral School of Military Science of the National University of Public Service, the Doctoral School of Military Engineering of the National University of Public Service and the Doctoral School of Security Sciences of Óbuda University. Summary of his scientific and teaching work: 104 scientific journal articles in domestic listed journals (262 independent citations), 7 in international listed journals (6 independent citations), 3 in other scientific journals in foreign languages (1 in Q1 journal, 99 independent citations). Number of published monographs: 6, 1 in foreign language. Independent Hirsch index: 11.

Dr. habil. NÉGYESI Imre ezredes, egyetemi docens, PhD, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Infokommunikációs Intézet és az Informatikai Tanszék vezetője. Polgári szakképesítése: Radiokémiai mérnök. Tudományos érdeklődés: A mesterséges intelligencia katonai alkalmazásainak kutatása. Tudományos testületi tagságai: Hadtudományi Doktori Iskola, a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskolájának, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának és az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának témavezetője és oktatója. Tudományos és oktatói munkásságának összefoglalása: Tudományos folyóiratcikk hazai listás folyóiratban 104 db (független hivatkozások száma 262 db), nemzetközi listás folyóiratban 7 db (független hivatkozások száma 6 db), egyéb tudományos folyóiratokban idegen nyelven 3 db (ebből Q1-s folyóiratban 1 db, független hivatkozások száma 99 db). Megjelent monográfiák száma 6 db, ebből idegen nyelvű 1 db. Független Hirsch indexe: 11.

OLÁH Róbert

olah.robert0721@gmail.com

My name is Róbert OLÁH. I graduated from Eötvös Loránd University as a certified software engineer and an engineering teacher at Óbuda University. I

OLÁH Róbert vagyok. Az Eötvös Loránd Tudományegyetem okleveles programtervező informatikusként, és az Óbudai Egyetemen mérnök tanárként végeztem.

have been actively participating in the work of the Artificial Intelligence Workshop at the Donát Bánki Faculty of Mechanical and Security Engineering of Óbuda University since February 2024. My current research is also based on this topic. My research area: AI-based image transformations and image recognition, Informatics network security science. I am a member of the John von Neumann Computer Science Society. Informatics has always played a major role in my professional career. I also participated in a TDK at Óbuda University on the topic of teaching algorithms and the impact of artificial intelligence in public education. I am interested in security science and will use this knowledge for my PHD research in the near future.

Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnika Mérnöki Karán működő Mesterséges intelligencia Műhely munkájában 2024 februárjától veszek aktívan részt. A jelenlegi kutatásom is ezen a témakörön alapul. Kutatási területem: AI alapú képtranszformációk és kép felismerés, Informatikai hálózati biztonságtudomány. A Neumann János Számítógép-Tudományi Társaság tagja vagyok. Az informatika mindig is fő szerepet játszik a szakmai pályafutásomban. Az Óbudai Egyetemen TDK-n is részt vettem az algoritmusok tanítása és mesterséges intelligencia hatása a köznevelésben témakörben. Érdeklődöm a biztonságtudomány iránt, és ezeket az ismereteket fogom felhasználni a közeljövőben a PHD kutatásomhoz.

SOMOGYI Tamás

somogyit588@gmail.com

Holds a Master's degree in IT engineering and a complementary degree in Legal Studies. He is currently a PhD student at the Doctoral School on Safety and Security Sciences, Óbuda University. His research area is the security issues of the financial sector's infrastructure, with a special focus on natural hazards. He has more than 15 years of experience in the banking industry.

Mérnök-informatikus, mérnök-szakjogász. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának hallgatója. Kutatási területe a bankszektor létesítményi infrastruktúrájának védelme és ellenállóképességének fokozása, elsősorban a természeti veszélyek jelentette fenyegetettséggel szemben, tágabban pedig a kritikus infrastruktúrák védelme. Több, mint 15 év banki munkatapasztalattal bír.

SZŰCS Endre

szucs.endre@bgk.uni-obuda.hu

Endre SZŰCS (1963) PhD degree in military science, certified security engineer, mechanical engineer, engineering teacher. Currently, he is a doctoral supervisor and advisor at Óbuda University's Doctoral School on Safety and Security Sciences, Instructor of the course "Review and analysis of the history and events of security technology", and he is also a lecturer at the Institute of Mechanical Engineering and Technology and Institute of Safety Science and Cybersecurity at Óbuda University, Bánki Donát Faculty of Mechanical and Security Engineering. His research interests are "The possibilities of the use of renewable energy sources in safety and security technology", "Investigation of the history of safety and security technology".

SZŰCS Endre (1963) a hadtudomány PhD fokozatosa, okleveles biztonságtechnikai mérnök, gépészmérnök, mérnök tanár. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában témavezető és témakiíró, „A biztonságtechnika történetének, eseményeinek áttekintése, elemzése" című tantárgyat oktató, illetve az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi és Kibervédelmi Intézet óradója. Kutatási területe A megújuló energiaforrások alkalmazásának lehetőségei a biztonságtechnikában. A biztonságtechnika történetének vizsgálata.

TAMPU Ferenc

fryczi@gmail.com

Ferenc TAMPU graduated as a history teacher at Eötvös Loránd University in 2004, followed by a master's degree in information and library science in 2016. He began his career in 2003 at the Library of the Faculty of

TAMPU Ferenc az Eötvös Loránd Tudományegyetemen 2004-ben történelem szakos tanári egyetemi diplomát, majd 2016-ban informatikus-könyvtáros oklevelet szerzett mesterképzésen. Pályafutását

Health Sciences at Semmelweis University, where he performed reader services and subject specialist duties for ten years. Since 2013, he has been responsible at the library's acquisition department. His work includes cataloging in terms of form and content, building the integrated catalog of the university, and ensuring that the faculty's collection remains up-to-date. In addition to his traditional librarian duties, he has been involved in faculty teaching for 13 years within the framework of the "Thesis Methodology" credit-bearing course. Topics covered in the course include: the place and role of the thesis in academic writing, formal requirements, structure, document literacy, literature review, use of databases, and professional research of academic information. In 2026, he began his research activities as part of a PhD program at the Doctoral School of Security Sciences at Óbuda University. His research area is OSINT (Open-Source Intelligence) in the service of academic research, with a particular focus on library science, medicine, and engineering.

2003-ban kezdte a Semmelweis Egyetem Egészségtudományi Karának Könyvtárában, ahol tíz évig olvasószolgálati és szaktájékoztatói feladatokat látott el. 2013-tól a könyvtár állománygyarapítását végzi. Munkájának része a beszerzett dokumentumok formai és tartalmi feltásása, az egyetem integrált katalógusának építése, a kar állományának naprakész biztosítása. A hagyományos könyvtárosi feladatai mellett 13 éve részt vesz a kari oktatásban Szakdolgozat módszertan kredites tantárgy keretén belül. A tantárgyhoz kapcsolódó témák: a szakdolgozat helye és szerepe a tudományos írásban, formai követelmények, struktúrája és felépítése, dokumentumismeret, szakirodalomkutatás, az egyetemi adatbázisok ismerete, a tudományos információ szakszerű kutatása. 2026-ban kezdte meg kutatási tevékenységét immár PhD képzés keretén belül is az Óbudai Egyetem Biztonságtudományi Doktori Iskolában. Kutatási területe: OSINT (Open-Source Intelligence) a tudományos kutatások szolgálatában, különös tekintettel a könyvtár-, orvos- és a műszaki tudományokban.

ZSARNOVSZKI Attila

zsarnovszki.attila@stud.uni-obuda.hu

Attila ZSARNOVSZKI is an electrical engineer and a registered member of the Hungarian Chamber of Engineers. He has more than thirty years of professional experience in engineering, inspection and conformity assessment activities related to industrial technologies operating in potentially explosive atmospheres. He is the founder and managing director of EX-ON Engineering Ltd., providing explosion protection engineering, expert, inspection and certification services. His professional activities focus primarily on the oil and gas industry, petrochemical technologies, pharmaceutical manufacturing and other hazardous industrial facilities. He is currently a PhD student at the Doctoral School of Safety and Security Sciences of Óbuda University. His research focuses on the assessment and temporal evolution of explosion safety conditions.

ZSARNOVSZKI Attila okl. villamosmérnök, a Magyar Mérnöki Kamara tagja. Több mint harminc éve foglalkozik robbanásveszélyes ipari technológiákhoz kapcsolódó mérnöki, felülvizsgálati és megfelelőségértékelési tevékenységekkel. Az EX-ON Mérnökiroda Kft. alapítója és ügyvezetője, amely robbanásvédelmi mérnöki, szakértői, felülvizsgálati és tanúsítási szolgáltatásokat nyújt. Szakmai tevékenysége elsősorban az olaj- és gázipar, a petrolkémia, a gyógyszergyártás és más robbanásveszélyes technológiák területére terjed ki. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD-hallgatója. Kutatási területe a robbanásbiztonsági állapotok értékelése és időbeli változásának vizsgálata.

Creator of the cover image | **A borítón látható kép alkotója**

BORS Györgyi

borsgyorgyi77@gmail.com

She was born in 1977 in Tapolca, Hungary. The tragic early death of his mother was decisive in her life because she was then raised in state care until she was 18 years old. During her years there, she realized

Magyarországon, Tapolcán született 1977-ben. Édesanyja tragikus korai halála meghatározó volt az életében, mert ezt követően 18 éves koráig állami gondozásban nevelkedett. Az ott töltött évek alatt jött rá,

that she found the greatest pleasure in art. She studied graphic art for several years at the Railway School of Music and Fine Arts in Budapest with the painter and sculptor György BENEDEK, and later with Árpád "Pika" NAGY and Zoltán SEBESTYÉN. In 2007 she graduated from the King Zsigmond College with a degree in Cultural Management. From 2017, her master is Kálmán GASZTONYI, from whom she learned the different techniques of oil painting. She is narrative painter. It is important for her to be creative about something, a feeling, an idea, an impression, or even a human quality. She creates using the tools of abstract painting. With her innovative style, she brings experiences, feelings and thoughts with the tools of painting to a universal level that we have all known or experienced in some form. Her work has been successfully featured in various domestic and international competitions and exhibitions (Budapest, London, New Jersey, Hong Kong) and has appeared in several contemporary art albums and art magazines. One of her works can also be found in the public collection of the Hungarian Museum of Circus Art. Her expression is geometric and lyrical abstract, which are side by side yet reinforce her art organically intertwined.

hogy a művészetben leli a legnagyobb örömet. Grafikai tanulmányokat folytatott több évig Budapesten a Vasutas Zene- és Képzőművészeti Iskolában BENEDEK György festő és szobrászművésznél, majd később NAGY Árpád „Pika"-nál és SEBESTYÉN Zoltánnál is tanult. 2007-ben diplomázott a Zsigmond Király Főiskola Művelődésszervező szakán. 2017-től Mestere GASZTONYI Kálmán, akitől elsajátította az olajfestés különböző technikáit. Narratív festő. Fontos számára, hogy alkotási szóljanak valamiről, egy érzésről, egy gondolatról, egy benyomásról, vagy akár egy emberi tulajdonságról. Az absztrakt festészet eszközeit felhasználva alkot. Innovatív stílusával olyan tapasztalatokat, érzéseket és gondolatokat emel a festészet eszközeivel egyetemes szintre, melyeket mindnyájan ismerünk vagy megéltünk már valamilyen formában. Munkái sikeresen szerepeltek különféle hazai és nemzetközi versenyeken és kiállításokon. (Budapest, London, New Jersey, Hong Kong) Több kortárs művészeti albumban, art magazinban jelentek meg munkái. Egyik alkotása a Magyar Cirkuszművészeti Múzeum közgyűjteményében is megtalálható. Kifejezésmódja a geometriai- és lírai absztrakt, melyek egymás mellett, de mégis szervesen összefonódva erősítik művészetét.

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 8, No 2, 2026. | **2026. VIII. évf. 2. szám**

CONTENT | TARTALOM

DOI: https://doi.org/10.12700/btsz.2026.8.2.1

CIVIL PROTECTION AND CRITICAL INFRASTRUCTURE IN BUDAPEST – SHELTER SYSTEMS, ORGANIZATIONAL STRUCTURES AND THE ROLE OF INDUSTRIAL PROTECTION IN CIVIL DEFENCE

LAKOSSÁGVÉDELEM ÉS KRITIKUS INFRASTRUKTÚRA BUDAPESTEN – ÓVÓHELYI RENDSZEREK, SZERVEZETI STRUKTÚRÁK ÉS AZ IPARVÉDELEM SZEREPE A POLGÁRI VÉDELEMBEN

LŐCSEI Anikó[1]

Abstract

Civil protection is a continuously evolving field of state security policy. This study presents the development of shelter systems and the conditions of civilian protection during wartime, with particular attention to Budapest's shelter network and the historical background of the Hungarian civil protection system. The analysis examines the organizational structure of civil defense during the Cold War period, as well as the characteristics of international and domestic civil protection models. The research investigates industrial evacuation and relocation processes between 1970 and 1980, the operation of industrial disaster management systems, and the main elements of flood defense and emergency planning. The study also introduces the development of modern decision-support systems, focusing on the application of geoinformatics, sensor technologies, and artificial intelligence in contemporary disaster management.

Keywords

civil protection, critical infrastructure, industrial facilities, shelter systems, decision support

Absztrakt

A lakosságvédelem az állami biztonságpolitika folyamatosan fejlődő területe. A tanulmány bemutatja az óvóhelyi rendszerek kialakulását és a háborús időszak lakosságvédelmi viszonyait, különös tekintettel Budapest óvóhelyi hálózatára és a polgári védelem fejlődésének történeti hátterére. Az elemzés kitér a hidegháborús időszak polgári védelmi szervezeti rendszerére, valamint a nemzetközi és hazai lakosságvédelmi modellek fejlődési sajátosságaira. A kutatás vizsgálja az 1970–1980 közötti időszak ipari kimenekítési és kitelepítési folyamatait, az üzemi katasztrófavédelmi rendszerek működését, valamint az árvízi védekezés és a veszélyhelyzeti tervezés főbb elemeit. A tanulmány bemutatja a modern, mai döntéstámogatási rendszerek fejlődését is, különös tekintettel a térinformatikai, szenzoros és mesterséges intelligencia alapú megoldások alkalmazására a katasztrófavédelem területén.

Kulcsszavak

lakosságvédelem, kritikus infrastruktúra, ipari létesítmények, óvóhelyi rendszerek, döntéstámogatás

[1] locsei.aniko@bparchiv.hu | ORCID: 0009-0005-7070-1982 | chief archivist, Budapest City Archives | főlevéltáros, Budapest Főváros Levéltára

BEVEZETÉS

A tanulmány bemutatja az óvóhelyek történeti kialakulását és fejlődését, valamint Budapest területén való elhelyezkedésüket egy 1944-es fővárosi térkép alapján, amely óvóhelyi kataszterként szolgál, mint elsődleges védelmi forrás.

A lakosság védelme a modern állami biztonságpolitika egyik alapvető, válsághelyzetekben különösen felértékelődő területe. A hidegháború időszakában kiépített polgári védelmi rendszerek ezt elsősorban szervezési, műszaki és igazgatási eszközökkel biztosították, kiemelt szerepet adva a kockázati információk központi kezelésének.

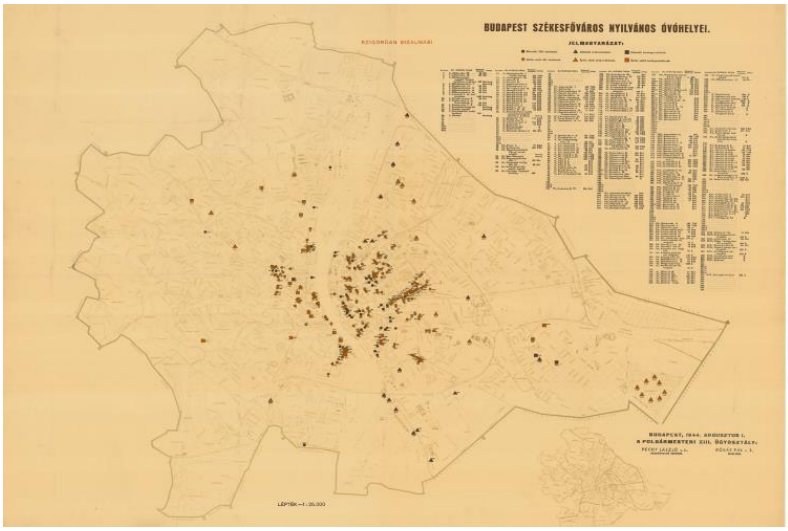
A kutatás a 1970–1980 közötti időszakot vizsgálja, mert ekkor a polgári védelem rendszerben egyszerre volt jelen a korábbi, korábbi védelmi eredetű struktúrák és a béke-időszaki modernizáció. Ez az átmeneti korszak lehetővé teszi a hagyományos és a centralizált államigazgatási védelmi megoldások együttes elemzését.

A vizsgálat középpontjában az 1976. évi polgári védelmi szabályozás és a kapcsolódó szervezeti dokumentumok állnak, kiegészítve szakirodalmi forrásokkal. A tanulmány célja a polgári védelem szervezeti fejlődésének és a kockázatalapú tervezés működésének feltárása, amely hozzájárulhat a korszerű lakosságvédelmi rendszerek további vizsgálatához.

Óvóhelyi hálózat kialakulása, típusai, osztályozási rendszere

Az egységes légoltalmi elvek bevezetése során a lakóházak óvóhelyeinek kialakítását a Székesfővárosi Közmunkák Tanácsa 1937. január 16-án rendelte el. Ekkor a kezdetleges védelmet nyújtó **TGS (törmelék-, gáz- és szilánkbiztos**) óvóhelyek jelentek meg. Az 1939: II. törvénycikk további TGS, később szükségóvóhelyek létesítését írta elő, utóbbiakat a beépített területeken, legalább 20 fő befogadására létesítették, védelmi funkciója a magasabb épületek talajszintje alattiak esetében korabeli szakirodalmi leírások szerint magasabb védelmi szintet biztosított. Budapesten 1941-ben 310 körzetben indult meg az építés. Az egyszerű **árokóvóhelyeket** – amelyek főként pince hiányában, kb. 2 m mélyen készültek – később S (szilánkbiztos) típussá fejlesztették. 1942-ig mintegy 6 km hosszban, 18 000 főre, 1944 tavaszára pedig 14 km-en, 40 000 főre tervezték őket. A szükségóvóhelyeket **RH (régiház)** óvóhelyekké minősítették (pincék, alagsorok stb.), míg a **BGS (bomba-, gáz- és szilánkbiztos)** típusok légitámadások ellen készültek. **Barlangóvóhelyek** Budapesten a Várhegy alatti szakaszban létesítettek a Sziklaközpont közelében, amely 1.600 fő befogadására volt alkalmas. 1944 tavaszára Budapesten 47 nyilvános óvóhely működött, mintegy 10 500 fő számára, azonban a védelem lefedettsége nem volt teljes körű: a lakosság kb. 65%-a (vidéken 30–35%) jutott óvóhelyhez. 1945-ben, Budapest bombázásai során a várost 37 találat érte. A civil áldozatok számát a szakirodalomban mintegy 38 000 főre becsülték, ugyanakkor későbbi kutatások ennél magasabb veszteséget valószínűsítenek. A háborút követően 1950-re a légoltalom kiépítése során városokat besorolták és kitelepítési terveket vezettek be, valamint 20 fő felett kötelezővé tették az óvóhelyek létesítését. Az óvóhelyeket I–V. osztályba sorolták, ahol a magasabb szám alacsonyabb védelmi kategóriát jelentett. A III–V. osztályú létesítmények különböző fokú, telitalálat elleni és gázvédelmi képességekkel rendelkeztek, zsiliprendszeres kialakítással.[1]

Az alábbi térkép a budapesti óvóhelyek elhelyezkedését és térbeli eloszlását mutatja, bemutatva azok koncentrációját Budapest főváros egészére nézve:

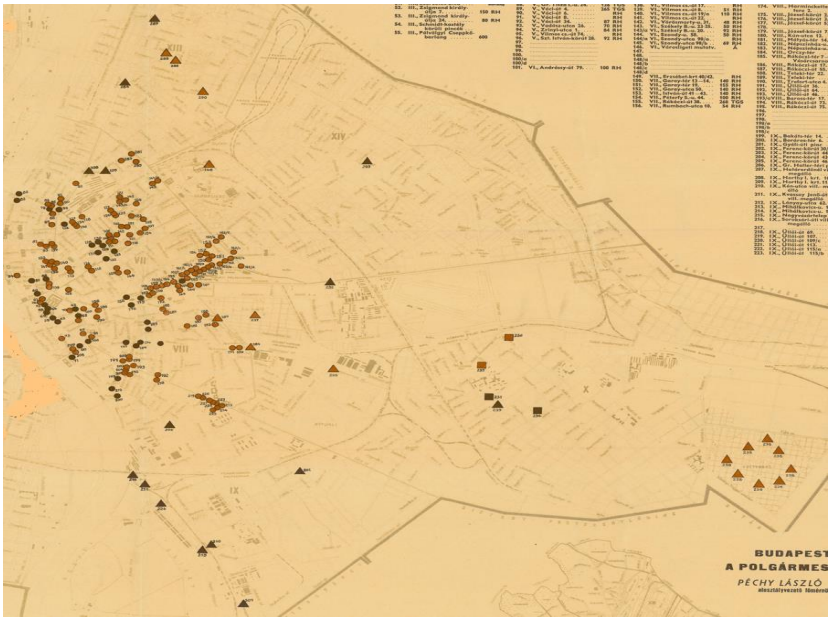


1. Ábra: Budapest nyilvános óvóhelyeinek térképe 300 óvóhely jelölésével és minősítésével (árok, barlang stb.), 1944. nyilvánosan megtekinthető a Hungaricana közgyűjteményi portálon, forrás: Budapest Főváros Levéltára (BFL).[2]

A 6. ábrán Budapest budai oldala az I–III., XI., XII. és XXII. kerületek nyilvános óvóhelyei láthatók:

2. Ábra: Budai kerületek nyilvános óvóhelyeinek térképe óvóhelyek jelölésével és minősítésével (árok, barlang stb.), 1944. nyilvánosan megtekinthető a Hungaricana közgyűjteményi portálon, forrás: Budapest Főváros Levéltára (BFL).[2]

A 7. ábra Budapest pesti oldalán a V–X. és a XIII–XIV. kerületek nyilvános óvóhelyeit mutatja be:



3. Ábra: Budai kerületek nyilvános óvóhelyeinek térképe óvóhelyek jelölésével és minősítésével (árok, barlang stb.), 1944. nyilvánosan megtekinthető a Hungaricana közgyűjteményi portálon, forrás: Budapest Főváros Levéltára (BFL).[2]

4. Ábra: A térképen látható jelmagyarázat jelölése az óvóhelyek minősítésére vonatkozóan (árok, barlang stb.), 1944. nyilvánosan megtekinthető a Hungaricana közgyűjteményi portálon, forrás: Budapest Főváros Levéltára (BFL)[2]

A polgári védelem kialakulása és a lakosságvédelem a hidegháború idején

A NATO (North Atlantic Treaty Organization) polgári védelemben betöltött meghatározó szerepe az 1950-es évek elejére vezethető vissza. 1952. november 19-én a NATO Tanácsa létrehozta a Polgári Védelmi Bizottságot (Civil Defence Committee), amely a tagállamok közötti polgári védelmi tevékenységek koordinációját látta el. A bizottság eredeti célja a hátországvédelem megerősítése és a háborús helyzetekre való felkészülés támogatása volt, széles körű, több ágazatra kiterjedő védelmi rendszer kialakításával. A feladatok összehangolására később létrejött a Polgári Szükséghelyzet Tervező Főbizottság (Planning Board for Civil Emergency Planning), amely a szakbizottságok munkáját koordinálta a NATO főtitkárának irányítása alatt. A főbizottság alárendeltségében több, különböző területre – így például hírközlésre, iparra, egészségügyre és polgári szükséghelyzeti tervezésre – fókuszáló szakbizottság működött.[3]. A Polgári Védelmi Bizottság tevékenysége és a szakbizottságok működése a hidegháborús környezetben jelentős szervezeti és elvi fejlődést

eredményezett. Ezzel párhuzamosan a német polgári védelmi rendszer a NATO által kidolgozott felkészültségi és reakciós elveket adaptálva alakította ki saját védelmi gyakorlatát, amely hatékony válaszadási képességet biztosított a különböző veszélyhelyzetekre.

A nyugat-német polgári védelem hidegháborús kiépülése túlmutatott az állami intézményrendszeren, és kiterjedt a civil segélyszervezetek, valamint a katonai egészségügyi szolgálatok együttműködésére is. A Technisches Hilfswerk (THW) és a Német Vöröskereszt önkéntes részvétele jelentős szerepet játszott a polgári felkészültség fejlesztésében, míg a katasztrófaorvoslás fejlődése mindenre kiterjedő veszélyhelyzeti megközelítést alkalmazott a nukleáris, kémiai és ipari kockázatok kezelésében. A katonai és civil egészségügyi szereplők együttműködése szakmai irányelvek összehangolásával hozzájárult a rendszer integrált működéséhez. Ezt a fejlődési irányt erősítette a Katastrophenschutzergänzungsgesetz (1989), amely a korábbi KatSG-68 jogszabály kiegészítéseként a nyugatnémet polgári védelem strukturáltabb működését biztosította. [4] A hazai polgári védelem fejlődésének értelmezéséhez a nemzetközi és nyugat-európai példák fontos viszonyítási alapot jelentenek. A magyar polgári védelem fejlődése sajátos történeti és politikai környezetben zajlott, ugyanakkor több ponton párhuzamokat mutatott a nemzetközi tendenciákkal.

A hazai polgári védelmi rendszer fejlődése és rendszerei

A hazai polgári védelem lakosságvédelmi tervezésének és végrehajtásának alapját a hidegháború időszakában kialakított jogszabályi és normatív keretek adták, amelyek közül meghatározó szerepet töltött be az 1960. évi IV. törvény, amely új alapokra helyezte a polgári védelem szervezetét. A következő táblázat összefoglalja a polgári védelem kialakulásának és fejlődésének főbb állomásait a szocialista időszakban, kiemelve a lakosságvédelmi feladatok szervezését és végrehajtását.

Év	Feladat meghatározása
1945	Légoltalmi szervezet felszámolása, kiképzések megszüntetése
1950–1951	BM VI. Főosztály alatti újjászervezése, kötelező óvóhelyépítés, **BM Légoltalom Országos Parancsnoksága** megalakulása
1951	Központi légoltalmi iskola megnyitása a képzés biztosítására
1953	Üzemi légoltalom megszervezése
1955	Nukleáris, biológiai, vegyi fegyverek elleni védelem előkészítése
1956–1957	Gyakorlatok és újjászervezés, alakulatok és szervezeti stabilizálás
1960	**Teljes állomány átszervezése (1960. évi IV. törvény)**

1. Táblázat: A polgári védelem fejlődésének főbb állomásai (1950–1960).
Forrás: Tolna Megyei Népújság, 1985. október (korabeli sajtóközlés), saját szerkesztés*[5]*

Az 1950-es évek közepétől a nukleáris fegyverek terjedése jelentősen formálta a magyar légoltalom feladatait, amely 1964-ben az Elnöki Tanács 1. számú rendelete szerint „Polgári Védelem” néven folytatta tevékenységét. A polgári védelem fő célja a lakosság és a népgazdaság védelme, valamint a tömegpusztító és hagyományos fegyverek és katasztrófák elleni mentő- és helyreállító feladatok megszervezése volt. 1961–65 között mintegy 1-2 milliárd forintot fordítottak a fejlesztésre, a 60-as évek végére a szervezetekbe 700 000

főt soroltak be, és a megyei nagy gyakorlatokon 1970-re több tízezres nagyságrendű részvétel volt jellemző. Az 1970-es felsőtiszai árvízi tapasztalatok igazolták a rendszer felkészültségét, ugyanakkor a 1976-os átszervezés során a katonai integráció érdekében jelentős létszámcsökkentés történt. 1976-ban létrehozták a Polgári Védelmi Kiképző Központot Budapesten, és országszerte korszerű kiképző bázisok, valamint 1976–1988 között új, korszerűsített óvóhelyeket is létesítettek.[6]

A polgári védelem megszervezését célzó, 1949-ben elfogadott IV. genfi egyezményt 1977-ben két jegyzőkönyv egészítette ki. Az első fegyveres összeütközések áldozatainak védelméről szólt, amelyben megjelent a polgári védelmi feladatrendszer. A 6. cikk a Vöröskereszt békeidőben betöltött szerepét hangsúlyozza, a 61. cikk a polgári védelem általános feladatait tartalmazza.[7]

Fővárosi polgári védelmi egységek területi és szervezeti felosztása

A főváros közigazgatási egységeinek kialakítása a veszélyeztetettségi fokozatok figyelembevételével történt. Az 1960 után fokozatosan megerősített polgári védelmi alakulatokat védelmi és mentesítési feladatokra alkalmazták. Az 2041/1974. (Mt. h.) határozat a polgári védelem alapvető szabályait rögzítette, amelyet végrehajtási rendeletek egészítettek ki. A rendszer a fővárosban a veszélyeztetettségi és kockázati szempontok alapján működő gyakorlatokkal, valamint a termelő üzemek bevonásával valósult meg, szoros együttműködésben az államigazgatási és tanácsi szervekkel. A lakosság és a legfontosabb veszélyeztetett üzemek dolgozói számára megfelelő az óvóhelyek létesítését programja. A jogállás és irányítási rendjének biztosításához, az operatív feladatok irányozta elő. A minisztériumok ágazati felelősségét és hatáskörét szakterületi feladatok ellátásához tartották fontosnak. A hatásköri feladatok ellátásában az állami szervek (minisztériumok, országos hatáskörű szervek, tanácsok, vállalatok és intézmények, valamint a szövetkezetek vezetői vettek részt.[8]

A központi szervek és üzemek kijelölését az Országos Tervhivatal, az illetékes miniszterek és a honvédelmi miniszter irányították. Az 9/1976. (HM) rendelet új alapokra helyezte a polgári védelem szervezetét és irányítását, különösen a fővárosban. A rendszer célja a támadó fegyverek hatása elleni védekezés, valamint a hatékonyabb, önvédelmi és hatósági területvédelmi szervezetek kiépítése volt.

Hatósági és önvédelmi szervezetet, 3 fontosabb egységbe sorolták:

- Az I. csoporthoz sorolt egységet a kiemelt területek és városok védelmére szervezték meg.
- A II. csoport egységei a városok és községek területén elsősorban a saját, és az I. csoportba sorolt városok lakosságának védelmét.
- A III. csoportba azok az egységek tartoztak, amelyek városok, községek és járások saját, de ezen túlmenően az első 2 csoportba sorolt feladatait is ellátta.

A háborús időszakban az üzemekben a polgári védelem hatósági (szakszolgálati) és önvédelmi szervezetei vettek részt a kitelepítésben. A hatósági alakulatok központosított riasztási, kitelepítési, befogadási, egészségügyi, műszaki mentési, óvóhelyi, tűzvédelmi, élelmezési és RBV-feladatokat láttak el, valamint ellenőrzési jogkörrel rendelkeztek, míg az önvédelmi egységek helyi, gyors beavatkozású mentési és ellátási feladatokat hajtottak végre. A fővárosi szervezet a Polgári Védelem Országos Parancsnoksága alárendeltségében működött, kerületi parancsnokságokkal, felderítő és RBV (radiológiai, biológiai, vegyi) védelmi egységekkel:

5. Ábra: Fővárosi Polgári Védelmi Igazgatóság szervezeti ábrája, forrás: A polgári védelmi szervezetek továbbfejlesztésének szabályai PVOP kiadása alapján, 1976, 43.pp. saját szerkesztés. [9]

A szervezet megalakulási bázisa, rendeltetése és vezetősége:

- Parancsnokság: A Fővárosi Tanács apparátusa: parancsnok, politikai helyettes, MIR parancsnok (5 fő)
- Törzskiegészítő állomány: operatív törzs tagjai voltak, szakágazati előadók, 14 fő.
- Önálló felderítő Szakasz: Szerepe a fővárosi tanács közvetlen irányítása alá tartozó üzemek, vállalatok, intézmények. Feladata a PV erők menetvonalainak támadása következtében kialakult kárterületek felderítése. Felső vezetők a parancsnokok és alárendelt állomány összesen 36 fő volt.
- Önálló Robbantó Raj: megalakulási bázis azon üzemek, vállalatok, amelyek robbantási tevékenységhez engedéllyel rendelkeztek, omlás veszélyes falak, épületszerkezetek, átjárók, védőlétesítmények részére gödrök robbantása állomány: rajparancsnok és robbantók összesen 3 fő.
- Önálló RBV Biztosító Század: Megalakulási bázisa a tanácsi alárendeltségű javítószolgáltató üzemek, intézmények. Rendeltetése a víz kitermelése, RBV ellenőrzése, mentesítése, vegyvédelmi anyagok, RBV műszerek javítása, sugáradag központosított kezelése (nyilvántartás, értékelés, ellenőrzés). Állománya: felsőbb szinten a század parancsnok, politikai helyettes és alárendeltek létszáma 4 fő. Alárendeltségébe tartozott az **Ivóvíz Biztosító Szakasz** 2 fő, és feladata az ivóvíz kitermelése, vízmentesítés, szállítás, fertőtlenítő gépkocsi, a szakasz alárendelt raj összlétszáma 22 fő. A RBV szd. másik legfontosabb ága a **RBV Mentesítő és Sugáradag Ellenőrző Állomáson** 2 fő, az állomás alá tartozott a RBV Század Minősítő Részleg: vezetője a részlegparancsnok, ahol egy vegyész, egy biológus, egy radiológus és szaktechnikai állomány 8 fővel, a másik a Sugáradag Ellenőrző Részleg 8 fő legénységgel rendelkezett. Az állománnyal egyenrangú minőségben állt a **RBV Anyagjavító és Hitelesítő Állomás**, vezetője az állomás parancsnok, vegyivédelmi anyag- és műszerjavító részlegek szerepeltek, összesen 17 fővel. A RBV század összesen 63 főből állt.[9]

Üzemi, árvízvédelmi és kitelepítési szolgálatok

Budapest az 1970-1980-as években Magyarország legfontosabb ipari központjává vált, ahol az ország ipari termelésének jelentős része koncentrálódott. A főváros veszélyeztetettsége több tényező mentén értelmezhető, így a tűz- és robbanásveszélyes üzemek, az ipari vegyi szennyezések, a radiológiai balesetek, valamint a Dunamenti kerületek esetében az árvízi katasztrófák alapján. Békeidőben a főváros ipari létesítményei teljes kapacitással működtek, míg rendkívüli helyzetben működésük korlátozását vagy leállítását irányozták elő. A veszélyeztetettség mértéke ettől függött, mivel az üzemek kiemelt kockázatot jelentettek a dolgozókra és a környező lakosságra.

A gyárak és üzemeik az ágazati szakminisztériumok fenntartásával működtek, fontosabb veszélyességi ágazatok: gépgyártás a Kohó- és Gépipari Minisztérium (KGM) felügyelete alatt, a vegyipar, gyógyszeripar és nehézipar – például vas- és acélgyártás – a Nehézipari Minisztérium (NIM) irányítása mellett, míg a bőr-, textil- és könnyűipar a Könnyűipari Minisztérium (KIM), a mezőgazdasági és élelmiszeripari területek pedig a Mezőgazdasági és Élelmezésügyi Minisztérium (MÉM) felügyelete alatt működtek. Az ipari irányítás ágazati széttagoltságát tükrözte, és egyben lehetővé tette a védelmi, termelési és működési prioritások meghatározását. A gyártás jellege meghatározta az üzemek védelmi hálózatát. A katasztrófavédelmi egységek összetett gyakorlatok alapján mutatták be a tervszerűen meghatározott káresemények riasztási, kitelepítési, mentesítési és kárfelszámolási feladatait, figyelembe véve az ágazati irányításból fakadó sajátos működési rendet és követelményeket, illetve a gyártás során alkalmazott anyagokat.

Az üzemi katasztrófák kármentesítését módszertani tervek alapján, komplex gyakorlatok keretében hajtották végre a veszteségek minimalizálása érdekében. A védelmi erők a parancsnokság intézkedési tervei szerint szervezték az egyéni védőeszközök ellátását és a dolgozók, valamint családtagjaik kitelepítését.

Feladataik üzemi katasztrófa esetén:

- Az üzem háborús állóképességének növelése.
- Szakszolgálati és önvédelmi parancsnoki csoport bevonásával a csapás utáni tevékenység mentő, mentesítő és halaszthatatlanul szükséges munkálatok.
- Üzemi technológiai leírások, tervek védett elhelyezése.
- Védőlétesítmények kiürítése, berendezések, személyi anyagi feltételek megteremtése.
- Riasztás és hangosítók biztosítása.
- Intézkedik a RBV védelmi tervben foglalt feladatok betartására.
- Elrendeli a különleges gépek, robbanóanyagok, savak, gázok védett elhelyezését
- Intézkedtek a befogadási helyek előkészítéséről, szállítási tervek megvalósításáról, üzem és védett objektum őrzésvédelmének fenntartásáról.
- Gondoskodik az érintett veszélyeztett lakosság és üzemi dolgozók, hozzátartozók elszállításáról.

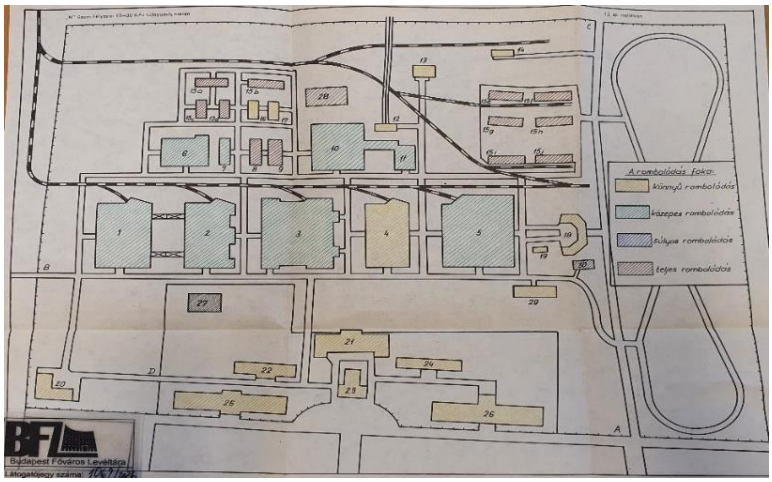
A levezetési gyakorlat egy feltételezett üzemi robbanási esemény hatásainak modellezését tartalmazza, amely során a túlnyomási zónák (10–30 kPa és 50–100 kPa) alapján folytatták le a műveleti tervet. A tervek szerint egy 50 kt hatóerejű földi robbanás következtében az „N" város területén elhelyezkedő ipari üzemet enyhe, 0,1-0,3 kp/cm² (10-30 kPa) és súlyos fokozatú rombolódási zónába soroltak, ahol a túlnyomás értéke 0,5-1 kp/cm² (50-

100 kPa). A robbanás következtében az üzemben összefüggő, mintegy 3000 m² kiterjedésű tűzterület alakult ki.

A gyakorlat során az alábbi kiinduló városi, üzemi tervezéshez szükséges adatok kerültek meghatározásra:

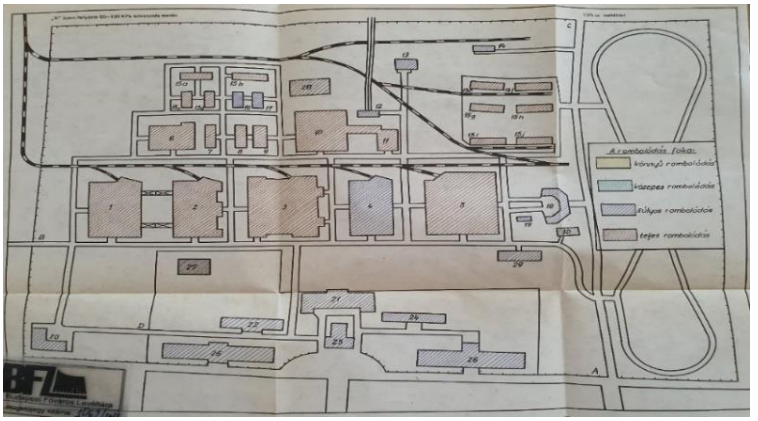
- Az érintett város I. csoportba sorolt település lakossága: 56.409 fő.
- A város területe: 535.800 m².
- Az érintett üzem sűrűn beépített, gyáregységek közötti területen helyezkedik el.
- Az üzem beépített alapterülete: 44.449 m².
- Beépítettség foka: 8,29%.
- Tűzveszélyességi besorolás: „D" kategória.
- Gazdasági tevékenység: gépipari nagyüzem (precíziós szerszámgépek, forgácsoló- és fémipari gépek gyártása).
- Dolgozók száma: 5.000 fő
- Műszakrend: két műszak, legnagyobb műszaklétszám 3.000.
- Polgári védelmi és üzemi létszám összesen: 830 fő.

A vizsgált üzemi területet érő lökőhullám túlnyomása megközelítőleg 0,1-0,3 kp/cm² (≈10-30 kPa) volt, amely az enyhétől a közepes szintű rombolódási zóna tartományába sorolható. E nyomástartományban az épületszerkezetek részleges károsodása, a könnyűszerkezetes elemek sérülése, valamint személyi sérülések kialakulása valószínűsíthető. A vizsgálat egy tervezett, szimulált üzemi kimenekítési gyakorlat keretében történt.



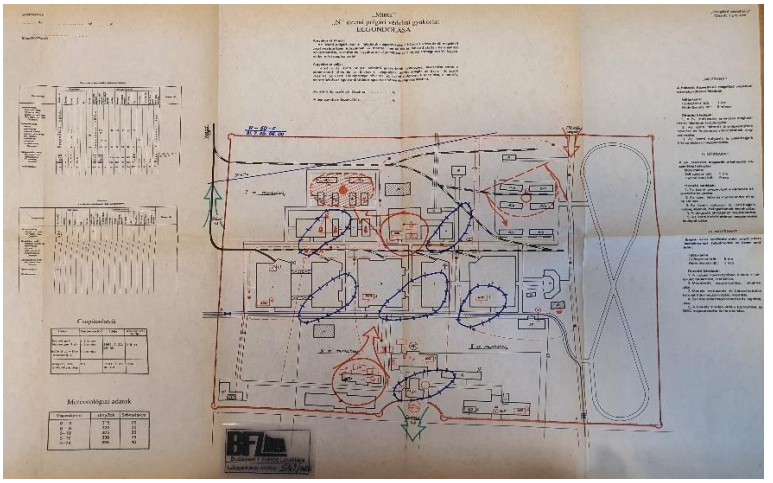
6. Ábra: A 10–30 kPa túlnyomású peremzóna hatásainak vázlata. Jelmagyarázat rombolódási szintekről: sárga- könnyű, zöld- közepes, lila- súlyos, barna- teljes rombolódási fokozat, forrás: Módszertani Útmutató, Üzemi Komplex pv. gyakorlat tervezésére és levezetésére, PVOP (1980) 12. sz. melléklete, saját szerkesztés[10].

A vázlatterv 12/b.sz. mellékletében (lásd 3. ábra) az üzemi területet ért lökőhullám túlnyomása megközelítőleg 0,5-1 kp/cm² (≈50-100 kPa) volt, amely a súlyos rombolódási zóna tartományába esett. A az épületszerkezetek teljes, illetve súlyos rombolódási fokozata látható.



7. Ábra: A 50–100 kPa túlnyomású peremzóna hatásainak vázlata. Jelmagyarázat rombolódási szintekről: sárga- könnyű, zöld- közepes, lila- súlyos, barna- teljes rombolódási fokozat, forrás: Módszertani Útmutató, Üzemi Komplex pv. gyakorlat tervezésére és levezetésére, PVOP (1980) 12/b. sz. melléklete, saját szerkesztés[10].

A káreseményeknél vészhelyzeti tervek tartalmazták az adott gyakorlati szabályokat, elsőként a levezetéshez szükséges gyakorlati elgondolási tervet részletezett munkatérkép és a terven megjelölt legfontosabb adatok alapján hajtották végre:



8. Ábra: Komplex üzemi-védelmi gyakorlat elgondolási terve, üzemi vezetési pontok, kitelepítési útvonalak, közműhálózat nyomvonalai, elzárási útvonalak, kármentés és mentesítési vázlata. Forrás: Módszertani Útmutató, Üzemi Komplex pv. gyakorlat tervezésére és levezetésére, PVOP (1980) 3. sz. melléklete, saját szerkesztés[10].

A kárelhárítás során az üzemi erők a szakszolgálatokkal együtt végezték a mentési és kárfelszámolási feladatokat: a mentő- és tűzvédelmi egységek a romok eltávolításában és a tüzek lokalizálásában, az egészségügyi szakasz az elsősegélynyújtásban, az RBV szakasz pedig a sugárellenőrzésben vett részt. A gyakorlatban 2500 fő kitelepítése történt Pest megyei befogadó településekre.[10] A többtényezős tervezési szemléletnek a fővárosi árvízvédelem során gyakorlati jelentősége volt

Árvízveszély esetén a tavaszi-nyári árhullámokkal kellett számolnia a védelmi erőnek. Közvetlenül veszélyeztett üzemi létesítmények, partszakasz melletti lakóházak védelme valósul meg. A legfontosabb védekezési területek a III., XI., XXI. és XXII. kerületek partmenti létesítményei. Egyik ismertebb árvízi esemény Budapesten 1965. június 18-án következett be. A Duna árhulláma 845 cm-en tetőzött. Budapesten a római-parti üdülőterületet ki kellett üríteni, több észak-budai és pesti töltést meg kellett erősíteni vagy át kellett építeni. A budatétényi és a Szilas-patak menti védművek nem bizonyultak elégségesnek, ezért több helyen gépi földmunkával és körtöltések építésével növelték a biztonságot. A Margit-szigeten is védekezni kellett a fakadó vizek ellen, homokzsákos erősítéssel és szivattyúzással. A folyó mértékadó árvízszintjét a Vigadó-téri vízmérce tartalmazza.[11]

A Kitelepítési szakszolgálat a polgári védelem rendfenntartó, szállító, híradási, egészségügyi, élelmezési és ivóvízellátási egységeivel együttműködve szervezte a lakosság kitelepítését és óvóhelyi elhelyezését. A fővárosi polgári védelmi parancsnok irányítása alatt, a kerületi parancsnokságokon keresztül működve a szakminisztériumi és helyi szervekkel összehangoltan biztosította a kitelepítést meghatározott útvonalakon a befogadó területekre. A befogadási szakszolgálat a megyei és járási szervekkel együttműködve gondoskodott az alapellátásról.[12] A 20. század végére a biztonsági rendszerek működésében szerepet kaptak az informatikai és hálózati megoldások. Az 1985 után a polgári védelem számítástechnikai és hálózati alapú vezetési rendszereket alkalmazott, amelyek a távközlési és operatív információáramlást támogatták. A RIA készültségi rendszer és az ügyeleti törzs az intézkedési tervek végrehajtását és az információszolgáltatást biztosította, korai számítógépes és telex-alapú rendszerek a Comodore 64 felhasználásával. A sugárhelyzet-értékelő alrendszer a polgári védelmi és katonai sugárfigyelő hálózatok, valamint meteorológiai adatok alapján végezte a helyzetértékelést. Az Országos Meteorológiai Szolgálat (OMSZ) által fejlesztett modellek a légköri terjedést, az eredő szélvektorokat és a domborzati hatásokat is figyelembe vették A rendszer feladata volt továbbá az atomcsapások paramétereinek, az epicentrumoknak és a 30 kPa túlnyomási zóna határainak meghatározása, valamint földi robbantások esetén a szennyezett felhő terjedési irányának és zónáinak becslése. A vegyi és sugárhelyzet-értékelés eredményei közvetlenül támogatták a polgári védelmi erők vezetését és beavatkozási döntéseit.[13]

Míg a 20. század második felében a polgári védelem működését elsősorban írott intézkedési tervek, manuális nyilvántartások és kezdetleges számítógépes rendszerek – a korszakban előforduló korai mikroszámítógépes megoldások (pl. Commodore 64 alapú alkalmazások) – is támogatták, addig napjaink katasztrófavédelmi rendszerei egyre inkább mesterséges intelligenciára és gépi tanulási modellekre épülnek. A korabeli rendszerek főként a sugárhelyzet-értékelés, a készültségi fokozatok kezelése és az operatív döntéshozatal támogatására szolgáltak, míg a modern adatvezérelt rendszerek már valós idejű szenzorhálózatok, meteorológiai adatok és előrejelző algoritmusok alapján működnek.

A gépi tanulás alkalmazásával ma már lehetőség nyílik az árhullámok, ipari balesetek vagy radiológiai szennyezések több nappal korábbi előrejelzésére, az automatikus riasztási láncok működtetésére, valamint a kitelepítési és védekezési döntések támogatására. Ezáltal a korábbi reaktív védekezési modell fokozatosan proaktív, előrejelzés-alapú katasztrófavédelmi rendszerré alakult.[14]

Hasonló elven működik az árvízi helyzet mérése nemzetközi szinten, ahol a korszerű árvízvédelmi rendszerekben a mesterséges intelligencia és a prediktív modellek valós

idejű meteorológiai, hidrológiai és szenzoradatok feldolgozásával képesek az árvízi kockázatok előrejelzésére és a veszélyzónák dinamikus meghatározására. [15] Magyarországon a mesterséges intelligenciához közelítő megoldások elsősorban a hidrológiai és meteorológiai előrejelző rendszerekben, valamint a katasztrófavédelem térinformatikai alapú döntéstámogató rendszereiben jelennek meg, amelyek a valós idejű adatfeldolgozás és kockázatelemzés révén támogatják a védekezést. [16]

Magyarországon a katasztrófavédelmi rendszerekben a digitális riasztási láncok, a térinformatikai (GIS) alapú helyzetértékelés és a veszélyhelyzeti modellek egyre inkább adatvezérelt, döntéstámogató rendszerekben működnek, amelyek a valós idejű információfeldolgozás révén a beavatkozások hatékonyságát növelik.[17]

A katasztrófavédelmi és sürgősségi műveletek hatékonyságának növelésében egyre nagyobb szerepet kapnak a dróntechnológiák, a mesterséges intelligencia (MI), valamint a gépi tanulási rendszerek. A modern veszélyhelyzetek – például ipari balesetek, földrengések, villámárvizek vagy erdőtüzek – gyors reagálást és valós idejű döntéstámogatást igényelnek. A drónok előnye, hogy gyorsan és biztonságosan képesek veszélyes vagy nehezen megközelíthető területek felderítésére. A drónokban elhelyezkedő kamerák és szenzorok valós idejű adatokat szolgáltatnak, amelyek támogatják a mentési műveletek irányítását és az evakuációs döntéseket. Hatékonyak lehetnek gyors lefolyású események – például robbanások, földrengések vagy vegyi balesetek – esetén. Különböző dróntípusok alkalmazásával és szenzoros eszközökkel – például kamerát, hőkamerát vagy levegőösszetétel-szenzort – rendel a természeti és civilizációs katasztrófák, például tüzek, árvizek, földrengések vagy veszélyesanyag-balesetek kezeléséhez. [18] A jelenkori technológiai fejlődés, így a gépi tanulási algoritmusok nagy mennyiségű adat feldolgozására képesek, miközben robusztusan kezelik a zajos vagy hiányos adatállományokat is. A katasztrófavédelem munkáját a neurális hálózatok alkalmazása is támogatja, mivel lehetővé teszik komplex térinformatikai és vizuális adatok feldolgozását, például drónfelvételek automatikus elemzését, objektumfelismerést, pontfelhő-feldolgozást, valamint sérült infrastruktúrák gyors azonosítását. Az automatizált rendszerek támogatják az evakuációs útvonalak kijelölését, a veszélyzónák meghatározását és a mentési erőforrások hatékonyabb koordinációját.[19]

A korábbi polgári védelmi rendszerekben a katasztrófavédelmi és lakosság-evakuálási feladatok összehangolása szervezési és technológiai szempontból jelentősen összetettebb és korlátozottabb volt, ugyanakkor az akkori fegyelmezett, centralizált és tervalapú működés fontos alapot teremtett a mai korszerű rendszerek kialakulásához. A háborús és katasztrófahelyzetek során szerzett tapasztalatok, valamint a történeti mentési és védelmi egységek működése hozzájárultak a modern, adatvezérelt és integrált katasztrófavédelmi megoldások fejlődéséhez, így a mai rendszerek hatékonysága jelentős mértékben támaszkodik a korábbi időszakok szervezési és operatív tanulságaira.

Az ipari kimenekítési és üzemi katasztrófavédelmi rendszerek vizsgálata továbbá rámutat arra, hogy a nagy létszámú dolgozói állományok védelme és szervezett kitelepítése már a korábbi polgári védelmi rendszerekben is kiemelt feladat volt. Az üzemi szintű védekezés, a szakszolgálati egységek összehangolt működése, valamint a kitelepítési és mentési tervek gyakorlati végrehajtása komplex szervezési hátteret igényelt, amely a veszélyhelyzeti tervezés egyik alapvető pillérévé vált. Ezek a rendszerek – bár technológiailag korlátozottabb környezetben működtek – jelentős tapasztalatot biztosítottak a lakosságvédelmi és iparbiztonsági feladatok integrált kezeléséhez. A jelenkori katasztrófavédelmi megoldások,

különösen a térinformatikai, szenzoros és mesterséges intelligencián alapuló rendszerek, ezekre a történeti alapokra épülve képesek valós idejű döntéstámogatást és hatékonyabb evakuációs tervezést biztosítani.

FELHASZNÁLT IRODALOM

[1] M. Balázs, „Lakossági óvóhelyek," in *Titkos bunkerek – A magyarországi óvóhelyek története 1917–2022*, szerk. M. Balázs, Budapest: Erdélyi Szalon Kiadó, 2023, pp. 51–62.

[2] Budapest Főváros Levéltára (BFL), HU-BFL XV.16.e.251/182, *Budapest székesfőváros nyilvános óvóhelyei: Budapest várostérképe a nyilvános óvóhelyek jelölésével*, szerző: Polgármesteri XIII. Ügyosztály, P. László és R. Pál, Budapest, 1944.

[3] J. Sajnovics, *Az európai kapitalista államok polgári védelme*. Budapest, Hungary: Polgári Védelem Országos Parancsnokság (PVOP Kiadása), 1967, pp. 3–9.

[4] M. Cronqvist, R. Farbøl, and C. Sylvest, Eds., **Cold War Civil Defence in Western Europe: Sociotechnical Imaginaries of Survival and Preparedness**. Cham, Switzerland: Palgrave Macmillan, 2021. doi: 10.1007/978-3-030-84281-9. [Online]. Available: https://doi.org/10.1007/978-3-030-84281-9

[5] *Tolna Megyei Népújság*, 1985. október, 35. évf., pp. 230–256. [Online]. Available: https://library.hungaricana.hu/hu/view/TolnaMegyeiNepujsag_1985_10/

[6] I. Berki, "A magyar polgári védelem történeti áttekintése," *RTF*, vol. XXIV, pp. 15–24,2014.[Online].Avalaible: https://epa.oszk.hu/02500/02511/00002/pdf/EPA02511_katonai_jogi_szemle_2014_01.pdf

[7] G. Schweickhardt, *A katasztrófavédelmi igazgatás rendszere, továbbfejlesztési lehetőségeinek vizsgálata*, Ph.D. dissertation, Katonai Műszaki Doktori Iskola, Nemzeti Közszolgálati Egyetem, Budapest, 2015. [Online] Available: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/schweickhardt_gotthilf.pdf

[8] S. Endre, *A magyar polgári védelem feladatai a VII. ötéves terv időszakában*, in *Honvédelem: a Magyar Néphadsereg Hadtudományi Folyóirata*, 3. különkiadás: *A polgári védelemről*, szerk. M. Berki, Budapest, 1986, pp. 19-29.

[9] Honvédelmi Miniszter, *A polgári védelmi szervezetek továbbfejlesztésének szabályai*, 9/1976. sz. intézkedés, PVOP Kiadása, Budapest, Hungary, 1976.

[10] Polgári Védelmi Országos Parancsnokság, *Módszertani útmutató az üzemi komplex polgári védelmi gyakorlat tervezésére és levezetésére*, PVOP, Nyt. sz. 31/279/1980, Budapest, 1980, pp. 15-23., 34–35.

[11] Fővárosi Csatornázási Művek Zrt., „Az árvízi védekezés fejlődése," FCSM. [Online]. Elérhető: https://www.fcsm.hu/szolgaltatasok/ar-es-belvizvedelem/az-arvizi-vedekezes-fejlodese

[12] J. Sajnovics, *Tansegédlet a kitelepítési és befogadási szakszolgálat általános kiképzéséhez*, PVOP Kiadása, Zrínyi Nyomda, Budapest, 1969, pp. 24–32.

[13] Dr. Bauer Frigyes (a hadtudományok kandidátusa) és Korondi Csaba mk. alezredes, „Automatizált vezetési rendszer a belkereskedelmi ágazat honvédelmi felkészülési munkájában," in *Honvédelem: a Magyar Néphadsereg Hadtudományi Folyóirata*, 3. különkiadás: *A polgári védelemről*, szerk. M. Berki, Budapest, 1986, pp. 144–152.

[14] W. Sun, P. Bocchini, and B. D. Davison, "Applications of artificial intelligence for disaster management," *Natural Hazards*, vol. 103, pp. 2631–2689, 2020. doi: 10.1007/s11069-020-04124-3.[Online].Available: https://ideas.repec.org/a/spr/nathaz/v103y2020i3d10.1007_s11069-020-04124-3.html
[15] FloodWaive Predictive Intelligence GmbH, "DeepWaive Flood Forecasting System," 2025. [Online]. Available: https://www.floodwaive.de/research
[16] Országos Vízügyi Főigazgatóság, "Órás idősor – vízállás és vízhozam adatok," *vizugy.hu*, [Online]. Available: https://www.vizugy.hu/?mapModule=OpGrafikon&AllomasVOA=16496059-97AB-11D4-BB62-00508BA24287&mapData=OrasIdosor
[17] *Országos Katasztrófavédelmi Főigazgatóság, Katasztrófavédelmi információs és döntéstámogató rendszerek*, [Online]. Available: https://www.katasztrofavedelem.hu/
[18] A. Takáts et al., „Drónos megfigyelések lehetőségei a katasztrófavédelem és tűzvédelem területén," in *XVII. Soproni Pénzügyi Napok konferenciakötet*, Soproni Egyetem Kiadó, 2023, pp. 72–93. [Online]. Available: https://doi.org/10.35511/978-963-334-495-8
[19] Siki Zoltán, *Gépi tanulás és mélytanulás a geodéziában / Machine Learning and Deep Learning in Land Surveying, XXV. Földmérő Találkozó, EMT – Erdélyi Magyar Műszaki Tudományos Társaság, gita Műszaki Térinformatika Egyesület, 2024.* [Online]. Available: *https://ojs.emt.ro/foldmero/article/view/1696/1746*

DOI: https://doi.org/10.12700/btsz.2026.8.2.15

THE EVOLUTION OF DOMOTICS SYSTEMS AND THEIR FUNCTION IN SMART BUILDINGS

A DOMOTIKA RENDSZEREK FEJLŐDÉSE ÉS SZEREPE AZ INTELLIGENS ÉPÜLETEK MŰKÖDÉSÉBEN

MÁRKOS Szilárd Attila[1] – KOLLÁR Csaba[2]

Abstract

The development of intelligent buildings has undergone significant transformation over the past two decades. In order to achieve comfort, energy-efficiency, and sustainability objectives, the most advanced technologies are increasingly being integrated into building operation systems. This study provides a systematic literature review of the technological development of domotics systems, their role in intelligent buildings, and their operational principles. The study presents the evolution of building automation from electromechanical control devices to systems supported by artificial intelligence. Furthermore, it discusses the role of IoT architectures, communication protocols, ESG/sustainability considerations, digital twin technology, edge computing, and cloud-based data processing. The study also addresses cybersecurity challenges and emphasizes the importance of user acceptance and organizational culture in the effective operation of intelligent buildings.

Keywords

Intelligent buildings, building automation, digital twin, IoT, edge computing

Absztrakt

Az intelligens épületek fejlődése az elmúlt két évtizedben jelentős átalakuláson ment keresztül. A komfort-, az energiahatékonysági és a fenntarthatósági célok elérése érdekében a legmodernebb technológiák épülnek be az épületüzemeltetésbe. A tanulmány a domotika rendszerek technológiai fejlődését, intelligens épületekben betöltött szerepét és működési alapelveit tekinti át szisztematikus irodalmi összefoglalás keretében. A tanulmány bemutatja az épületautomatizálás fejlődését az elektromechanikus vezérlőeszközöktől egészen a mesterséges intelligenciával támogatott rendszerekig, továbbá ismerteti az IoT-architektúrák, a kommunikációs protokollok, az ESG/fenntarthatósági szempontok, a digitális iker technológia, az edge computing és a felhőalapú adatfeldolgozás szerepét. A tanulmány külön kitér a kiberbiztonsági kihívásokra, továbbá hangsúlyozza a felhasználói elfogadás és a szervezeti kultúra szerepét az intelligens épületek hatékony működtetésében.

Kulcsszavak

Intelligens épületek, épületautomatizálás, digitális iker, IoT, edge computing

[1] markos.szilard@bgk.uni-obuda.hu | ORCID: 0009-0007-1044-6099 | university intern, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi gyakornok, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] kollar.csaba@uni-obuda.hu | ORCID: 0000-0002-0981-2385 | senior research fellow and leader, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Artificial Intelligence Workshop | tudományos főmunkatárs és vezető, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely

BEVEZETÉS

Az épületek vezérlési technológiája az elmúlt két évtizedben gyökeresen megváltozott. Ami korábban statikus infrastruktúra volt, az mára adatvezérelt, hálózatba kapcsolat rendszerré vált. A modern intelligens rendszerek működése egyre inkább arra épül, hogy az épület képes legyen alkalmazkodni a benne élők igényeihez és a környezet folyamatos változásaihoz. Ennek eredményeként a különböző gépészeti megoldások összehangoltabban működhetnek, miközben a rendszer előre reagálhat bizonyos helyzetekre a komfort és a hatékonyság fenntartása érdekében [1], [2].

Az Európai Unió statisztikái szerint a teljes energiafogyasztásának közel 40 százalékáért az épületállomány felel [3]. Ez a volumen önmagában is magyarázatot ad arra miért lett ez a terület stratégiai kérdés. Ez az arány olyan mértékű, amelyre politikai és gazdasági szabályozások épülnek: energiahatékonysági irányelvek, szén-dioxid-kvóták, kötelező felújítási programok. Ebben a kontextusban az intelligens épületüzemeltetés már nem csak a gazdaságos üzemeltetésről és a komfortról szól, hanem központi gazdasági és szabályozási szükségszerűség [4].

A fejlődés üteme figyelemre méltó. Két-három évtized alatt jutott el a terület az egyszerű időkapcsolóktól az önoptimalizáló, AI-vezérelt rendszerekig. Ma egy épületfelügyeleti platform nemcsak vezérel, hanem előre jelez, tanul és dönt [5]. Az IoT, a felhőalapú platformok és a gépi tanulás kombinációja olyan képességeket adott az épületüzemeltetésnek, amelyek korábban csak ipari folyamatirányításban léteztek [6], [7].

A domotika szerepe azon túl, hogy gazdaságosan üzemeltethető egy épület a felhasználói komfort, az üzemeltetési megbízhatóság, a hosszú távú ingatlanérték fenntartásában is kiemelt szerepet kap [2], [8]. Egy jól felépített rendszer átfogó irányítási stratégiát dolgoz ki és valósít meg.

Mindezzel együtt jár a kockázati profil megváltozása. Minél több érzékelő, vezérlő és hálózati eszköz kerül egy épületbe, annál nagyobb a potenciális kibertámadási felület [9], [10]. Egy HVAC-rendszer vagy beléptető infrastruktúra feltörése ma már nem csak adatvédelmi incidens, fizikai következményekkel is járhat. Az intelligens épületek, különösen közintézményi és ipari környezetben, fokozatosan a kritikus infrastruktúrák kategóriájába kerülnek, és ezt a szemléletet az üzemeltetési gyakorlatnak is követnie kell [11].

A tanulmány a domotika rendszerek fejlődését, technológiai alapjait és szerepét tekinti át az intelligens épületek kontextusában. A vizsgálat kiterjed a fejlődéstörténetre, technológiai felépítésre, energetikai és biztonsági vonatkozásokra, valamint a mesterséges intelligencia épületirányításban betöltött szerepére. A tanulmány a terület meghatározó szakirodalmának feldolgozására épül. A cél az, hogy az olvasó átfogó képet kapjon, hogyan jutottunk az analóg időkapcsolóktól az AI-alapú épületirányításig.

A DOMOTIKA FOGALMI ÉS TECHNOLÓGIAI ALAPJAI

A domotika nem egyszerű szinonimája az épületgépészeti vezérlésnek, hanem annál lényegesen tágabb fogalom. A hagyományos épületautomatizálás az épületgépészeti alrendszerek, elsősorban a fűtés, hűtés, szellőzés, világítás, árnyékolás és biztonságtechnika integrált automatizálása [1]. A modern domotika azonban ennél lényegesen több: az infor-

matikai, kommunikációs és fizikai infrastruktúrák összekapcsolt rendszere, amely adatvezérelt, önoptimalizáló működésre képes [1], [2]. Ez az átalakulás az elmúlt két évtized terméke és szorosan összefügg az IoT és a számítógépes fizikai rendszerek megjelenésével.

A szó a latin domus szóból ered, de ez az etimológia mára kissé szűknek bizonyult. A modern domotika rendszerek egy lakás, egy teljes irodaház, kórház vagy ipari létesítmény digitális idegrendszereként működnek: érzékelnek, feldolgoznak, következtetnek és beavatkoznak, valós időben, folyamatosan [1], [2].

Az épületek belső architektúrája is sokat változott. A korai domotika rendszerek erősen centralizáltak voltak. A centralizált vezérlési architektúrának jelentős sérülékenységet hordoztak, ha a központi egység meghibásodott, az egész rendszer leállt [4]. Ezt akkoriban elfogadható kompromisszumnak tartották. Azonban később, a kritikus infrastruktúrák szemléletének terjedésével egyértelművé vált, hogy ez túl nagy kitettséget jelent és ezt a rendszer tervezése során lehetőség szerint el kell kerülni. A mai intelligens épületekben osztott intelligencia működik: az alrendszerek önálló döntéshozatalra képes egységekként viselkednek, amelyek egymástól függetlenül bővíthetők és fejleszthetők.

Egy közepes irodaépületben ma már több száz érzékelő működik párhuzamosan: hőmérséklet, páratartalom, szén-dioxid-szint, mozgás, fényintenzitás, energiafogyasztás [2], [5]. Ezen adatfolyamokat használja fel a vezérlési logika, az előrejelző modellek és a döntéstámogatás segítésének érdekében.

Az aktuátorok végzik el a vezérlési utasítások fizikai végrehajtását: egy fűtési szelepet mozgat, egy lámpa kapcsol, egy árnyékolót mozgat. Itt találkozik a digitális és a fizikai világ.

A kommunikációs protokoll megválasztása az intelligens épület egyik legtartósabb következményű döntése. A KNX elosztott, eseményvezérelt felépítéssel főként lakó- és kiskereskedelmi épületekben terjedt el; a BACnet nyílt protokollként a kereskedelmi szegmens referenciaszabványává vált; a Modbus az ipari és energetikai alrendszereknél maradt releváns [3], [4], [12].(

A vezeték nélküli technológiák, a ZigBee, Z-Wave, Bluetooth Low Energy és a Matter, rugalmasabb telepítést és könnyebb bővíthetőséget kínálnak, de emelt biztonsági kockázattal. Az IoT elterjedésével az intelligens épület ma már nem egyetlen zárt rendszer, hanem heterogén eszközök és platformok összekapcsolt halmaza [2], [5]. Egyszerre jelenti azonban azt is, hogy a rendszer biztonsági szintjét a leggyengébb láncszem határozza meg.

A felhőalapú és az edge computing megközelítés jól kiegészíti egymást, és az egyensúly megtalálása az intelligens épület egyik legfontosabb tervezési kérdése. A felhő alapú erős hosszú távú elemzésnél, nagy adatvolumennél, összesített riportingnál [6]. Az edge computing ott nélkülözhetetlen, ahol a válaszidő valóban számít.

A modern domotika rendszerek tehát kiberfizikai rendszerekké váltak: olyan infrastruktúrává, ahol a fizikai tér és a digitális vezérlés szoros kölcsönhatásban működik [5], [6]. Ez az integráció hatékonyságot és alkalmazkodóképességet ad. Egyúttal azt is jelenti azonban, hogy egy digitális kompromittáció fizikai következményekkel járhat.

A DOMOTIKA RENDSZEREK FEJLŐDÉSTÖRTÉNETE

A korai automatizálási rendszerek

Az épületautomatizálás gyökerei az 1960-as-1970-es évtizedekbe nyúlnak vissza. A korai megoldások az elektromechanikus logikára épültek [1]. Mai szemmel nézve ezek egyszerű

eszközök voltak: időkapcsoló relék, hőfokszabályozók és analóg vezérlőegységek. De a maguk korában komoly lépést jelentettek azáltal, hogy lehetővé tették az épületüzemeltetés részleges automatizálhatóságát, ezzel sikerült az emberi beavatkozást részben kiváltani.

Az 1973-as olajválság indikátorként hatott az épületüzemeltetés fejlődésére. Az energiaárak drasztikus megugrása rávilágított arra, hogy az épületek pazarló üzemeltetése [2]. Ez a gazdasági kényszer valódi keresletet teremtett az automatizált energiafelügyelet iránt, amit addig inkább csak kényelmi szempontból szorgalmaztak. A korszak rendszerei egymástól elszigetelve működtek, melyek nem kommunikáltak egymással és nem voltak képesek alkalmazkodni a változó körülményekhez. Ezen rendszerek rugalmatlansága jelentősen korlátozta a működésük hatékonyságát.

Visszatekintve ezekre a korai rendszerekre, nehéz lenne intelligensnek nevezni, hiányzott belőlük az alkalmazkodóképesség és a hálózati integráció [1]. Kezdetlegességük ellenére kiemelt jelentőséggel bírnak a logikai alapok lefektetésében, ami a modern rendszerek alapját képezik elsősorban a HVAC szabályozás és az energiafelügyelet területén.

Az analóg szabályozók egyik paradoxona a statikus beállíthatóság, ami egyszerre erény és korlátozó tényező is. Megbízhatóak és könnyen üzemeltethetőek voltak, azonban mivel egy előre beállított logika alapján működtek, képtelenek voltak alkalmazkodni a környezeti változásokhoz [3]. Ez a rugalmatlanság olyan igényt teremtett, amelyet az analóg világ nem tudott kielégíteni.

A mikroprocesszoros korszak

Az 1980-as évek elején megjelent mikroprocesszorok valódi fejlődési ugrást jelentettek az épületautomatizálásban. Nemcsak gyorsabb volt az analóg logikánál, hanem programozható is: lehetett benne szabályokat tárolni, feltételeket kezelni, és idővel egyre összetettebb vezérlési logikát futtatni [4]. Az épületautomatizálás ekkor lépett ki az egyszerű időzítők és küszöbértékek szűk keretei közül.

Ebből a mikroprocesszoros alapból nőttek ki az első valódi épületmenedzsment-rendszerek. Ezek már arra is képesek voltak, amit korábban elképzelhetetlennek tartottak: egyetlen kezelőfelületen látni és vezérelni egy egész épület HVAC, világítás és energiamenedzsment rendszerét [5]. Az energetikai megtakarítások mérhetők lettek, a működés átláthatóbbá vált. Az optimalizálás szó azonban még nem volt helyénvaló, mert a rendszer csak azt csinálta, amire betanították.

A korszak egyik fontos eredménye a kommunikációs protokollok első generációjának megjelenése volt. Addig minden gyártó saját, zárt rendszerben gondolkodott. Az első protokollok ezt a falat kezdték lebontani: különböző gyártók eszközei elkezdtek egymással „kommunikálni" [6]. A kompatibilitás azonban korántsem volt teljes, és a különböző szabványok közötti feszültség évtizedeken át tartott.

Hálózatba kapcsolt intelligens rendszerek

A 2000-es évek elején az internet alapú kommunikáció egyszerre hozta el az intelligens épületek egyik legnagyobb lehetőségét és egyik legnagyobb kockázatát. Az internet megjelenése az épületautomatizálásban forradalmasította az integrációt: különböző alrendszerek össze tudtak kapcsolódni, adatot tudtak megosztani, és egy átfogó felügyeleti rendszerbe lehetett őket integrálni [7]. Ugyanakkor az addig fizikailag elszigetelt infrastruktúra nyitottá vált a világ felé és ezáltal kibertámadási kockázatot jelentett. Az épületautomatizálási szektor csak évekkel később kezdett el az ilyen veszélyek elhárításával komolyabban foglalkozni.

A KNX, a BACnet és a LonWorks ebben az időszakban váltak iparági szabvánnyá [8]. Az Ethernet megjelenése az épülethálózatokban növelte az adatátvitel kapacitását és az összekapcsolható eszközök számát. Egy valódi épületintegráció első generációja jött létre: a HVAC, a világítás, a biztonságtechnika és az energiafelügyelet közös adatbuszra kerülhetett.

Az integrált rendszerek egy olyan üzemeltetési modellt tettek lehetővé, amelyet korábban csak elméletben lehetett elképzelni: az épület különböző alrendszerei valós idejű adatokat cseréltek, és ezek alapján összehangoltan vezéreltek [7]. A monitoring és az automatizált szabályozás egymást erősítő elemmé vált. A korábban egymástól elszigetelt alrendszerek összekapcsolhatóvá váltak és egy komplex épület automatizálási rendszer részét képezték.

A hálózati integráció lehetővé tette az adatvezérelt épületmenedzsmentet, de olyan komplexitást is teremtett, amellyel a kor üzemeltetői nehezen boldogultak [8]. Vegyes protokollok, inkompatibilis platformok, integrációs problémák a mai napig problémát okoznak.

A kiberbiztonsági gondolkodás felismerése nem tartott lépést a technológiai fejlődéssel. Az épületüzemeltetők és tervezők fizikai infrastruktúrában gondolkodtak, amelynek biztonságát fizikai védelemmel biztosították. Az internetkapcsolat megjelenése teljesen megváltoztatta a fenyegetési modellt [9] amit a tervezési és üzemeltetési gyakorlat csak évekkel később követett le.

IoT és mesterséges intelligencia alapú korszak

Napjainkban az intelligens épületek fejlődése már egy teljesen új dimenzióba lépett. Az IoT, a felhőalapú adatfeldolgozás, a mesterséges intelligencia és a kiberfizikai rendszerek egymást erősítő konvergenciája olyan képességeket ad az épületüzemeltetési rendszereknek, amelyeknek korábban elképzelhetetlenek voltak [10]. A modern intelligens épület nem vezérel, hanem gondolkodik: mintázatokat ismer fel, döntéseket hoz, és tanul.

A leglátványosabb változás az optimalizálás fogalmában van. A statikus szabályozás végrehajtása helyett ma az optimalizálás az időjárás-előrejelzés, az aktuális energiaárak, a hálózati terhelés és a felhasználói szokások egyidejű figyelembevételét jelenti [13]. A rendszer nem reagál, hanem megelőz. A prediktív karbantartás, az alkalmazkodó vezérlés, az önoptimalizáló üzemeltetés, ma már az épületüzemeltetés szerves részét képezi.

Az IoT-korszak számos előnye mellett a korábbi biztonsági kockázatokat tovább fokozza. Minél több eszköz kapcsolódik a hálózathoz, annál több a potenciális belépési pont egy esetleges támadáshoz [14]. Az IoT-eszközök sokszor korlátozott biztonsági képességekkel érkeznek: gyenge hitelesítés, ritka frissítések, gyártói támogatás idő előtti megszűnése. A modern intelligens épületek, különösen közintézményi és ipari környezetben, ma már a kritikus infrastruktúrák biztonsági logikájával kezelendők [11].

A digitális iker és az edge computing technológiái szorosan kapcsolódnak ehhez a területhez, részletes bemutatásuk azonban az 5. fejezetben történik.

A DOMOTIKA RENDSZEREK SZEREPE AZ INTELLIGENS ÉPÜLETEK MŰKÖDÉSÉBEN

Energiahatékonyság és optimalizálás

Az intelligens épületek legkézzelfoghatóbb hozzáadott értéke az energiafelhasználás csökkentése, ami nem csak környezeti, hanem egyre erősebb gazdasági érdek. Az épületek a teljes energia fogyasztás jelentős részét teszik ki [1]. Egy jól üzemeltetett intelligens

épületautomatizálási rendszer ezt az arányt szignifikánsan csökkenteni tudja. A szén-dioxid-kvóták miatt ez a kérdés már nem csak a végfelhasználókat érinti, hanem egy komoly stratégiai érdek.

A HVAC-rendszerek az épületek energiafelhasználásának tipikusan a legnagyobb tételét teszik ki. Intelligens szabályozással ez lényegesen csökkenthető, az igények pontosabb előrejelzésével, figyeli a helységek foglaltsági mintáit, a külső időjárási tényezők aktuális és várható paramétereit és az aktuális energiaárakat [2]. A rendszer nem a jelenlegi hőmérsékletet kezeli, hanem modellezi, mire lesz szükség egy óra múlva, és már most megteszi a szükséges lépésket. A hőkomfort és az energiatakarékosság, amelyek sokáig egymásnak ellentmondó céloknak tűntek, így egyszerre valósítható meg.

A gépi tanulás megjelenése az energiamenedzsmentben jelentős előrelépést hozott. Az adatvezérelt rendszerek energiafogyasztási mintázatokat azonosítanak, és proaktívan módosítják az épület működését [3]. Az adatvezérelt megközelítés különösen nagy épületeknél hozza a legjelentősebb megtakarítási eredményeket, ahol a mintázatok komplexek és a megtakarítási potenciál nagy.

A világításvezérlés kevésbé látványos tétel, de az összkép szempontjából nem elhanyagolható. Jelenlétérzékelők, természetes fény mérése, automatizált fényerőszabályozás: ezek kombinációja nemcsak az energiafelhasználást csökkenti, hanem a vizuális komfortot is javítja [4], [15]. Irodaépületeknél, ahol a munkavállalói teljesítmény mérhető, ez az összefüggés közvetlenül gazdasági értékké fordítható.

Az árnyékolástechnika az egyik leginkább alulértékelt energetikai eszköz. A napenergia-bevitel megfelelő szabályozása egyszerre csökkenti a nyári hűtési csúcsokat és a téli fűtési igényt [5]. Nagy üvegfelületű épületeknél ez különösen kritikus dimenzió.

A megújuló energiaforrások integrációja az intelligens épületeket teljesen új szerepbe hozza. Az épület aktív energiapiaci szereplővé válik. A napelemes termelés, az akkumulátoros tárolás és az elektromos töltőinfrastruktúra koordinálása olyan feladat, amelyre hagyományos épület nem képes [6]. A smart grid-del összekötött intelligens épület alkalmazkodik a hálózati terheléshez, felesleges termelését visszaadja, és kedvező árakon tárol.

Komfort és felhasználói élmény

A modern rendszerek valóban képesek megtanulni a felhasználói szokásokat, és ehhez igazítani az üzemeltetési paramétereket [7]. Ez az alkalmazkodóképesség azonban nem korlátlan, a technológia nyújtotta lehetőségek és a felhasználói elvárások közötti eltérések olykor feszültséget eredményezhetnek.

A domotika rendszerek komfortfunkciói mára már jóval túlmutatnak az egyszerű hőmérséklet beálltáson, a hőkomfort nem egyenlő a hőmérséklettel. A páratartalom, a légáramlás, a sugárzó felületek és a szemközti fal hőmérséklete mind befolyásolja, hogy valaki melegnek vagy hidegnek érzi a teret [2]. Az intelligens HVAC-rendszerek ezeket a tényezőket egyszerre kezelik, és valós idejű visszajelzés alapján finomhangolnak. A kutatások ezt összefüggésbe hozzák a munkavállalói produktivitás mérhető javulásával is.

A levegőminőség-figyelés az utóbbi években felértékelődött, és ebben a COVID-19 járványnak komoly szerepe volt. A beltéri levegő minősége, a szén-dioxid-szint, az illékony vegyületek, a finom részecskék: ezek egészségügyi következményei korábban keveset szerepeltek az épülettervezési vitákban [8], [16]. A szakirodalom részletesen tárgyalja, hogyan integrálhatók az intelligens szellőztetési stratégiák a domotika rendszerekbe, és milyen

mértékben csökkenthető ezzel a felesleges energiaveszteség [16]. Az igény szerinti szellőztetés egyszerre egészségügyi és energetikai megoldás.

Az emberközpontú világításvezérlés a komforttechnológia egyik legkomplexebb területe. A napszakhoz igazodó, dinamikus fényvezérlés a látást segítésén túl, igazoltan befolyásolja a biológiai ritmust, a koncentrációt és a pszichológiai jóllétet [9]. Az optimalizálás itt nem fizikai paraméterekről szól elsősorban, hanem az emberi szervezet reakcióiról. Ez személyre szabottabb és árnyaltabb megközelítést igényel és jóval összetettebb, mint amit egy egyszerű fényerő-szabályozó biztosíthat

A mesterséges intelligencián alapuló alkalmazkodóképesség ígéretes, de nem problémamentes. Az intelligens rendszerek megtanulják a felhasználói szokásokat, és képesek erre alapozva döntéseket hozni [10]. Azonban a túlzott automatizálás csökkenti a felhasználók kontrollérzését, és elidegenedést kelthet. Az adatvédelmi kérdések, különösen a jelenlétérzékelés és a viselkedési adatok gyűjtése, szintén etikai mérlegelést igényelnek.

Biztonság és védelem

Az intelligens épületek biztonsági infrastruktúrája az elmúlt évtizedben teljesen átalakult. Ami korábban párhuzamos, egymástól független rendszerek halmaza volt, ma egyetlen integrált architektúrában működik: videómegfigyelés, beléptető rendszerek, mozgásérzékelés, tűzjelzés és digitális vezérlőrendszerek egyszerre [13]. Az integráció növeli a hatékonyságot, de a potenciális támadási felületet is.

Az integrált rendszerek egyik legnagyobb előnye valós idejű reagálóképesség. Automatizált vészhelyzeti protokollok, valós idejű riasztás, azonnali beavatkozás: ezek drasztikusan lerövidítik az időt, amely egy incidens azonosítása és kezelése között eltelik [17]. Tűzriasztásnál, jogosulatlan belépési kísérletnél vagy műszaki meghibásodásnál ez a reakcióidő biztonsági és vagyoni szempontból is kiemelt jelentőségű.

A mesterséges intelligencia a biztonsági alkalmazásokban, kiváltképpen az anomáliadetektálásban és a videóelemzésben, meghatározó fejlődést hozott. Az algoritmusok szokatlan eseményeket észlelnek, és figyelmeztetést adnak még azelőtt, hogy az incidens bekövetkezne [18]. Az emberi hibákból eredő kockázatok csökkentése ebben az összefüggésben különösen értékes.

A zero trust és a IoT-eszközök sérülékenysége is szorosan kapcsolódnak ehhez a területhez, részletes bemutatásuk azonban az 6.3 fejezetben történik.

A személyi kockázatok témakör szorosan kapcsolódik ehhez a területhez, részletes bemutatásuk azonban az 6.4 fejezetben történik.

Fenntarthatóság és ESG szempontok

A fenntarthatóság mára az intelligens épületek tervezésének megkerülhetetlen keretelemévé vált. Az ESG-szempontok beépülésével ez épületek energia fogyasztásának, és ezzel együtt a széndioxid lábnyomának csökkentése egyszerre befektetői, szabályozói cél. Az ESG-szempontok ingatlanpiaci hatása ma már mérhetően kimutatható. Egy rosszul minősített épület nehezebben adható bérbe, nehezebben hitelezik meg, és veszít az értékéből [19]. Ez azt jelenti, hogy az intelligens épülettechnológiákba való beruházás megtérülési kalkulációjában ma már nemcsak az energiaszámla szerepel.

A LEED, BREEAM és WELL minősítési rendszerek egyre pontosabban számszerűsítik az intelligens automatizálási megoldások hozzájárulását [20]. A minősítési szem-

pontrendszer az iparági elvárások fejlődését is alakítja, és ösztönzi a fejlesztőket, hogy korszerű domotika megoldásokat alkalmazzanak. A kedvező minősítés megszerzése az egyik leghatékonyabb eszköz, amellyel a szabályozói szándék a beruházói döntésekbe beépül.

Ugyanakkor a fenntarthatósági célok és a megvalósítás valósága között máig komoly szakadék tátong. Magas beruházási költségek, interoperabilitási hiányosságok, technológiai avulás: ezek különösen a meglévő épületállomány esetén valódi akadályok [19]. A fenntarthatóság, mint cél és a megvalósítás közötti feszültség az intelligens épületek fenntarthatósági ambícióinak egyik megoldatlan kihívása.

MESTERSÉGES INTELLIGENCIA ÉS ADATVEZÉRELT ÉPÜLETIRÁNYÍTÁS

A HVAC-rendszerek energiaoptimalizálása az a terület, ahol az AI a legmarkánsabb eredményeket produkálja. A gépi tanulási algoritmusok az aktuális hőmérséklet monitorozása mellett az épület teljes energiafelhasználási profilját is elemzik, a felhasználói szokásokat, az időjárási előrejelzéseket, az energiaárak napi változásait [2]. Ennek alapján mindig egy lépéssel a bekövetkező esemény előtt járnak és meg tudják indítani a megelőző intézkedéseiket. Ez a különbség a hagyományos termosztát és egy valódi intelligens rendszer között.

A prediktív vezérlés lényege a megelőzés, amíg a hagyományos rendszer a már bekövetkezett változásra válaszol, az előrejelző algoritmus a várható változást modellezi, és megelőző lépést tesz [3]. A fogyasztási csúcsok csökkentése és az energiaelosztás optimalizálása nemcsak az épület hatékony működése miatt fontos, hanem a villamosenergia hálózat terhelésének kiegyensúlyozásában is egyre nagyobb szerepet kap, különösen a smart grid rendszerek terjedésével.

A prediktív karbantartás az AI alkalmazások egyik leginkább alulértékelt területe. A szenzorhálózatokból érkező adatfolyamok elemzésével az algoritmusok képesek azonosítani a meghibásodások korai jeleit, sokszor hetekkel azelőtt, hogy a probléma láthatóvá válna [4]. A megelőző karbantartás ezt a kockázatot érdemben csökkenti.

Az anomáliadetektálás az a pont, ahol az energetikai és a kiberbiztonság találkozik. A normál működési mintáktól eltérő energiafogyasztás, szokatlan hálózati forgalom vagy gyanús hozzáférési kísérlet egyaránt utalhat rendellenes működésre [5].

A digitális iker technológia talán a legösszetettebb és egyben a legtöbb potenciállal rendelkező terület. Az épület valós idejű virtuális modellje lehetővé teszi, hogy különböző beavatkozásokat teszteljünk anélkül, hogy az éles rendszerben kísérleteznénk [6]. Energiaoptimalizálási változtatásokat, karbantartási forgatókönyveket, szélsőséges üzemi helyzeteket lehet szimulálni, és a várható hatásokat megvizsgálni egy virtuális térben [18]. Ez az üzemeltetési kockázatkezelés egy teljesen új szintje.

A felhőalapú feldolgozás erős centralizált elemzésnél, de ahol alacsony válaszidő kritikus, például a vészhelyzeti rendszereknél, a helyi adatfeldolgozás nem lehet mással kiváltani [7] [17]. Az edge computing adatvédelmi szempontból is előnyösebb mint a felhő alapú adatfeldolgozás, így az üzemeltetés közben gyűjtött érzékeny adatok nem hagyják el a helyszínt.

Az önoptimalizáló épületek hatékonyságot és kényelmet biztosítanak [8], de az üzemeltetői kompetencia és a beavatkozási képesség megőrzése tudatos tervezési döntést igényel. Amit a rendszer automatikusan kezel, azt az ember fokozatosan elfelejti kezelni. Ez hosszú távon üzemeltetési sebezhetőséget is teremthet.

A gépi tanulási modellek döntéshozatalának átláthatósága, különösen mélyebb neurális hálózatok esetén, nem tekinthető evidensnek [9]. A modellek megbízhatósága változó üzemi körülmények között ingadozhat, és fennáll a veszélye annak, hogy kiberbiztonsági támadás célpontjává váljon.

KIHÍVÁSOK ÉS KORLÁTOK

Interoperabilitási problémák

Az épületautomatizálás korai éveiben gondot okozott, hogy különböző gyártók eszközei egyáltalán nem tudtak egymással kommunikálni [1]. A különböző gyártók eltérő protokolokat és vezérlési logikákat alkalmaztak, ami a mai napig kompatibilitási problémákat okazhatnak. A nagyobb platformok rendkívül szigorú feltételeket szabnak és csak az ennek megfelelő kompatibilis eszközök kapják meg az adott rendszer minősítését. Az iparágak korai szabvány választása a mai napig meghatározzák az egyes területek milyen rendszerre építenek. Ezért egy központi platformon működő rendszer átjáró kapukon keresztül kommunikáló alplatformokat fog össze. Például a világítási rendszerek tradicionálisan Dali szabványra épülnek a HVAC rendszerek modbus rendszerűek, a központi rendszer pedig KNX.

A KNX, a BACnet és a Modbus megjelenése az iparági egységesedés felé tett lépés volt, de a valóság ennél szövevényesebb. A gyártók saját kiterjesztéseket fejlesztenek, zárt platformokat tartanak fenn, és az integrációs munkát végül az üzemeltetőre hárítják [2], [3].

A vendor lock-in jelenség ebből következik és hosszútávon a legnagyobb kockázatot jelenti. Ha egy épület üzemeltetési rendszere egyetlen gyártó ökoszisztémájára épül, az üzemeltető elveszíti a szabad bővítés lehetőségét, és beszorul az adott keretrendszer határai közé [4]. Minden frissítés, minden bővítés, minden javítás ugyanattól a szállítótól érkezik, annak feltételei és árazása alapján. Ez a kötöttség különösen hosszú üzemeltetési ciklussal rendelkező épületek esetén lehet kockázatos.

A felhőalapú és edge architektúrák elterjedése egy újabb dimenzióval bővítette a kompatibilitási problémákat. Az eltérő adatkezelési modellek, programozási interfészek és kommunikációs protokollok az amúgy is heterogén épületmenedzsment-környezetet tovább bonyolítják [5]. Az iparág konszenzusa szerint a nyílt szabványok és az interoperábilis architektúrák felé kell haladni, azonban a megvalósítás üteme mégis messze elmarad az elvárásoktól.

Gazdasági korlátok

A domotika rendszerek szélesebb körű terjedését a kezdeti viszonylag magas beruházás korlátozza. A telepítési költségek, különösen meglévő épületek esetén, valóban számottevők [6]. Egy retrofit épület elektromos hálózata, csőrendszere, épületgépészete sokszor nem kompatibilis azzal, amit egy modern domotika rendszer megkövetel [8]. A megtérülési idő tipikusan meghaladja azt a horizontot, amelyen belül egy egyszeri döntéshozó gondolkodik. Közintézményi és önkormányzati környezetben ez az megtérülési időtáv visszafogott adoptációt okoz.

A megtérülési számítás önmagában is komplex feladat. Az energiaárak változékonysága, a kihasználtsági minták, a karbantartási igény és a rendszer várható élettartama mind befolyásolják a megtérülési időt [7]. Bizonytalan energiaárak alakulása és a hosszú

megtérülési idő mellett a kockázatkerülő szervezetek beruházási hajlandósága kifejezetten alacsony.

A technológiai avulás az a kockázat, amelyet a beruházási kalkulációkban a legtöbbször figyelmen kívül hagynak. Szoftverfrissítési igények, új biztonsági szabványok, hardveres kompatibilitási problémák, ezek folyamatos fenntartási költségeket termelnek [9]. Moduláris, nyílt felépítéssel ez mérsékelhető, de nem szüntethető meg teljesen. Egy épület harminc évig üzemel, de a mögötte lévő technológia öt-tíz évenként generációt vált, amivel érdemes lépést tartani.

Az ESG-elvárások intézményesülése, az energiaárak tartós emelkedése és a fenntarthatósági minősítések ingatlanpiaci hatása együttesen olyan nyomást teremt, amely fokozatosan átírja a kalkuláció megtérülési idejét [10]. Ami ma hosszú megtérülési időnek tűnik, holnap versenyképességi kérdéssé válhat.

Kiberbiztonsági kockázatok

Az intelligens épületek kiberbiztonsági helyzete az internetkapcsolat megjelenésével teljesen megváltozott. Az épületüzemeltetési infrastruktúra korábban fizikailag elszigetelt volt, és ebből adódóan nem volt kitéve külső támadásoknak [13]. A rendszerek elérhetők a hálózatról, és ezzel együtt sebezhetővé is váltak. Ezek a támadások az adatlopás mellett fizikai károkat is okozhatnak a berendezésekben.

A sérülékenységek spektruma széles és jól ismert: nem megfelelő hitelesítés, elavult szoftverek, titkosítatlan kommunikáció, gyártóspecifikus kiskapuk [17]. Az intelligens épületek különösen vonzó célpontok zsarolóvírusos támadásokhoz, mert az üzemfolytonosság kényszere gyors döntést kényszerít ki. Egy kórháznál vagy adatközpontnál ez a nyomás óriási, és a támadók ezt használják ki.

A fizikai és a digitális infrastruktúra integrációjából fakadó kockázat az, ami az intelligens épületek kiberbiztonságát veszélyezteti. Egy HVAC-rendszer manipulációja egészségügyi következményekkel járhat. Egy tűzjelzési rendszer feltörése emberéleteket veszélyeztethet. Egy beléptető rendszer kompromittálása fizikai behatolást tesz lehetővé [18]. Ez nem informatikai probléma, amelyet az IT-részleg kezel: épületbiztonsági probléma, amelynek digitális forrása van. Ez megköveteli, hogy a kiberbiztonság együtt kezelje az informatikai veszélyeket az épületbiztonsági kérdésekkel.

Az IoT-eszközök biztonsági gyengesége legtöbbször az eszközök felépítéséből és a természetéből fakad. Korlátozott számítási kapacitás, hosszú frissítési ciklus, gyártói támogatás idő előtti megszűnése, ezeken szoftverfrissítéssel nem lehet változtatni [14]. Egy épületben évtizedekig működő, vegyes korú és gyártójú eszközpark egységes biztonsági keretbe szervezése elsősorban hálózati architektúra kérdése. Szegmentálás, zero trust megközelítéssel és folyamatos monitorozással lehet a helyzetet a legjobban kezelni. A módszertan jól ismert: titkosítás, többfaktoros azonosítás, hálózati szegmentálás, rendszeres frissítések, anomáliadetektálás [21]. A zero trust architektúra szemlélete megjelent az épületüzemeltetési kontextusban is, amely nem feltételez megbízhatóságot egyetlen hálózati szereplővel szemben sem, és minden hozzáférési kérelmet hitelesít.

A kiberbiztonság tehát nem informatikai kérdés, hanem az intelligens épületek üzemeltetésének legkritikusabb területe [13], [21]. Az épületüzemeltetőknek olyan kompetenciákat kell fejleszteniük, amelyek korábban nem tartoztak a munkájukhoz. A kulturális és

szervezeti változás mindig lassabb, mint a technológiai fejlődés. Ez az eltérés ma az egyik legnagyobb biztonsági rés.

Humán tényezők

Az intelligens épületek biztonsági szintje nem csupán technológiai kérdés, hanem szervezeti kockázatokat is jelent. A gyártóspecifikus zárt platformok, a heterogén IoT-környezetek és az egységes szabványok hiánya olyan komplexitást teremtenek, amellyel a legtöbb üzemeltető nehezen birkózik meg [14], [21]. A biztonsági kultúra és a szervezeti felkészültség sokszor fontosabb, mint az alkalmazott technológia. A legfejlettebb automatizálási rendszer sem működik jól, ha a felhasználó nem tudja kezelni, nem érti a működését és ezáltal bizalmatlan a rendszer megfelelő működésével kapcsolatban és kerüli a használatát. Tehát az elfogadás éppúgy befolyásolja a software ergonómiája, mint a technológia megbízhatósága. A tervezés során az ember-gép interakcióra kiemelt figyelmet kell fordítani [22]

A túlzott komplexitás az intelligens rendszerek egyik leggyakoribb gyengesége. Nehezen áttekinthető felületek, átláthatatlan vezérlési logikák, érthetetlen visszajelzések: ezek nem esztétikai hibák, hanem üzemeltetési kockázatok [19]. Azok a rendszerek, a melyek csak teszik a dolgukat és nem jeleznek vissza a felhasználónak mit miért csinálnak alacsonyabb elfogadottsági mutatókkal rendelkeznek [23].

A digitális kompetenciák hiánya különösen közintézményi és lakossági környezetben okoznak gondot [20]. Az összetett domotika rendszerek kezelése tudást feltételez, ami sokszor nem áll rendelkezésre. A nem megfelelően beállított vagy elhanyagolt rendszer nemcsak rosszul működik, hanem sebezhető is.

Az adatvédelmi kérdéseket nem lehet technikai problémaként kezelni. A jelenlétérzékelés, a viselkedési minták rögzítése, az energiafogyasztási adatok tárolása: ezek GDPR-kérdések és etikai kérdések egyszerre. Az a döntés, hogy egy épületrendszer milyen adatokat gyűjt, túlmutat a mérnök hatáskörén [24].

Az intelligens épületek hosszú távú fenntarthatóságát nem kizárólag a technológiai fejlettség határozza meg, hanem az is, hogy a felhasználók mennyire képesek és hajlandók együttműködni ezekkel a rendszerekkel. A felhasználóbarát kezelőfelületek, a rugalmas működési logika és a megelőzésközpontú adatvédelmi szemlélet mellett ezért kiemelt jelentőségű az emberi elfogadás és a támogató szervezeti kultúra, mivel ezek alapvetően befolyásolják a rendszerek hatékony és fenntartható működését.

KÖVETKEZTETÉSEK

A domotika rendszerek az elmúlt hat évtizedben hatalmas fejlődésen mentek keresztül, az egyszerű elektromechanikus automatizálástól egészen az adatvezérelt, gépi tanuláson alapuló önoptimalizáló mesterséges intelligenciával támogatott rendszerekig. Ez a folyamat jól tükrözi a technológiai lehetőségek folyamatos bővülését és a társadalmi elvárások változását. A technológia alapjaiban íta át az ember-gép interakciót. A domotika rendszerek ma már az intelligens épületek idegrendszerét alkotják.

Az energiahatékonyság, a felhasználói komfort, a fenntarthatóság és a biztonság korábban egymástól független területek voltak, amelyeket külön rendszerek kezeltek. Ma ezek egyetlen, integrált infrastruktúrában találkoznak [1], [2]. Ez az összevonás rengeteg

lehetőséget teremt, de komoly felelősséget is: egy rosszul tervezett vagy elhanyagoltan üzemeltetett intelligens rendszer nemcsak hatékonyságveszteséget okoz, hanem biztonsági kockázatot is jelent.

A mesterséges intelligencia, az IoT, az edge computing és a digitális iker technológiák összefonódása alapvetően átírja, mit értünk optimalizálás alatt [3]. Ahogy a rendszerek egyre önállóbbak lesznek, a felülbírálati és beavatkozási képesség megőrzése egyre fontosabb kérdéssé válik [4]. A felhasználónak ebben a folyamatban nem szabad passzív megfigyelővé válnia.

Az összekapcsoltság megnöveli a kiberbiztonsági fenyegetettséget, azáltal, hogy a rendszer nyitott a külvilág felé, és a sebezhetőség több fronton is megnyílik. Egyetlen kompromittált IoT-eszköz komoly rendszerszintű következményekkel járhat, és mivel a digitális és fizikai rétegek egymásba fonódnak, a támadások fizikailag károkat is képesek tenni a rendszerben [5]. A kiberbiztonsági szemlélet beépítése az épületüzemeltetésbe ezért ma már szükséges alapkövetelmény. Az interoperabilitás, a zero trust elvek következetes alkalmazása és a nyílt szabványok előnyben részesítése együttesen teremtik meg azt az alapot, amelyre megbízható rendszerek építhetők [6].

Az ESG-szempontok térnyerése az intelligens épületek gazdasági megítélését is megváltoztatta. Az energiafelhasználás, a szén-dioxid-kibocsátás és a minősítési pontszámok ma már közvetlenül hatnak az ingatlan értékére és finanszírozhatóságára [7]. A domotika rendszerek tehát egy épület hosszú távú értékét meghatározó infrastrukturális feltétel.

Az intelligens épületek fejlődése nem ér véget. A következő évek valószínűleg tovább mélyítik az autonóm működést, és egyre több döntés kerül az algoritmusok hatókörébe. Hogy ez valóban jobb épületeket jelent-e, az nem csupán technológiai kérdés: függ az üzemeltetési kultúrától, a szabályozási környezettől és attól, hogy a tervezők és fejlesztők mennyire veszik komolyan az emberi tényezőt. A domotika rendszerek önmagukban csak eszközök. Hogy mire használják őket, az rajtunk múlik.

FELHASZNÁLT IRODALOM

[1] A. H. Buckman, M. Mayfield, and S. B. M. Beck, “What is a smart building?,” Smart and Sustainable Built Environment (2014) 3 (2): 92–109. doi:10.1108/SASBE-01-2014-0003

[2] A. I. Dounis and C. Caraiscos, “Advanced control systems engineering for energy and comfort management in a building environment—A review,” Renewable and Sustainable Energy Reviews, vol. 13, no. 6–7, pp. 1246–1261, 2009. doi: 10.1016/j.rser.2008.09.015.

[3] United Nations Environment Programme, 2022 Global Status Report for Buildings and Construction, Nairobi, Kenya, 2022. [Online]. Available: https://globalabc.org/resources/publications/2022-global-status-report-buildings-and-construction (letöltve: 2026.01.02.)

[4] S. Wang, Intelligent Buildings and Building Automation. London, U.K.: Spon Press, 2010.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013. doi: 10.1016/j.future.2013.01.010.

[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016. doi: 10.1109/JIOT.2016.2579198.
[7] Y. Pan and L. Zhang, "Roles of artificial intelligence in construction engineering and management: A critical review and future trends," Automation in Construction, vol. 122, 2021, Art. no. 103517. doi: 10.1016/j.autcon.2020.103517.
[8] D. Clements-Croome, Intelligent Buildings: Design, Management and Operation. London, U.K.: ICE Publishing, 2013.
[9] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017. doi: 10.1109/JIOT.2017.2703172.
[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015. doi: 10.1016/j.comnet.2014.11.008.
[11] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," International Journal of Critical Infrastructure Protection, vol. 8, pp. 53–66, 2015. doi: 10.1016/j.ijcip.2014.12.002.
[12] Cs. Kollár, „A biztonság fontosabb fogalmai," Biztonságtudományi Szemle, vol. 7, no. 1, pp. 15–23, 2025. doi: 10.12700/btsz.2025.7.1.15
[13] ISO/IEC 14543-3, Information Technology — Home Electronic System (HES) Architecture — Part 3: Communication Layers — KNX Net/IP, International Organization for Standardization, Geneva, Switzerland.
[14] W. Bolton, Programmable Logic Controllers, 6th ed. Oxford, U.K.: Newnes, 2015.
[15] C. E. Ochoa, M. B. C. Aries, and J. L. M. Hensen, "State of the art in lighting simulation for building science: A literature review," Journal of Building Performance Simulation, vol. 5, no. 4, pp. 209–233, 2012. doi: 10.1080/19401493.2011.558211.
[16] Sz. Márkos, "Intelligens szellőztetési stratégiák a domotika rendszerben," Biztonságtudományi Szemle, vol. 7, no. 4, pp. 41–55, 2025. doi: 10.12700/btsz.2025.7.4.41
[17] ASHRAE Standard 135-2020, BACnet—A Data Communication Protocol for Building Automation and Control Networks. Atlanta, GA, USA: ASHRAE, 2020.
[18] L. Pérez-Lombard, J. Ortiz, and C. Pout, "A review on buildings energy consumption information," Energy and Buildings, vol. 40, no. 3, pp. 394–398, 2008. doi: 10.1016/j.enbuild.2007.03.007.
[19] C. Boje, A. Guerriero, S. Kubicki, and Y. Rezgui, "Towards a semantic Construction Digital Twin: Directions for future research," Automation in Construction, vol. 114, 2020, Art. no. 103179. doi: 10.1016/j.autcon.2020.103179.
[20] A. Pandharipande and D. Caicedo, "Daylight integrated illumination control of LED systems based on enhanced presence sensing," Energy and Buildings, vol. 43, no. 4, pp. 944–950, 2011. doi: 10.1016/j.enbuild.2010.12.018.
[21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, National Institute of Standards and Technology, Gaithersburg, MD, USA: NIST Special Publication 800-207, 2020. doi: 10.6028/NIST.SP.800-207
[22] Cs. Kollár, „A biztonság megjelenése a humán tudományokban (3. rész)," Biztonságtudományi Szemle, vol. 6, no. 4, pp. 1–14, 2024. [Online]. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/524 (letöltve: 2026.02.14.)

[23] Cs. Kollár, „A biztonság megjelenése a humán tudományokban (2. rész)," Biztonságtudományi Szemle, vol. 6, no. 3, pp. 1–12, 2024. [Online]. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/504 (letöltve: 2026.02.14.)
[24] Cs. Kollár, „A biztonság megjelenése a humán tudományokban (1. rész)," Biztonságtudományi Szemle, vol. 6, no. 2, pp. 13–22, 2024. [Online]. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/464 (letöltve: 2026.02.14.)

DOI: https://doi.org/10.12700/btsz.2026.8.2.29

RISK ANALYSIS OF ELECTROTHERAPY TREATMENT FOR PATIENTS UNABLE TO PROVIDE FEEDBACK

VISSZAJELZÉSRE KÉPTELEN PÁCIENSEK ELEKTROTERÁPIÁS KEZELÉSÉNEK KOCKÁZATELEMZÉSE

MORVAY László[1] – SZŰCS Endre[2]

Abstract

Electrotherapy is a widely used, non-invasive physiotherapy method for pain relief, muscle and nerve stimulation, and inflammation reduction. Despite its benefits, it can be risky for those who are unable to provide feedback during treatment. The aim of the study was to identify, analyse, and develop measures to reduce the risks for this vulnerable group. We analysed the treatment protocol, current and pulse parameters, biophysical and histological characteristics, as well as the design and use of electrodes. Based on the reviewed literature and two decades of professional experience, the greatest dangers are thermal injury, abnormal muscle contraction, and infection, particularly in patients who are unconscious, sedated, or suffering from peripheral nerve damage. The risks were classified and ranked using an Ishikawa diagram and a risk matrix. As a result, recommendations were made regarding the management protocol, patient care, training, equipment supervision, infection control, fire safety, and data protection. The targeted measures reduced high and medium risks to a low or minimal level.

Keywords

electrotherapy, lack of feedback, risk assessment, patient safety, risk mitigation

Absztrakt

Az elektroterápia nem invazív fizioterápiás kezelési mód fájdalomcsillapításra, izom- és idegstimulációra és gyulladáscsökkentésre. Előnyei mellett kockázatos lehet azoknál, akik kezelés közben nem tudnak visszajelzést adni. A kutatásunk célja e sérülékeny csoport kockázatainak azonosítása, elemzése és a feltárt kockázatok csökkentésére vonatkozó intézkedések kidolgozása volt. Elemeztük a kezelési protokollt, az áram- és impulzusparamétereket, a biofizikai és szövettani jellemzőket, valamint az elektródák kialakítását és használatát. A szakirodalom és a két évtizedes szakmai tapasztalat alapján a legnagyobb veszélyt a termikus sérülés, a kóros izomkontrakció és a fertőzés jelenti, különösen eszméletlen, szedált vagy perifériás idegkárosodásban szenvedőknél. A kockázatokat Ishikawa-diagrammal és kockázati mátrixszal osztályoztuk, rangsoroltuk. Eredményként ajánlások készültek a kezelési protokollra, képzésre, eszközfelügyeletre, infekciókontrollra, tűzbiztonságra és adatvédelemre. A célzott intézkedések a magas és közepes kockázatokat alacsony vagy minimális szintre mérsékelték.

Kulcsszavak

elektroterápia, visszajelzés hiánya, kockázatértékelés, betegbiztonság, kockázatcsökkentés

[1] morvay.laszlo@phd.uni-obuda.hu | ORCID: 0009-0004-2064-8856 | doctoral student, Óbudai University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X | senior lecturer, Óbudai University Doctoral School on Safety and Security Sciences | egyetemi oktató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

HIGHLIGHTS

- Risk of electrotherapy were mapped for patients unable to give feedback.
- Treatment failure emerged as the highest-priority hazard.
- Skin and muscle damage were identified as clinically relevant risks.
- Targeted risk controls reduced all hazards to low or minimal levels.
- Standardised safety guidance is needed for this vulnerable group.

INTRODUCTION

Electrotherapy is a widely applied modality in physiotherapy, utilising electrical currents to alleviate pain, stimulate muscles and nerves, and promote tissue regeneration. Its clinical relevance is largely attributable to its non-invasive nature and its capacity to complement pharmacological treatments. The currents triggered by the millivolt and microvolt level voltages used during the treatment exert a gentle and controlled effect on the cells, minimizing the risk of damage. By modulating cellular activity, electrotherapy enhances metabolic processes, improves oxygen and nutrient uptake, and facilitates tissue repair. The patient's mobility improves; increased blood flow and nutrient supply accelerate tissue regeneration and reduce inflammation. In addition, electrically induced muscle contractions may help prevent disuse atrophy associated with prolonged inactivity. [1]

The importance of electrotherapy in rehabilitation is further underscored by the high incidence of injuries particularly in combat actions and sports. According to data from the Rugby Football Union (RFU) in England, during the twenty seasons examined between 2002 and 2023, a total of 13,193 male professional rugby players sustained injuries during matches, which averages to 660 injuries per season. [2] According to the International Ski Federation (FIS), between the 2006 and 2019 seasons, a total of 3,950 injuries occurred, which averages to 790 injuries per year. [3] Hospitalisation data related to musculoskeletal and connective tissue disorders demonstrate a considerable and variable burden on healthcare systems across Europe. In 2021, Austria had the highest number of discharges following musculoskeletal diseases, with 2,403 discharges per 100,000 inhabitants. On the other hand, the same figure was the lowest in Malta, with fewer than 300 per 100,000 inhabitants. A discharge occurs when a patient leaves the hospital due to the completion of treatment, leaves against medical advice, is transferred to another healthcare facility, or passes away. [4]

Despite its therapeutic advantages, electrotherapy is not without risk. The application of electrical currents to biological tissues may induce thermal, chemical, and physiological effects, which, under inappropriate conditions, can result in adverse outcomes such as burns, tissue damage, or excessive muscle contraction. [1] According to a finite element (FEM: Finite Element Method) bioheat-technical model, with a flat electrode, the peak temperature of the skin tissue can reach up to 51.6 °C, which can already cause tissue damage. Heat generation at the electrode–skin interface, influenced by factors such as electrode design, current intensity, and environmental conditions, represents a particularly important risk factor. [5] In addition, inappropriate stimulation parameters may lead to pathological neuromuscular responses or, in extreme cases, tissue necrosis. According to research, alternating current of 30 milliampere or direct current of 150 milliampere passing through the human body already poses a health risk. [6] Environmental temperature and humidity affect

the skin's conductivity and heat regulation, which means these two parameters also influence heat generation during electrotherapy. According to a numerical model, an increase of 4 °C in environmental temperature raises the voltage experienced by neural tissues at the boundary of the epidermis (outer layer) and dermis (inner layer) by about 0.8 Volt, while a 12.5% rise in relative humidity increases it by approximately 1 Volt. Therefore, in a warm, humid environment, the skin's resistance decreases, allowing the current to penetrate deeper into the body, which increases the amount of heat generated. [7]

The muscle contractions that occur during electrotherapy can be traced back to two main causes. The treatment stimulates the peripheral nerves, which triggers the activation of motor neurons, resulting in muscle contraction. [8] In addition, the electric current also affects the spinal cord, modulating the activity of the central nervous system, which causes increased spontaneous muscle contractions. [9] The extent of these responses is strongly dependent on treatment parameters, including frequency, current intensity, and duration. Higher frequencies (e.g., 100 Hz) trigger more intense contractions, while low-frequency (e.g., 5 Hz) TENS (Transcutaneous Electrical Nerve Stimulation) can also enhance muscle activity, but requires longer treatment duration. A longer treatment duration (from 20 minutes to 1 hour) results in increased muscle activity. [10]

In routine clinical practice, the safe application of electrotherapy relies heavily on patient feedback, which allows the therapist to adjust treatment parameters in real time. However, there exists a clinically significant subgroup of patients who are unable to provide such feedback. Loss of consciousness in patients with severe injuries is most often a result of cranial trauma, hypovolemic shock (significant blood loss), or hypoxia (lack of oxygen). Due to the temporary or permanent loss of brain functions, the patient is unable to process sensory stimuli and respond motorically. [11] Confused states can be the result of diffuse brain damage, anoxia (cessation of oxygen supply), or metabolic disorders. Due to dysfunction of the cerebral cortex and the reticular (neuron network) activating system, the patient does not perceive peripheral sensory stimuli. [12] Sedative (tranquilizing or anaesthetic) and analgesic (pain-relieving) drugs commonly used in intensive care (e.g., midazolam, propofol, fentanyl) significantly reduce consciousness and sensation. Additionally, changes in blood circulation and skin temperature can distort the sense of heat, so there is an increased risk of burns during electrical stimulation. [13] The nervous system of infants is not yet fully developed. Although the nociceptive (sensory nerve) pathways are functioning, due to the lack of cognitive processing and communication abilities, the therapist do not receive reliable feedback about excessive stimulus intensity. [14] In severe forms of disorders, like intellectual, perceptional, or attentional, communication is simultaneously or individually limited. Such patients are often unable to accurately localize or interpret thermal and pain stimuli. [15] Due to damage to the peripheral nerves, patients have reduced or absent heat and pain sensation. This is because the small-diameter C and A-delta fibres that transmit heat and pain degenerate. [16]

Given these considerations, there is a clear need for a structured and systematic approach to risk identification and management in electrotherapy, specifically tailored to patients who are unable to provide feedback. The aim of this study is therefore to identify and analyse the risks associated with this vulnerable patient population, and to develop evidence-based recommendations to enhance treatment safety.

METHODS

It was hypothesised that the reduction of risks identified within the electrotherapy treatment protocol would significantly enhance the safety of patients unable to provide feedback, while maintaining therapeutic effectiveness.

As an initial step, the individual stages of the electrotherapy treatment process were systematically identified and arranged in chronological order. Potential patients were categorised into three groups: (i) outpatients capable of providing feedback, (ii) outpatients unable to provide feedback, and (iii) unconscious inpatients unable to provide feedback. (The resulting process flow is presented in Figure 1.) The subsequent risk analysis focused specifically on patients unable to provide feedback.

A detailed risk analysis was conducted in accordance with the principles outlined in Chapter 6 of ISO 31000:2018, Risk Management - Guidelines. [17] Relevant standards and regulatory frameworks applicable in the United States, the United Kingdom, and the European Union were also taken into consideration.

Potential hazards were identified based on the defined therapeutic protocol and systematically assigned to the individual steps of the treatment process. This enabled the compilation of a comprehensive hazard inventory (Table 3.) Subsequently, the possible causes associated with each identified hazard were analysed. In cases where multiple contributing factors were identified, emphasis was placed on determining the underlying root causes (Table 4). Following hazard identification and causal analysis, a structured hazard evaluation was performed. Cause–effect relationships were visualised using an Ishikawa (fishbone) diagram (Figure 2), which provided a conceptual framework for the subsequent risk assessment. Risk assessment was carried out using a risk matrix incorporating both the severity of potential consequences and the likelihood of occurrence. Hazard severity was classified into four categories: catastrophic, critical, minor, negligible. The probability of occurrence was categorised as frequent, probable, occasional, rare, or unlikely. Based on these parameters, overall risk levels were defined as high, medium, low, or minimal, drawing on both established risk assessment principles and practical experience in electrotherapy applications. [18]

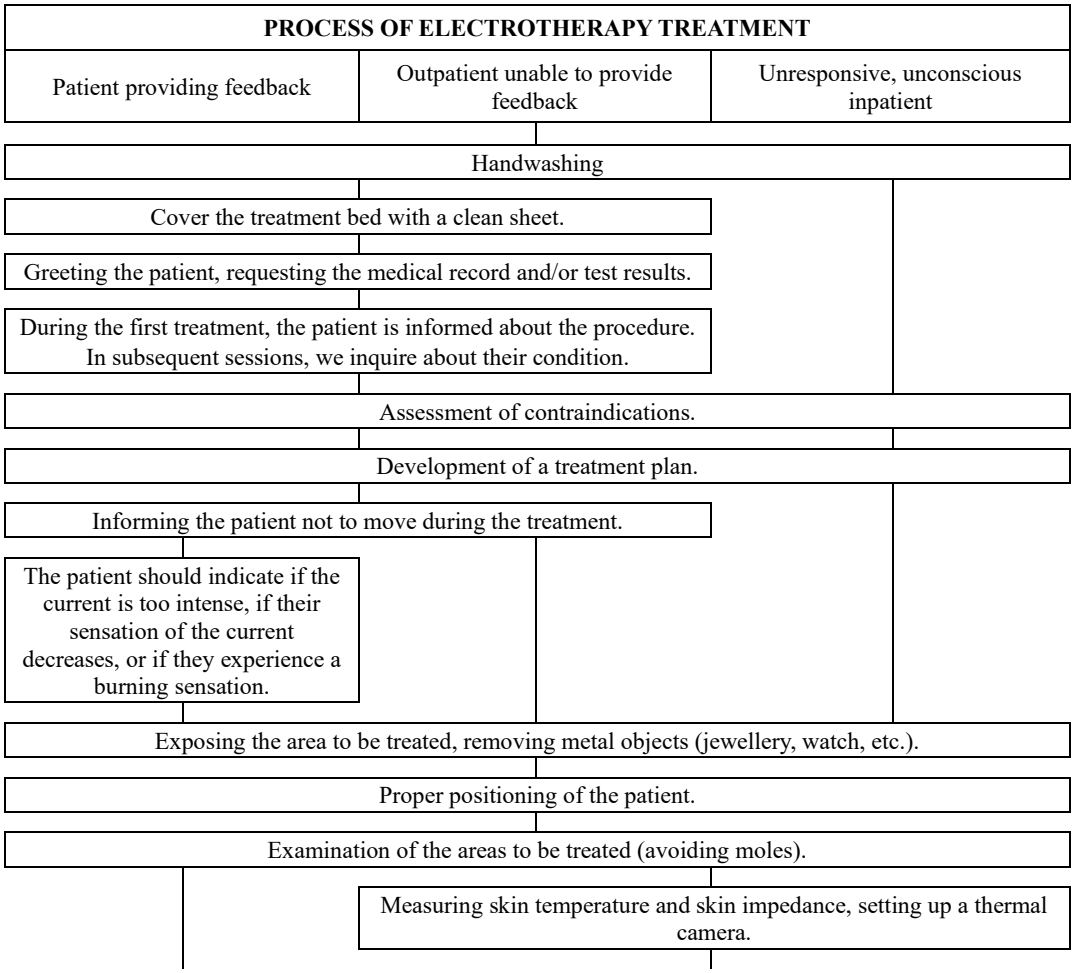
RISK ASSESSMENT MATRIX			PROBABILITY				
			Common (5)	Probable (4)	Occasional (3)	Rare (2)	Unlikely (1)
SEVERITY	Disastrous (4)		20	16	12	8	4
	Critical (3)		15	12	9	6	3
	Minimal (2)		10	8	6	4	2
	Negligible (1)		5	4	3	2	1
Evaluation	1-3	small	Acceptable (no action needed)				
	4-6	low	Examination required (action depends on the result)				
	8-10	medium	After the examination, risk reduction is necessary!				
	12-20	high	Avoid, immediate risk reduction is necessary!				

1. Table: Risk assessment matrix [18]

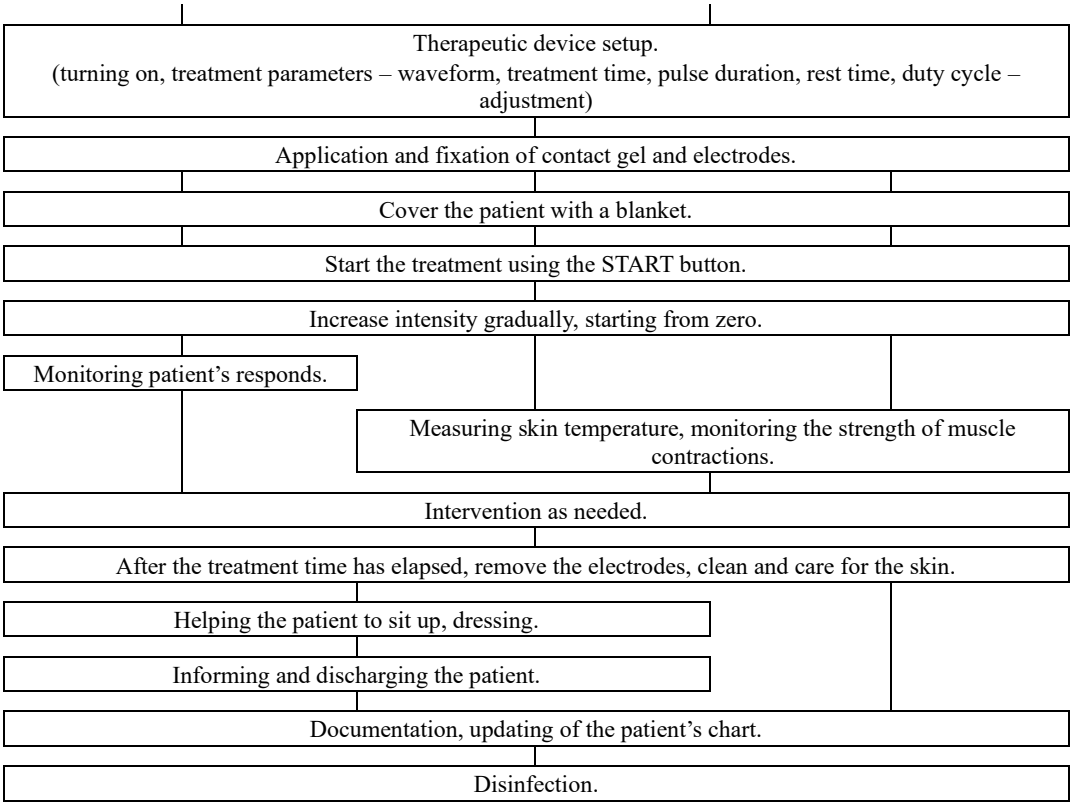
To support the development of targeted risk mitigation measures, the identified hazards were prioritised according to their risk classification (Table 5). The risk classification framework was informed by practical experience derived from electrotherapy treatments conducted over a five-year period in a private physiotherapy practice of one of the authors. Focused on patients who are unable to provide feedback, particular attention was given to risks associated with treatment failure and patient injury, which were considered critical and requiring immediate intervention. Additional focus was placed on risks related to incorrect treatment planning, the application of excessive therapeutic parameters, and infection.

RESULTS

Following the identification and systematic organization of the electrotherapy treatment steps across the three predefined patient groups, a comprehensive process flow diagram was developed (Figure 1).



1. Figure Electrotherapy treatment protocol (continued on the next page)



1. Figure: Electrotherapy treatment protocol (continuation of the previous page)

Safety considerations

Electrotherapy devices operate by converting mains voltage into low-intensity currents in the milliampere and microampere range suitable for therapeutic application. (typically ~230 Volts / 50 Hz in Europe, 117 Volts / 60 Hz in the United States). Accordingly, compliance with relevant electrical safety, technical, and clinical standards is required.The applicable regulatory frameworks in Hungary (EU), the United Kingdom, and the United States are summarised in Table 2.

Area	Hungarian / EU	United Kingdom	USA (standard / law)
Safety of Machinery	MSZ EN 60204-1:2018/A1	BS EN 60204-1	NFPA 79 – Electrical Standard for Industrial Machinery
Medical electrical equipment (Electromagnetic disturbances)	MSZ EN 60601-1-2:2015/A1:2021	BS EN IEC 60601-1-2	ANSI/AAMI IEC 60601-1-2 (FDA-approved consensus standard)
General occupational safety and health (framework law)	Act XCIII of 1993 on Labor Safety	Health and Safety at Work etc. Act 1974	Occupational Safety and Health Act (OSH Act, 1970)
Occupational health / work fitness / occupational medicine	Decree 20/2009 (VI. 18.) of the Ministry of Health	Management of Health and Safety at Work Regulations 1999 + related HSE regulations	OSHA 29 CFR (pl. 1910 Subpart Z, medical surveillance)

2. Table: Standards and regulations related to electrotherapy in the EU, UK, and USA

List of hazards

The identified hazards associated with the electrotherapy treatment process are presented in Table 3.

Tasks	Hazards
Ensuring hygienic conditions	Infection.
Assessment of the patient's condition	Lack of medical history. Incorrect measurement of parameters. Ignoring contraindications. Faulty treatment plan.
Ensuring the technical conditions of the treatment	Treatment failure. Under- or overtreatment.
Treatment	Exceeding the treatment limits. Damage to muscle fibres. Skin burns. Malfunction of electrodes or their connections. Damage to the therapeutic device.
Post-treatment procedures	Unauthorized use. Risk of infection. Data protection incident.

3. Table List of hazards

Causes of hazards

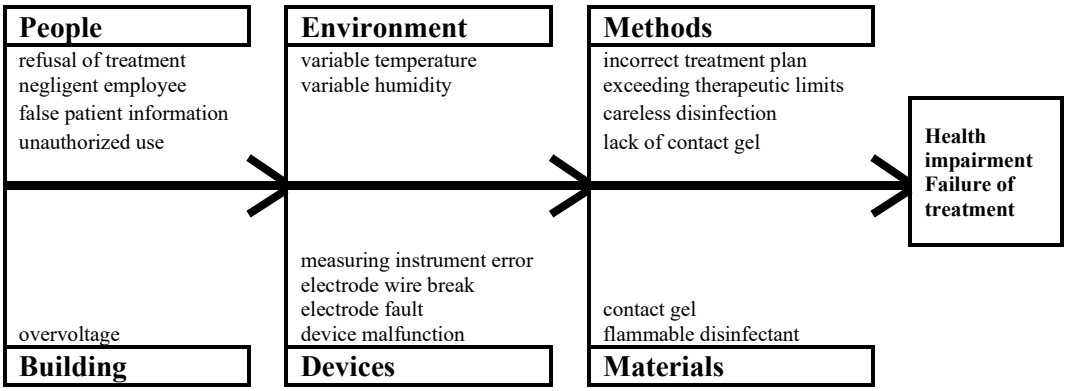
The potential causes associated with these hazards are summarised in Table 4.

Hazards	Potential causes
Treatment failure	The patient is uncooperative and refuses treatment. Malfunction of the therapeutic device. The area to be treated is not suitable for electrode placement.
Incorrect treatment plan	The patient provides incomplete and/or misleading information. Undocumented medical history. Incorrect environmental and biological measurement data.
The use of therapeutic parameters higher than permitted	Calculations based on incorrect initial data. Incorrect settings of the therapeutic device. Tired, careless employee.
Risk of infection	Treatment beds, measuring instruments, therapeutic electrodes, or objects in common areas not properly disinfected. A patient or medical staff hiding their illness.
Damage to the skin surface and/or muscle fibres	The patient conceals their actual condition. Due to an incorrect treatment plan, the therapy may be of too high intensity, have the wrong waveform, or last too long. Use of inappropriate therapeutic electrodes. Too little or missing contact gel. Malfunction of the therapeutic device.
Fire hazard	Improper storage of chemicals used for disinfection.
Damage to the therapeutic device	The chemical used for disinfection flows into the device. Due to incorrect use, the connection between the device and the electrodes is lost (wire breakage). Mains overvoltage.
Unauthorized use	Failure to lock the therapeutic device.
Data protection incident	Improper storage of medical records.

4. Table Causes of Hazards

Ishikawa (cause-and-effect) diagram

The relationships between hazards and their underlying causes were further analysed using an Ishikawa diagram (Figure 2). The hazards were assigned to six different groups depending on what causes the occurrence of each hazard. The possible causes were assigned to the persons involved in the treatment, the treatment environment, the methods applied, the building, the equipment, and the materials used in the treatment. Each of the possible causes leads to the two highlighted outcomes: health impairment and treatment failure.



2. Figure Cause-and-effect diagram of hazards

Risk classification of hazards

Based on the defined risk assessment matrix (Table 1), the identified hazards were classified according to their severity and probability (Table 5). Treatment failure was categorised as a high-risk hazard due to its potentially severe consequences and moderate likelihood of occurrence. Damage to the skin surface and muscle fibres was classified as a medium-level risk. Other hazards, including incorrect treatment planning, excessive therapeutic parameters, infection, fire hazard, equipment damage, unauthorised use, and data protection breaches, were predominantly classified as low or minimal risks.

Hazards	Severity	Probability	Risk classification
Treatment failure	disastrous	occasional	high
Incorrect treatment plan	critical	rare	low
The use of therapeutic parameters higher than permitted	critical	rare	low
Risk of infection	minimal	rare	low
Damage to the skin surface and/or muscle fibres	disastrous	rare	medium
Fire hazard	critical	unlikely	small
Damage to the therapeutic device	minimal	unlikely	small
Unauthorized use	minimal	unlikely	small
Data protection incident	minimal	rare	small

5. Table Risk classification of hazards

Following the implementation of risk mitigation measures, a revised risk classification was established (Table 6). The results indicate a reduction in risk levels across all categories, with previously high- and medium-level risks being reduced to low or minimal levels.

Hazards	Severity	Probability	Risk classification
Treatment failure	disastrous	unlikely	low
Incorrect treatment plan	critical	unlikely	small
The use of therapeutic parameters higher than permitted	critical	unlikely	small
Risk of infection	minimal	unlikely	small
Damage to the skin surface and/or muscle fibres	disastrous	unlikely	low
Fire hazard	critical	unlikely	small
Damage to the therapeutic device	minimal	unlikely	small
Unauthorized use	minimal	unlikely	small
Data protection incident	minimal	unlikely	small

6. Table Effects of risk-reducing measures

DISCUSSION

The present study aimed to identify and systematically evaluate the risks associated with electrotherapy for patients unable to provide feedback, and to develop targeted risk mitigation strategies. The findings highlight that, although electrotherapy is generally considered a safe and effective therapeutic modality, its application in this vulnerable patient population requires enhanced precautionary measures.

One of the most critical risks identified was treatment failure, which may arise from multiple factors, including patient non-cooperation or inadequate communication. In particular, insufficient patient information and suboptimal staff–patient interaction may lead to refusal of treatment, thereby compromising therapeutic outcomes. These findings underline the importance of effective communication strategies and continuous professional training of healthcare personnels. The treatment may also fail due to a malfunction of the therapeutic device or a break in the electrode wires. In this case, the faulty device or electrode must be promptly sent to a professional service centre. The failure of the treatment can be prevented by using a replacement device with similar parameters or by using spare electrodes.

Tissue damage, including skin injury and muscle fibre damage, was also identified as a significant risk. This may result from inappropriate treatment parameters, inadequate electrode application, or insufficient use of contact gel. Due to inaccurate treatment plan, therapy of too high intensity, incorrect waveform, or prolonged duration may be occurred, which in milder cases can result in ineffective treatment, in more severe cases can cause damage to the skin or muscle fibres. In patients unable to provide feedback, such adverse effects may remain undetected until significant damage has occurred. Therefore, the implementation of objective monitoring methods, such as skin temperature measurement, is essential to ensure patient safety. In case of injury, the patient must receive medical care. Coverage for any significant monetary claims resulting from the patient's potential damages can be provided through an appropriate level of professional liability insurance. If the injury occurs due to electrodes of inadequate size or quality, or due to insufficient contact gel, the

activities of the attending staff and the content of the therapeutic protocol must be reviewed. In case of faulty electrodes, the electrode must be replaced, and the defective electrode must be sent to a professional service centre.

The analysis further demonstrated that incorrect treatment planning constitutes an important contributory factor to several identified hazards. This is particularly relevant in cases where patient-related information is incomplete or unreliable. For patients unable to provide feedback, reliance on accurate medical documentation and objective diagnostic measurements becomes crucial. In this context, the involvement of a physician in prescribing and supervising electrotherapy may significantly reduce associated risks.

Although less frequent, fire hazards and technical failures were also identified as potential risks associated with electrotherapy. These risks are primarily linked to improper storage of flammable materials, inadequate maintenance of devices, and electrical faults. Appropriate storage practices, routine equipment inspection, and the availability of suitable fire extinguishing equipment (Class ABC) are therefore necessary components of safe clinical practice.

Infection risk remains a fundamental concern in all physiotherapeutic interventions. The findings emphasise that adherence to established infection control protocols, including regular disinfection of equipment and treatment environments, is essential. In the European Union, the regulation is uniform. In Hungary, the current regulation in force is Decree 20/2009 (VI.18.) of the Ministry of Health, concerning the prevention of healthcare-associated infections, the professional minimum requirements for these activities, and their supervision. The decree requires the existence of infection control, whose purpose is to prevent avoidable infections associated with healthcare. The regulation mandates that healthcare providers must have an infection control manual. The content of the manual must be reviewed at least every two years based on experience, and any amendments must be recorded. The provisions contained in the manual are binding for all employees and contracted personnel of the healthcare provider. [19]

Data protection represents an additional, non-clinical risk factor. Improper handling or storage of patient records may result in data protection breaches. Ensuring secure storage systems and restricting access to authorized personnel are essential measures to mitigate such risks. The risk of data protection incidents can be reduced by storing patient records away from the treatment room, in a physically separate, lockable cabinet. It is the responsibility of the medical staff to ensure that only the records of the currently treated patient are accessible in the room during the treatment session. The compliance with the new protocol established based on measures taken to reduce risk must be regularly monitored. According to Section 54 (3) of Act XCIII of 1993 on Occupational Safety, in force in Hungary, "the employer is obliged to carry out risk assessments, risk management, and the determination of preventive measures – in the absence of other legal provisions – before starting the activity, afterwards if justified, but at least every 5 years." [20]

The risk assessment must be documented in every case, even if it is determined during this process that there has been no change in the risks and the measures applied continue to be adequate. The employer must prove that they have taken all necessary measures to assess and eliminate the risks, or to minimize them. Proper documentation of the results includes the process followed during the risk assessment and the goals achieved.

The documentation prepared as a result of the risk assessment has no prescribed form, however, at least the following must be recorded:

- the date, place, and subject of the risk assessment,
- the identifying data of the person conducting the assessment;
- identification of hazards;
- identification of those at risk and the number of people affected;
- factors that exacerbate the risk;
- qualitative and/or quantitative evaluation of the risks and the determination of whether the conditions comply with occupational safety regulations and whether the risks are maintained at an acceptable level;
- necessary preventive measures, their deadlines, and the persons responsible;
- the planned next date for preparing the risk assessment;
- the date of the previous risk assessment.

The employer must keep the document for at least 5 years. [20]

From a broader perspective, the findings of this study highlight the importance of integrating risk management into routine clinical practice in physiotherapy. Continuous monitoring, regular updating of treatment protocols, and the incorporation of risk assessment into institutional procedures are essential to ensure patient safety. A key contribution of this study is the identification of the lack of a unified, widely accepted professional protocol for the electrotherapy of patients unable to provide feedback. This gap in clinical practice underscores the need for the development of standardized guidelines and evidence-based recommendations.

LIMITATIONS

The risk assessment was primarily based on qualitative analysis and practical experience, which may limit the generalisability of the findings. Future research should aim to validate the proposed risk classification and mitigation strategies through quantitative studies and clinical data.

Overall, the findings support the implementation of a comprehensive, multidisciplinary approach to risk management in electrotherapy, particularly in the treatment of patients who are unable to provide feedback.

CONCLUSIONS, RECOMMENDATIONS

Electrotherapy in patients unable to provide feedback is associated with a range of potentially underestimated risks arising from patient-related, human, and technical factors. The absence of reliable sensory feedback significantly increases the likelihood of undetected adverse events, including tissue damage and ineffective treatment. This study demonstrates that the application of a structured risk assessment framework enables the systematic identification and effective mitigation of these risks. The implementation of targeted measures—particularly in relation to treatment planning, objective patient monitoring, staff training, equipment maintenance, and infection control—can substantially improve patient safety. The findings emphasize the necessity of regularly updating treatment protocols and integrating risk management into routine clinical practice. Strengthening both physical and

data security within the therapeutic environment is also essential. Importantly, the absence of a unified professional protocol for the electrotherapy of patients unable to provide feedback highlights a critical gap in current practice. The development of standardized, evidence-based guidelines is therefore strongly recommended.

Overall, a comprehensive and proactive approach to risk management is essential to ensure the safe and effective application of electrotherapy in this vulnerable patient population.

FUNDING STATEMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

[1] B. G. Diriczíné., *Elméleti és gyakorlati fizioterápia*, 2nd edition. Budapest: Kádix Bt., 2013.

[2] Rugby Football Union, *Total number of match injuries among male professional players recorded by the Rugby Football Union (RFU) in England from 2002/03 to 2022/23 [Graph]*, [Online], 0 13, 2024.

[3] International Ski Federation (FIS), *Total number of reported injuries that at International Ski Federation (FIS) events between the 2006 and the 2019 season, by discipline [Graph]*, [Online], May 28, 2019.

[4] Eurostat, *Number of hospital discharges after a disease of the musculoskeletal system and connective tissue in 2021, by European country (per 100 thousand inhabitants) [Graph]*, 0 03, 2024. [Online]. Available: https://www.statista.com/statistics/1241247/hospital-discharges-following-a-disease-of-the-musculoskeletal-system-europe/

[5] L. Chen, Y.-K. Lo, Y. Wang, and W. Liu, 'Thermal model of spiked electrode in Transcutaneous Electrical Nerve Stimulation (TENS)', in *2017 8th International IEEE/EMBS Conference on Neural Engineering (NER)*, Shanghai, China: IEEE, May 2017, pp. 219–222. doi: 10.1109/NER.2017.8008330.

[6] W. Zschiesche, 'Electric shock accidents at the workplace : Hazards, effects on health, medical surveillance', *Arbeitsmedizin Sozialmedizin Umweltmedizin*, vol. 45, no. 4, pp. 164–169, 2010, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-77952177090&partnerID=40&md5=711bc31eba4d856fa787fd8bba42bfba

[7] D. Gao, K. Yue, C. Yuan, and X. Zhang, 'Numerical Simulation of the Influence of Ambient Temperature and Humidity on Skin Sweating and Electrical Characteristics', presented at the BIBE 2024 - Conference Proceedings, 7th International Conference on Biological Information and Biomedical Engineering, 2024, pp. 49–55. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85216003713&partnerID=40&md5=72e2810b5dcfab06a596461915e56e65

[8] Y. Laufer, H. Tausher, R. Esh, and A. R. Ward, 'Sensory transcutaneous electrical stimulation fails to decrease discomfort associated with neuromuscular electrical stimulation in healthy individuals', *American Journal of Physical Medicine and Rehabilitation*, vol. 90, no. 5, pp. 399–406, 2011, doi: 10.1097/PHM.0b013e318214f64a.
[9] K. Saito *et al.*, 'The modulatory effect of electrical stimulation on the excitability of the corticospinal tract varies according to the type of muscle contraction being performed', *Frontiers in Human Neuroscience*, vol. 8, no. OCT, 2014, doi: 10.3389/fnhum.2014.00835.
[10] M. Kafri, N. Zaltsberg, and R. Dickstein, 'EMG activity of finger flexor muscles and grip force following low-dose transcutaneous electrical nerve stimulation in healthy adult subjects', *Somatosensory and Motor Research*, vol. 32, no. 1, pp. 1–7, 2015, doi: 10.3109/08990220.2014.937413.
[11] M. A. Ramasamy *et al.*, 'Outcomes of IED Foot and Ankle Blast Injuries', *Journal of Bone and Joint Surgery*, vol. 95, no. 5, p. e25, Mar. 2013, doi: 10.2106/JBJS.K.01666.
[12] S. Laureys, A. M. Owen, and N. D. Schiff, 'Brain function in coma, vegetative state, and related disorders', *The Lancet Neurology*, vol. 3, no. 9, pp. 537–546, Sep. 2004, doi: 10.1016/S1474-4422(04)00852-X.
[13] J. Barr *et al.*, 'Clinical Practice Guidelines for the Management of Pain, Agitation, and Delirium in Adult Patients in the Intensive Care Unit':, *Critical Care Medicine*, vol. 41, no. 1, pp. 263–306, Jan. 2013, doi: 10.1097/CCM.0b013e3182783b72.
[14] K. J. S. Anand and P. R. Hickey, 'Pain and Its Effects in the Human Neonate and Fetus', *N Engl J Med*, vol. 317, no. 21, pp. 1321–1329, Nov. 1987, doi: 10.1056/NEJM198711193172105.
[15] J. L. Matson and M. Shoemaker, 'Intellectual disability and its relationship to autism spectrum disorders', *Research in Developmental Disabilities*, vol. 30, no. 6, pp. 1107–1114, Nov. 2009, doi: 10.1016/j.ridd.2009.06.003.
[16] S. Tesfaye *et al.*, 'Diabetic Neuropathies: Update on Definitions, Diagnostic Criteria, Estimation of Severity, and Treatments', *Diabetes Care*, vol. 33, no. 10, pp. 2285–2293, Oct. 2010, doi: 10.2337/dc10-1303.
[17] International Organization for Standardization, *Risk Management*. pp. 22–32.
[18] Morvay L. and Szűcs E., 'Risk assessment, evaluation and management in low level laser therapy (LLLT)', *Safety and Security Sciences Review*, vol. 6, no. 2, pp. 33–46, Jun. 2024, [Online]. Available: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/463
[19] Ministry of Health, *20/2009. (VI. 18.) Ministry of Health Regulation on the Prevention of Healthcare-Associated Infections, the Professional Minimum Requirements for These Activities, and Their Supervision*. 2009. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a0900020.eum
[20] Parliament, *Act XCIII of 1993 on Labor Safety*. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=99300093.TV

DOI: https://doi.org/10.12700/btsz.2026.8.2.43

THE DEVELOPMENT OF AN EMERGING DISCIPLINE: EXCERPTS FROM THE OSINT LITERATURE

EGY SZÜLETŐ TUDOMÁNYÁG FEJLŐDÉSI ÍVE: SZEMELVÉNYEK AZ OSINT SZAKIRODALMÁBÓL

TAMPU Ferenc[1] – BEREK László[2]

Abstract

The use of open-source intelligence is as old as human history itself. Its meaning has changed and expanded greatly over the years, but the acronym OSINT itself was coined just over 30 years ago. The information technology revolution and the spread of the World Wide Web have led to its widespread use in everyday life. Computerization, machine learning, and artificial intelligence have opened new perspectives for open-source intelligence gathering. Its development—often divided into three eras—along with the emergence of its sub-disciplines and the rapid growth of its literature, marks the rise of a new field of science. Throughout the changes of the eras, various aspects of security have been a constant common thread, linking the past with the expansion of current meaning. Considering the development curve of the sources re-viewed and the growth of its literature, it can be said that its relevance will only increase over time, and accordingly, its designation as an independent field of science cannot be disputed.

Keywords

OSINT, Open-Source Information, Artificial Intelligence, AI, History, Literature

Absztrakt

A nyílt forrású hírszerzés használata egyidős az emberiség történetével. Jelentéstartalma az évezredek során sokat változott, bővült, de az OSINT mozaikszó maga alig több mint 30 éve született meg. Az információs technológia és forradalma, majd a világháló térnyerése a mindennapi életben széleskörű használatát vonta maga után. A számítógép, a gépi tanulás és a mesterséges intelligencia új perspektívákat nyitott meg a nyílt forrású információszerzés számára. A három korszakra osztható fejlődéstörténete, szakágainak kialakulása és szakirodalmának exponenciális növekedése napjainkban egy új tudományág létrejöttének kezdetét jelenti. A korszakok változásaiban a biztonság különböző aspektusai az állandó közös, az köti össze a múltat az aktuális jelentéstartalom bővülésével. Mint megannyi tudományágnak, a jövője nyitott. Az áttekintett források fejlődési ívét és szakirodalmának növekedését figyelembe véve elmondható, hogy aktualitása az idő haladtával csak erősebb lesz, ennek megfelelően az önálló tudományág megnevezést elvitatni nem lehet.

Kulcsszavak

OSINT, nyílt forrású információ, mesterséges intelligencia, MI, történet, szakirodalom

[1] fryczi@gmail.com | ORCID: 0009-0002-6824-1188 | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola | PhD Student, Obuda University - Doctoral School for Safety and Security Sciences

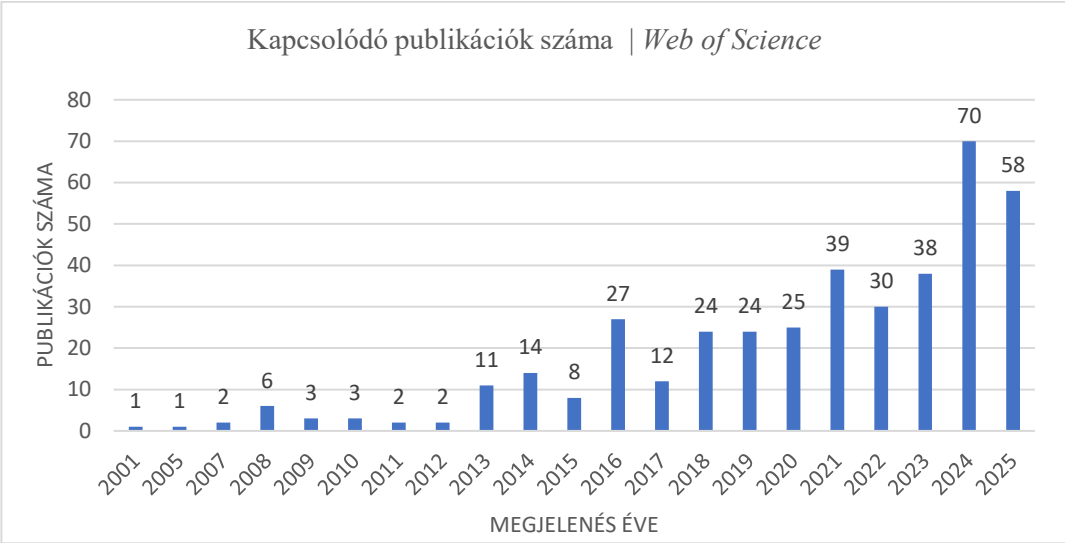
[2] berek.laszlo@uni-obuda.hu | ORCID: 0000-0002-4126-1528 | könyvtárigazgató, Óbudai Egyetem Egyetemi Könyvtár; Óbudai Egyetem Innováció Menedzsment Doktori Iskola; Gábor Dénes Egyetem | Library director Obuda University University Library; Obuda University Doctoral School of Innovation Management; Dennis Gabor University

BEVEZETÉS

Az elmúlt 30 év az informatika, az internet és az infókommunikációs eszközök világában annyi változást, fejlődést hozott, hogy az OSINT (Open Source Intelligence, Nyílt forrású hírszerzés) akronim szót – különösképpen szakmai körökben – ma már nem csak a hagyományos hírszerzéssel azonosítják, de sokkal inkább a gazdasági, üzleti célú nyílt forrású információszerzéssel. Nyílt forrásokból való információszerzés története az emberiség hajnaláig nyúlik vissza. E tevékenység fontossága az állam megalakulása, annak intézményeinek létrejötte utáni időszakban felerősödik. Állambiztonsági szempontból, katonai felderítés okán, vagy csak egyszerűen a szomszédos országok vagy az ellenség szándékainak megismerése céljából nélkülözhetetlenné vált a nyílt forrású információk gyűjtése. Az évszázadok során azonban a hírszerzési tevékenység sokat változott, módszerei teljesen átalakultak, forrásai megsokszorozódtak, céljai pedig ma már szerte ágazóak. Maga az OSINT elnevezés azonban csak a 20. század végén született meg. [1]

Tanulmányunk célja áttekinteni ennek a ma már „új tudományágnak" aposztrófált terület szakirodalmát, megvizsgálni a különböző korokban annak tartalmi jelentését, változásait és fejlődését. A hírszerzési tevékenység, a nyílt forrású információk gyűjtése nem mindig ugyanazt jelentette a különböző korszakokban. A 20. század végétől mást jelent a szakirodalomban a katonai, állambiztonsági hírszerzés, és egészen mást a kereskedelmi, gazdasági (vállalati) célú nyílt forrású információgyűjtés még akkor is, amikor mindkét esetben OSINT tevékenységről beszélünk. A kémkedésről – mely a nyílt forrású információszerzéssel ellentétben nem legális - mint egy egészen másfajta hírszerzési tevékenységről nem is beszélve. Napjainkban ezek már világos határvonalakkal elkülöníthető, önálló szakterületek. Az internet és az infokommunikációs technológiák dinamikus fejlődése, a keresőmotorok széles körű elterjedése, valamint az információmennyiség exponenciális növekedése egy új tudományterület létrejöttének és intézményesülésének feltételeit teremtette meg. E folyamatok egyúttal hozzájárultak a vizsgált terület forrásainak bővüléséhez és módszertani eszköztárának folyamatos finomodásához. Ennek eredményeképpen az OSINT kifejezés napjainkban egy sokkal tágabb fogalom lett. Az OSINT egyszerre jelent ma már tevékenységet, adatot, információt és ezek hitelesítése esetén beszélhetünk hitelesített OSINT információról. [2] Ennek – a tudomány és kutatás rohamosan fejlődő világában – pedig éppen egy újabb jelenség ad még nagyobb lendületet, a mesterséges intelligencia (MI). Ezek fényében beláthatatlan mi lesz a következő fejlődési lépcsőfok.

A külföldi és a magyar szakirodalmat - a teljesség igénye nélkül - párhuzamosan vizsgáljuk, így könnyebben nyomon követhető és megérthető az „új tudományág" hazai szakirodalmának kialakulása, fejlődése és jelenlegi állása. Az OSINT akronim értelmezésébe, definíciókkal való kifejtésébe nem kívánunk belemenni, hiszen azt több tanulmány, tudományos anyag is próbálja megvilágítani, tiszta képet adni róla [3], de célunk meghúzni a különböző korok határvonalait, tartalmának változásaira, bővülésére mindenképpen szeretnénk reflektálni, a legjelentősebb forrásokat áttekinteni. Ennek fontosságát altámasztja, hogy napjainkban több értelmezésben, különböző kontextusokban használja a szakirodalom és a felhasználó közösség az OSINT-ot, pedig kronológiailag jól elkülöníthető három generációra lehet azt felosztani [4] és még több szakágra [2], mely további vita tárgyát képezi. A vita lényegi pontja, hogy a szakágak közötti határvonalak legtöbbször elmosódnak. [5]



1. Ábra. Az OSINT szakirodalmi források számszerű alakulása Web of Science alapján. Saját szerkesztés. Forrás: Web of Science.

AZ OSINT ELSŐ GENERÁCIÓJA

Külföldi kitekintés

Bár nyílt forrású információszerzési tevékenységet mindig is végzett az emberiség, ebben a korszakban a mai értelemben vett OSINT-ról - mint a nyílt forrású információszerzés módszeres alkalmazásáról egy adott témában, egy bizonyos cél érdekében - még nem beszélhetünk. A szakirodalommal összhangban megállapítható, hogy a nyílt forrásokból való hírszerzés egyidős az emberiség történetével. E korszakot az emberiség kezdetétől az internet megjelenéséig datáljuk. [4] Ekkor még – különösképpen háború idején – a katonai felderítés és az állambiztonsági szervek alkalmazták. Az első korszakban még a titkosszolgálati tevékenységeket és a kémkedést egyaránt a műfaj részeként kezeli a szakirodalom. Ez utóbbi két fogalom majdnem szinonimája egymásnak. Pontosabban amíg a hírszerzés magába foglalhat nyílt forrásokat is, a kémkedést a hírszerzés agresszívabb és illegálisabb formájának lehet tekinteni, titkos jellegével különbözik a hagyományos hírszerzéstől, melyet a nemzetközi [6] és a nemzeti jog [7] egyaránt büntet. Alkalmazásának legfőbb célja egy állam vagy hatalom számára a maga biztonságának megteremtése, esetleges veszélyekkel szembeni alkalmazása, a polgárok védelme. A témában publikált egyik első külföldi kiadvány Roger Mennevée 1929-ben megjelent kétkötetes műve, a *L'espionnage international en temps de paix* (Nemzetközi kémkedés békeidőben). A nyomozati műveiről ismert francia író, újságíró a békeidőben történő kémkedés témáját dolgozza fel és rendszerezi. Tematikája stratégiai, politikai, gazdasági, katonai információk illegális vagy titkos módszerekkel történő gyűjtésére terjed ki. Az első kötet általános megfogalmazásokkal foglalkozik, mint például az információ szükségessége és annak megszerzési módszerei, továbbá foglalkozik a hivatalos és titkos forrásokkal, a kémhálózatokkal, a központi szervekkel és a különböző minisztériumokkal. A második kötet kitér a kémkedésre vonatkozó jogszabá-

lyokra, az ellenfelderítésre, továbbá tartalmaz árulási ügyekben hozott ítéleteket, minisztériumi körleveleket, mindezt pedig egy témával kapcsolatos bibliográfiával egészít ki. Mennevée műve a fentiek alapján még nem tekinthető mai értelemben vett OSINT tevékenységnek, az vitán felül a titkosszolgálati tevékenységet és a kémkedést fedi le. [8]

Donovan (1946), aki maga is a második világháború alatt vezette az OSS-t (Office of Strategic Services, Stratégiai Szolgálatok Hivatala) egyik cikkében határozott állást foglal a nyílt forrásokból származó információk felhasználásának fontossága mellett egy központi hírszerző szolgálat (Central Intelligence Service) keretein belül. Az erről szóló cikke a Life Magazin szeptemberi számában jelent meg. A szerző alapvetése, hogy a hírszerzés békeidőben is fontos, különösen az új globális fenyegetésekkel szemben, a kibontakozó hidegháborúval összefüggésben az Egyesült Államok védelmi állásainak megerősítése végett. Tanulmányában ő már a nyílt forrásokból származó információ felbecsülhetetlen értékéről ír, mely a hírszerző szolgálatok számára is nélkülözhetetlen. Ez a gondolat számított igazán forradalmi koncepciónak. A sokat idézett cikk, mely egy szélesebb körű akadémiai, újságírói vita része volt, hozzájárult a Központi Hírszerző Ügynökség (Central Intelligence Agency, CIA) 1947-es megalakulásához és ahhoz, hogy a kérdés évtizedekig a közvélemény figyelmének a fókuszában maradjon. [9]

Annak ellenére, hogy Donovan már a 20. század közepén felhívta a figyelmet a nyílt forrású információk felhasználásának fontosságára, mégis az 1990-es évekig kevés figyelmet kapott a téma. Robert Steele 1990-ben megjelent cikkével, *Intelligence in the 1990's: recasting national security in a changing world* [1] újabb mérföldkőhöz érkezett a nyílt forrású információk felhasználásának kérdése. Egyrészt ő használja először a napjainkban elterjedt OSINT mozaikszót: "… kevés figyelmet szenteltünk a nyílt forrásokra (OSINT) …" [1]. Másrészt a hidegháború vége alapjaiban igényelt átalakítást a hírszerzés és a nemzetbiztonság terén a hagyományostól eltérő, komplexebb fenyegetésekkel szemben. Egy olyan informatikai infrastruktúra létrehozását szorgalmazza, mely integrálja a távközlést, az informatikai feldolgozást és az elemzést, ezzel lehetővé téve az emberi erőforrásból - (HUMINT), jelekből - (SIGINT), képekből - (IMINT) és a nyílt forrásokból (OSINT) származó adatok teljes körű kiaknázását és felhasználását. Ezzel a hírszerzési tevékenység tagolásába megjelent az OSINT kifejezés a mai napig használt formájában, mint önálló szakterület. [1] Ezt követően 1992-ben az Egyesült Államokban megrendezésre került az első konferencia a témában, melynek anyagát az American Intelligence Journal 1993-ban egy különszámban adta ki. A kiadványban megjelent Steele cikkének címe is jelzi (Nemzeti hírszerzés és nyílt források: az iskolától a Fehér Házig), hogy az OSINT használata nélkülözhetetlen a társadalom legalsó szintjétől a legmagasabb szintű hivatalig. [10]

Lehetetlen pontos kronológia szerint számba venni az OSINT első generációjának szakirodalmát – melyet ekkor még leginkább az állambiztonság erre kijelölt hírszerző szervei alkalmaztak – mivel a második generáció időszakában született meg az első korszakról ma is használt tudományos kiadványok többsége. Ezek közül a legjelentősebbeket néhány gondolat erejéig górcső alá vesszük. Andrew, Christopher grandiózus műve, a *The Secret World. A History of Intelligence* (*A titkos világ: a hírszerzés története*) bár 2018-ban jelent meg mégsem a mai értelembe vett OSINT-t ismerteti. A 30 fejezetből és több mint 950 oldalból álló műve visszamegy az emberiség kezdetéig, a bibliai Mózes történetétől kezdve végigmegy az emberiség történetén a 2001.09.11-én bekövetkezett New York székhelyű

Világkereskedelmi Központ (World Trade Center) ellen elkövetett merényletig. Részletesen elemzi és felfedi a hírszerzés és a kémkedés közel 3000 ezer évének „feledésbe" merült történetének nagy részét, az elkövetett hibákat és azok okait. Mondandója arra épül, hogy akik nem értik a múlt hibáit, azok újból elkövetik azokat. Erre nagyon jó példa a hírszerzés. [11] A kiadvány hatását és aktualitását mutatja az is, hogy egy évvel megjelenése után Neil Kent egy nagy ívű cikkben alaposan ismerteti és elemzi a könyv és a téma jelentőségét. [12]

Az előzőektől eltérően az OSINT történetének kezdeteit több, a témával foglalkozó szakember is a második világháború előestélyére datálja az OSINT történetének kezdeteit, a BBC Monitoring Service 1939-es megalakulásával (Nagy-Britannia) és a Foreign Broadcast Monitoring Service (FBMS) 1941-es létrehozásával (Egyesült Államok) egyidőben. [13-16] Ennek legfőbb oka, hogy ez utóbbiak a mai értelemben vett OSINT, vagyis a nyílt források felhasználásának kezdeteiről írnak, nem pedig a hírszerző szolgálatok kezdetektől alkalmazott klasszikus hírszerző tevékenységéről, netán a kémkedés világának kezdeteiről. Ezzel jól elkülönítve a nyílt forrású információszerzés mai értelmezését a hírszerzés és kémkedés világától. A hidegháború idején azonban a vasfüggöny mindkét oldalán jöttek létre nyílt forrásokat felhasználó hírszerzési intézmények, bővítették kapacitásaikat, amelyeket beágyaztak saját hírszerzési rendszereikbe is. [17]

A tudományos szakirodalmon és tanulmányokon túllépve egy apró kitekintés erejéig áttekintettünk néhány internetes forrást is a témában. Ezek tartalma az OSINT megjelenésére és fejlődésére vonatkozólag megegyezik azokkal az állásfoglalásokkal, melyek a 20. század közepére teszik a nyílt forrású hírszerzés kezdeteit, arra az időszakra, mikor létrejönnek az első intézmények célzottan erre a feladatra. [18]

Magyarország

Az OSINT első generációjának tárgyalása a magyar szakirodalomban is szorosan kapcsolódik a katonai felderítés, a kémelhárítás, valamint az állambiztonság szempontjából kulcsfontosságú hírszerzési tevékenységhez. Az alábbiakban – a teljesség igénye nélkül – azokat a műveket emeljük ki, amelyeket a téma szempontjából a legmeghatározóbbnak tartunk.

Magyarországon az első összefoglaló mű 1936-ban jelent meg Pilch Jenő összeállításában. A három kötetes, több mint 1100 oldalas kiadvány méltán tekinthető Mennevée könyvéhez hasonlóan úttörőnek hazánkban. [19] E grandiózus mű kronológiailag egy jól felépített logika mentén ismerteti az ókortól egészen a megjelenés időszakáig a hírszerzés és a kémkedés jelentőségét, múltját, a különböző korok változásait, módszereit rengeteg érdekességgel színesítve[3]. A trilógia harmadik kötetében kitér a nők hírszerzésben és kémkedésben betöltött szerepére, az ipari és gazdasági hírszerzés jelentőségére, mely ismeretlen volt az első világháború előtt. Már-már filozófiai fejtegetésnek tekinthető az a gondolatmenete, mely szerint a propaganda közeli rokona a kémkedésnek, amennyiben közös a céljuk: az ellenséges vagy bármely állam katonai és politikai viszonyairól megbízható információk gyűjtése, melyek segítségével ellehetetleníthető egy állam támadó szándék esetén.

Közel egy évszázados távlatból is elmondható, hogy a témában megjelent nagyszabású szakmai anyag tartalma nem veszített sem értékéből, sem alkalmazhatóságából. A

[3] Ilyen például - többek között - a II. Rákóczi féle szabadságharcban alkalmazott titkosírás módszer, melynek lényege, hogy csak az író és a címzett ismerte. Így a hírvivő célba érés előtti elfogása nem jelenthette automatikusan a hírhez való hozzáférést.

szakma napjainkban is használja és ajánlja. Ennek egyik ékes bizonyítéka Nándori Nikoletta Petra 2019-ben megjelent részletes ismertetése is (Szakmatörténeti forrásajánló) a Nemzetbiztonsági Szemlében. [20]

Az előző terjedelménél lényegesen kisebb (közel 130 oldalas), de szakmailag nem mellőzhető Ónodi György műve sem: *A hírszerzés története – Ókor, középkor, újkor*. Többek között abban is különbözik Pilch Jenő 3 kötetes „életművétől", hogy nagyon olvasmányosan dolgozza fel a témát. Egy igazi történelmi összefoglaló, különösképpen a kémkedés évszázadokon átívelő változásaira és korunkig tartó fejlődésére helyezi a hangsúlyt. [21] A kémkedés – és nem annyira a hírszerzés – történetének másik kiemelkedő kutatója a Sachenhousen koncentrációs tábort is megjárt, majd az 1956-os magyar forradalomban is résztvevő, annak leverése után Ausztriába menekülő Janusz Piekałkiewicz lengyel író, televíziós és filmrendező producer. Az ókortól napjainkig kiséri végig a kémek, felderítők világát. A könyv tényszerű ismeretket ad át, felvonultatja a világtörténelem híres kémfiguráit olvasmányos stílusban. [22]

Az OSINT első generációjának vége után is több figyelemreméltó mű jelent meg e korszakról. Ezek közül az egyik a legjelentősebb összefoglaló Boda József és Regényi Kund szerkesztésében jelent meg 2019-ben, mely egy közel 200 oldalas többszerzős tanulmánykötet. A kiadvány jelentőségét az is megalapozza, hogy – az ókortól egészen a második világháború végéig – rendkívül részletes áttekintést nyújt a témáról, és az egyes jelentősebb országok hírszerzési tevékenységét külön-külön is bemutatja. Emellett nem csupán a kémkedés és a titkosszolgálatok történetével foglalkozik, hanem a mai értelemben vett nyílt forrású információgyűjtés (OSINT) előzményeire is kitér. A mű így átfogó képet ad a hírszerzés módszereiről, valamint a biztonsági szolgálatok által alkalmazott információszerző tevékenységekről is. [23]

E korszak magyar nyelvű szakirodalmából nem hagyható figyelmen kívül Regényi Kund Miklós Nemzetbiztonsági Szemlében megjelent cikke sem. E tanulmány egyrészt azért is figyelemre méltó, mert részletesen bemutatja az internet előtti időszakban alkalmazott nyílt forrású információszerzés forrásait. Másrészt ebben a korszakban jelenik meg először az OSINT-információ fogalma, valamint az a felismerés, hogy a nyílt forrású információgyűjtés a nemzetbiztonsági hírszerzés szerves részét képezi. [24]

AZ OSINT MÁSODIK GENERÁCIÓJA

E korszakot az internet tömeges elterjedéséhez köti a szakirodalom. Ennek pontos éve ugyan nem nevezhető meg, hiszen az internet kezdetei sokkal korábbra datálhatók annál, minthogy az az 1990-es évek elejétől hozzáférhetővé válik a széles tömegek számára is. [25-27] Ekkortól (web 2.0) számítjuk az OSINT második generációját a 2000-es évek elejéig, a szemantikus web (web 3.0) elterjedéséig. Ebben az időszakban születik meg a ma is használt OSINT terminológia. Nemcsak széleskörű használata terjed roham szerűén, de szakirodalma is kiugróan megnövekszik. Szakemberek és intézmények egyaránt foglalkoznak a születő „új tudományággal", tanulmányok, cikkek, kézikönyvek, konferenciák sora jelzi a robbanásszerű fejlődést.

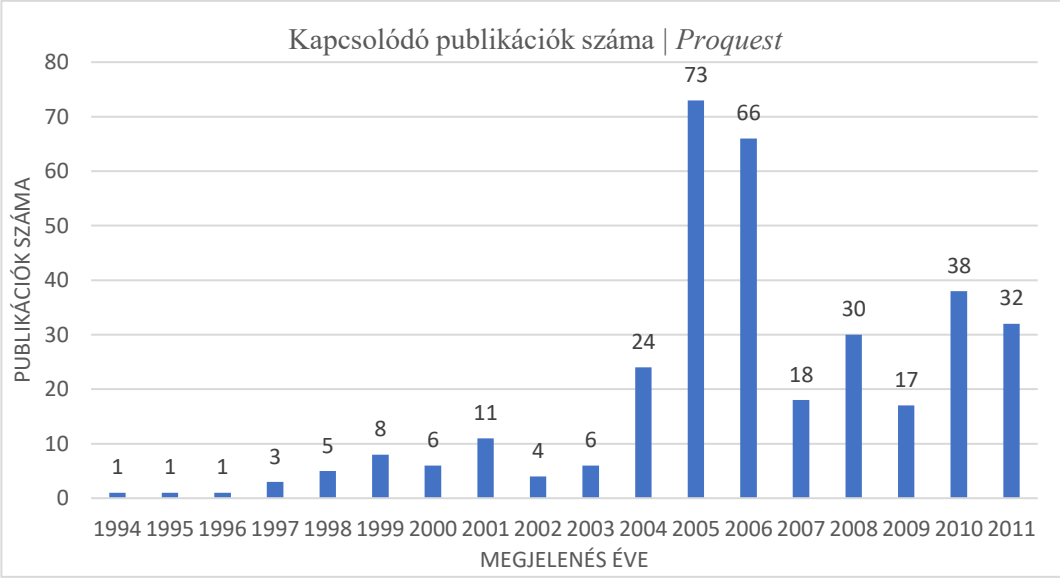
Külföldi kitekintés

Időrendben haladva nem hagyható figyelmen kívül Steele és Lowenthal (mindketten CIA tisztek voltak) 1990-es évek végén publikált oktatókönyve az OSINT-ról, melyben

összegzik a forrásokat, az adatgyűjtés kezelését és integrációját minden forráselemzésben és műveletben. A monográfia elsőként ad részletes áttekintést a nyílt forrású információszerzés és -elemzés különböző technikáiról és módszereiről, egyúttal gyakorlati útmutatást is nyújt azok alkalmazásához. [28] Ennek szükségességét és aktualitását adta az internet tömeges elterjedése és használata, mely új lehetőségeket nyitott az adatokhoz és információkhoz való hozzáférés terén, elősegítve egy nagyobb gyakorlati közösség kialakulását az 1990-es évek közepétől kezdődően.

Az OSINT – és szakirodalmának (2. ábra) – exponenciálisan növekvő szerepét és felhasználását jól mutatja, hogy 2001-ben a NATO egy saját kiadvánnyal, *NATO Open Source Intelligence Handbook* című kézikönyvvel járul hozzá az új tudományág megértéséhez, alkalmazásához. A mű az OSINT e rövid korszak történetében korszakalkotónak tekinthető, mivel a világ egyik legrangosabb szervezet elsőként látja szükségesnek rendszerezni, megfogalmazni, definíciókkal megvilágítani a téma szerteágazó használatát. Nem elhanyagolhatóak a kézikönyv jogi és etikai kérdésekre adott válaszai és ajánlásai, melyek szervezetek, magánszemélyek és a civil szféra számára egyaránt útmutatást jelentenek. [29]

Hasonló nagyságú és jelentőségű – bár nem kifejezetten az OSINT-ról, inkább a hírszerzésről általában, a titkos műveletekről és az ellenhírszerzésről szóló – kézikönyv a 2007-ben megjelent *Handbook of Intelligence Studies* című, közel 400 oldalas kiadvány. A 26 fejezetből álló könyv megjelenéséhez hozzájárult az is, hogy a 2001-es amerikai ikertornyok ellen elkövetett terrorcselekmény és az azt követő iraki tömegpusztító fegyverekről szóló tévedések következtében a hírszerzés folyamatosan helyet kapott a hírekben. Számos tanulmány foglalkozik a hírszerzési ciklus elemzésével annak érdekében, hogy feltárja és megértse az információgyűjtés és -értékelés világszerte jelentkező kihívásait, valamint a kémelhárítással kapcsolatos problémákat. [30] A nyílt forrású információszerzés nélkülözhetetlenségét jelzi a hírszerzési és kémkedési műveletekben, hogy egy önálló fejezet az OSINT-ot mutatja be. [31]



2. Ábra. Az OSINT második korszakának szakirodalmi forrásai Proquest adatbázis alapján. Saját szerkesztés. Forrás: ProQuest Central.

E korszakról megkerülhetetlen Van Puyvelde és Rienzi, nevéhez fűződő tudományos cikk, a *The rise of open-source intelligence*. Elsőként mondja ki, hogy az OSINT immár önálló tudományág. „Azért minősül tudományágnak, mert strukturált tudásanyagon alapul, beleértve a bevált fogalmakat és módszereket. Egy aktív közösség foglalkozik a kapcsolódó szabványok meghatározásával". [32] Definíciókkal határozza meg az OSINT fogalmát és tisztázza a nyílt forrású hírszerzés és nyílt forrású információ közötti határvonalat, illetve három alapvető kihívást tárgyal, amelyekkel az OSINT-gyakorlók szembesülnek: az információtúlterhelést, a megbízhatóságot, valamint az etikai és szabályozási határokat. [32] Legnagyobb vita abban van köztük és Williams Heather között, hogy az internet okozta robbanásszerű információdömping az OSINT fejlődésében forradalmi jelenség, vagy pedig egy evolúciós folyamatnak a következménye? Williams bár mérsékelten fogalmaz, forradalmi fejlődésnek nevezi a nyílt forrású hírszerzés gyors térnyerésének folyamatát, mellyel új fázisba (korszakba) lépett az új tudományág [33]. Van Puyvelde és társa szerint az OSINT térnyerése a hagyományos hírszerzési gyakorlatok fejlődését tükrözi. Megfogalmazása szerint habár a nyílt forrású adatok exponenciális növekedése átalakította a hírszerzési környezetet, ez nem jelenti annak forradalmasítását. Sokkal inkább azt, hogy az államnak meg kell vizsgálnia, hogy hogyan integrálja az OSINT gyakorlatokat, illetve hogyan lehet javítani a digitális írástudást. Az evolúciós folyamat következménye mellett foglal állást Gioe Davis is (2020), amikor azt állítja, hogy „Talán a hírszerzés forradalma még előttünk van" [34]

Magyarország

A magyar szakirodalomban található kutatási eredmények, elemzések egybehangzanak a külföldön megjelentekkel. A szerényebb számú publikációk főleg állam- és nemzetbiztonsági, biztonságtudományi és a bűnügyi szakterülethez kapcsolódó hírszerzést, az OSINT módszertanát, illetve annak történetét fedik le. Ezek közül a legátfogóbb és legrendszerezettebb kiadvány – bár terjedelmét tekintve lényegesen rövidebb, de tömörebb Pilch Jenő művénél – Boda József és Regényi Kund szerkesztésében 2019-ben megjelent *A hírszerzés története az ókortól napjainkig* című szakkönyv. Közel 80 év után megjelent hasonló átfogó mű a témában újra értelmezi a hírszerzés jelentőségét és fontosságát, aktualitást ad és új kontextusba helyezi azt. Fókusza a titkos hírszerzésre, kémkedésre és a titkos információszerzésre irányul, mint az állam és a kormányok eszköze a polgárok és az állam biztonságának védelméért folytatott küzdelemben. Az információt olyan stratégiai és nemzetbiztonsági tényezőként definiálja, mely fegyvert és hatalmat jelent egy adott szervezet vagy kormány kezében. Ennek szellemében részletesen mutatja be egyetemes és magyarországi történetét, fejlődését, működését és változásait a kezdetektől, vagyis az ókortól az 1990-es évek elejéig. [23]

A legtöbb tudományos publikáció e korszakról a Nemzetbiztonsági Szemlében jelent meg. Ezek egy-két kivételtől eltekintve már az OSINT mozaikszót használják következetesen és annak különböző aspektusait mutatják be, de közös elemként jelenik meg majdnem mindegyikben a biztonsághoz – akár adat-, nemzet-, internet- vagy kiberbiztonság stb. – fűződő jelentéstartalom. Bányász Péter korunk legdinamikusabban fejlődő digitális platformjáról, a közösségi médiáról, mint a nyílt forrású információgyűjtés egyik területéről és annak lehetőségeiről ír. Nem véletlen, hogy az ebben rejlő lehetőségeket a nemzetbiztonsági szolgálatok is időben felismerték. [35] Ennek alkalmazását támasztja alá Dihen Mihály cikke is a polgári hírszerzésről [36], amit a nemzetbiztonságról szóló törvény

53 § is rögzít. [37] Czinner Zoltán az internet adta kimeríthetetlen információgyűjtési lehetőségek korlátairól és veszélyeiről egyaránt ír, mivel az OSINT eszközöket alkalmazók ezekre nem mindig fordítanak kellő figyelmet. [38]

Dobák Imre gondolatai rávilágítanak arra, hogy az infokommunikáció területen végbemenő technológiai környezet fejlődése komoly hatást gyakorol a nyílt forrású információszerző eszközök fejlődésére is. Ez elsősorban abban nyilvánul meg, hogy az egyre növekvő információmennyiségből a legrelevánsabb adatok kinyeréséhez, rendszerezéséhez és elemzéséhez egyre fejlettebb informatikai eszközökre és szoftverekre van szükség. Figyelemreméltó azon megállapítása is, hogy az OSINT alkalmazását a biztonságért felelős kormányzati szerveken kívül a gazdasági szereplők is egyre többet használják. Elég, ha a globálisan elterjedt üzleti célú adatgyűjtésre gondolunk. Ezen üzleti-vállalati megoldások ma már önálló piaci szakterületet képeznek. Fontos az adatvédelmi és etikai kérdések felvetése, akárcsak az álhírek, dezinformációk kiszűrése OSINT alkalmazásakor. [39]

A nyílt forrású információszerzés bűncselekmények megelőzésében és felderítésében betöltött szerepét a szakirodalomban többek között Márton Balázs és Nyeste Péter tanulmánya is alátámasztja. A rendvédelmi és bűnüldöző szervek szükség esetén a világhálón elérhető nyílt forrású információkat is felhasználják, amelyek feltárásához és elemzéséhez különféle OSINT-eszközöket és módszereket alkalmaznak. [40, 41] Nemzetbiztonsági szempontból szintén nélkülözhetetlenek a nyílt forrású információk a katonai műveletekben, hiszen ezek felgyorsítják a műveleti információk gyűjtését és magát a döntéshozatalt is. [42]

Gál István László tanulmányában azt a kérdést feszegeti, hogy a nyíltan hozzáférhető adatokból származó információk továbbításával elkövethető-e a kémkedés bűncselekménye? Az érdekes fejtegetés abból indul ki, hogy a kémkedés alapestben bűncselekmény, amit a törvény büntet. A nyílt forrású információk gyűjtése, felhasználása etikai kereteken belül azonban legális. Mégis bűncselekmény elkövetésével szembesülhet az, aki „egy ellenérdekelt titkosszolgálat részére kormányzati, politikai vagy gazdasági információk gyűjtése, elemzése, feldolgozása és továbbítása” következtében kárt okoz az adott államnak. [43]

Korunk egyik sokrétű veszélyforrását a digitális térben megjelenő potenciális bűncselekmények jelentik. A biztonságtudomány egyik fontos feladata, hogy felhívja a felhasználók figyelmét ezekre a kockázatokra. Ennek kapcsán gyakran esik szó a digitális tudatosság jelentőségéről, valamint arról, hogy a rólunk szóló adatok és információk sok esetben gyanútlanul kerülnek fel a világhálóra. Az OSINT-eszközök elterjedésével különösen fontossá válik a körültekintő online jelenlét, hiszen a megfelelő óvatosság hiányában a világhálón hagyott digitális lábnyomok akár beláthatatlan következményekkel is járhatnak. [44]

A nyílt forrású információgyűjtő eszközök vizsgálata kapcsán Solti István rámutat arra, hogy nem tekinthető OSINT-nak az a tevékenység, amely során az információk hackinggel, mások jogosultságainak megszerzésével, illetve szándékos megtévesztő magatartással kerülnek megszerzésre. [45] A nyílt forrású információ minősített OSINT információvá (OSINT-V – Validated OSINT) pedig csak azután válik, ha szakértők által más (akár minősített) forrásból származó tényekkel összevetik és azok megbízhatónak bizonyulnak. [2, 46]

AZ OSINT HARMADIK GENERÁCIÓJA, A SZEMANTIKUS WEB KORSZAKA

2000-es évek elejétől az internet világában jelentős változás veszi kezdetét, ez a szemantikus web diadalútjának kezdete és a mesterséges intelligencia első lépcsőfoka. Ennek lényege, a felhasználó által létrehozott strukturálatlan tartalmak gépi megértése, rendszerezése, az adatok feldolgozása, mélyebb elemzése. Egy olyan tudásgráf, mely megkönnyíti a tartalom, a metaadatok és más információs objektumok gépi megértését és feldolgozását. [47] A gépi tanulás és a mesterséges intelligencia nagyban hozzájárulnak ennek a komplex információszerző és feldolgozó, elemző tevékenységnek a tökéletesítéséhez. Az OSINT eszközeinek használata, a nyílt forrású információk gyűjtése, rendszerezése, elemzése ma már kéz a kézben jár a ML-lel és az AI-val. Erről számos tanulmány, tudományos szakirodalmi forrás tanúskodik.

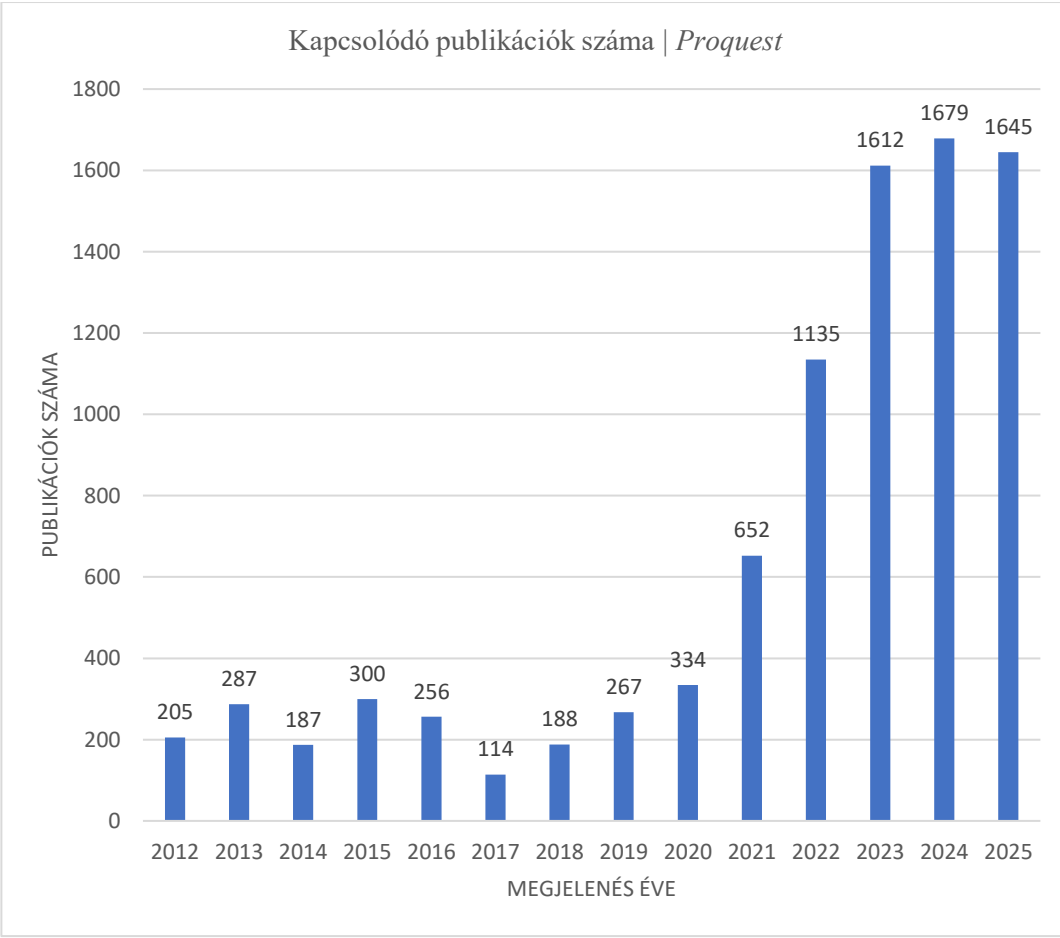
Ezek közül kiemelhető Browne és munkatársai 2024-ben írt *A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications* című tudományos műve. A széleskörű elemzésben (több, mint 160 cikket azonosítottak a témában) olyan OSINT alkalmazásokat vizsgáltak, melyek MI-t és gépi tanulási algoritmusokat használtak. [48] A gépi tanulás utánozza azt, ahogyan az ember tanul. Például adatokat értelmez, következtetéseket von le, kategorizálja őket és elemzéseket végez. Vitathatatlan előnye, hogy sokkal gyorsabb, hatékonyabb és pontosabb az embernél. A mesterséges intelligencia gépek általi emberi intelligencia utánzása, különböző algoritmusokból áll és az emberi gondolkodás bizonyos aspektusait utánozza. Egyik speciális területe a gépi tanulás. E gépi tanulási algoritmusok a természetes nyelv (Natural Language Processing, NLP) feldolgozásában is alkalmazhatóak és képesek tudást és információt kinyerni szöveges adathalmazokból. Ezen technológiák képesek olyan feladatokat ellátni, melyeket korábban csak emberek végeztek. E technikai megoldások skálája napjainkban széleskörű. Az MI előrelépést és új lehetőségeket kínál az OSINT műveletekben használt rendszerek sebességében és hatékonyságában (pl. a téves adatok, információk, félretájékoztatás kiszűrésére is). Digitális világunkban az információk és adatok növekedése, tárolása, feldolgozása exponenciálisan nő. Ebben a környezetben az MI és az OSINT kombinációja egy merőben új eszköz az OSINT műveletek számára. Ennek tükrében a gépi tanulás és az MI integrálása az OSINT eszközökbe új módszereket kínál. Automatizál és lehetővé tesz hatalmas mennyiségű adatfeldolgozást, felgyorsítja a vizsgálatokat és hozzájárul a gyűjtés, elemzés hatékonyságához. A témában megjelent tudományos cikkek eredményei alapján megállapítható, hogy az OSINT és az MI összekapcsolása dinamikusan növekvő kutatási terület, mely a jövőben kétséget kizáróan további eredményeket és innovatív megoldásokat fog hozni. [48]

Az OSINT és a MI kapcsolatát, integrált használatát, a nagy nyelvi modellek (Large Language Models, LLM) alkalmazását vizsgálja, a MI és kapcsolódó tevékenységek (pl. prompt engineering) jelentőségét elemzi Jan Cerny (2024*) Prompt Engineering: Tactics and Techniques in Open-Source Intelligence* című tanulmánya. Kutatása eredményeként megállapítható, hogy az MI OSINT használatakor nemcsak a világhálón megjelenő bármilyen adat elérhetőségében nyújt segítséget, hanem a gyors és hatékony adat- és információgyűjtésben, rendszerezésben és elemzésben is. [49]

Ghioni Riccardo és társai egy alapos, átfogó szakirodalmi elemzéssel értékelték közel 600 publikáción keresztül az MI-alapú OSINT valamint az OSINT-szoftverek fejlesztésének jelenlegi állását. Az MI és az OSINT integrációjáról szóló kutatásokról egyre nagyobb számú szakirodalomi forrás jelenik meg és ez a jövőben meghatározó lesz. [50]

Az AI használata OSINT információgyűjtéskor olyan egyedi megoldásokra is képes, mint a képfelismerés, illetve a képen szereplő személyek azonosítása. Dane és Verhoef a 20. század legelejéről származó képek esetében alkalmazták. Három különböző csoportképeken látható személyeket és azok szerepét azonosították sikerrel. [51] Az MI alkalmazása az OSINT használatakor tehát nemcsak az információszerzés gyorsaságát, feldolgozását és hatékonyságát növeli, de a szövegbányászat és a képfelismerés, az azokban lévő összefüggések keresésére és elemzésére egyaránt alkalmazható. [52]

A lentebbi ábra is jól szemlélteti, hogy az OSINT harmadik korszakában a szakirodalmi források megjelenésének tekintetében egy számszerűen stabil (a korszak első felében), majd egy exponenciális emelkedés (a korszak második felében) következik be.



3. Ábra. Az OSINT harmadik korszakának szakirodalmi forrásai Proquest adatbázis alapján. Saját szerkesztés. Forrás: ProQuest Central.

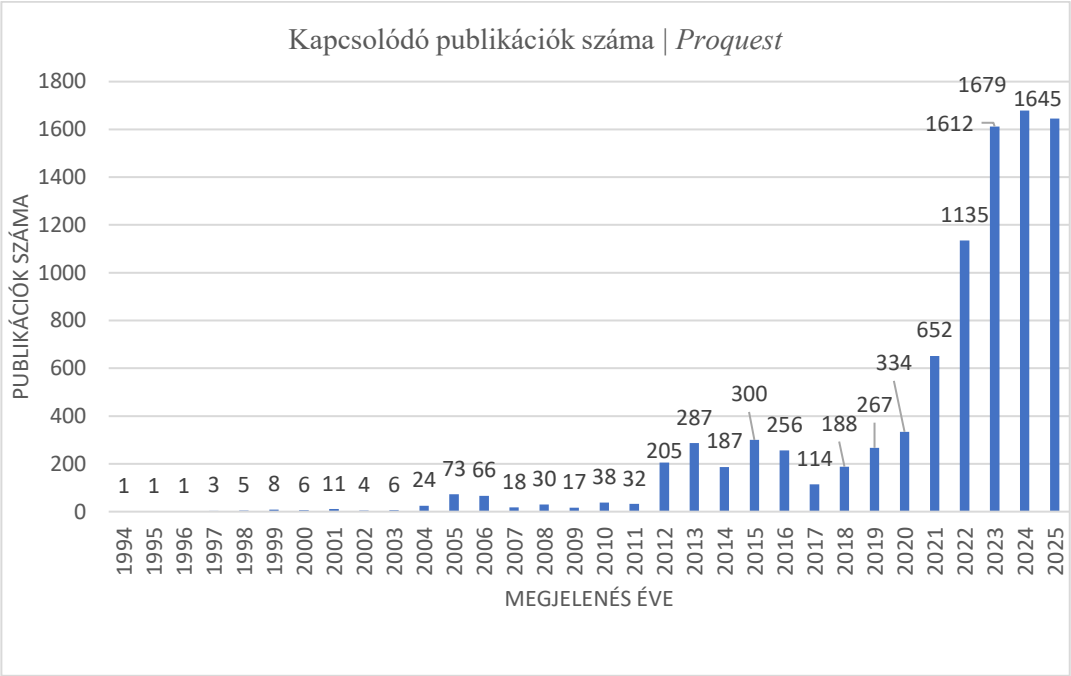
Területek, melyen kiemelkedően alkalmazzák az OSINT-ot

Nemzetbiztonsági szolgálatok feladata alapvetően megkívánja, hogy a legspeciálisabb eszközöket használják széleskörű információforrások kiaknázására. A bűnüldöző szervek ennek megfelelően akár a kereskedelmi forgalomban lévő adatokat is használhatják (például mobiltelefon-felhasználók helyadatait). Ez alapvető jogokat sérthet, például személyes adatok védelmének a jogát, azonban az állam meghatározza a hírszerzési szakemberek számára, hogyan használják fel jogszerűen a kereskedelmi forgalomban elérhető információkat a nemzetbiztonság védelme érdekében. Ennek lényege, hogy meg kell teremteni a nemzetbiztonság és a magánélet közötti egyensúlyt. [53]

A terrorizmus vitathatatlanul napjaink egyik globális problémája, mely ellen minden eszközzel küzdenek a nemzetbiztonsági szervek. Nem meglepő, hogy ezen szervezetek a leghatékonyabb és legmodernebb információszerzési eszközöket, módszereket és technikákat alkalmazzák. Ezek pedig az MI támogatott OSINT eszközök. [54, 55] Ám ezeket sajnos nemcsak az állami, nemzetbiztonsági szervezetek használják, hanem sokszor a különböző terrorcsoportok maguk is bizonyos célpontok kiválasztásakor, sok esetben például egészségügyi intézmények vagy azok dolgozói ellen. [56, 57]

Korunk másik figyelmet érdemlő területe, melyen az AI alapú OSINT használata nélkülözhetetlen az egyre kifinomultabb kibertámadások, különösképpen ott, ahol a rendszerek összekapcsolódnak egymással. Az automatizált OSINT elemzés praktikus módszert kínál a szervezetek számára támadási felületeik átláthatóságára. [58] Az OSINT eszközök olyan kiberbiztonsági feladatok elvégzéséhez is használhatóak, mint behatolási teszteléshez, hálózati elemzéshez, fenyegetés-információkhoz, potenciális fenyegetési vektorok azonosításához stb. [59] Egy erre a feladatra létrehozott nyílt forráskodú hírszerzési OSINT eszköz például az InfoCrawler, melyet információgyűjtésre és ember által olvasható jelentések készítésére terveztek kiberbiztonság területen. Az InfoCrawler automatizálja a nyilvánosan elérhető adatok gyűjtését és elemzését olyan technikák alkalmazásával, mint a webes feltérképezés, webes adatgyűjtés, adatbányászat és az adatok vizualizálása. Vagyis az InfoCrawler egy olyan innovatív OSINT eszköz mely kiberbiztonság területen információgyűjtéssel és az ember által olvasható jelentésekkel foglalkozik. [60]

Fentieken túl az OSINT-ot ma már számos társadalmi kihívás és bűncselekmény kezelésére is alkalmazzák. Például környezetkárosítás, az emberi jogok megsértése, a gyermekek kizsákmányolása, a családon belüli erőszak, katasztrófák vagy éppen az eltűnt személyek felkutatása során. [61] Nem elhanyagolható az orvostudomány epidemiológiai tudományterületen betöltött, nélkülözhetetlen szerepe sem az AI-al összekapcsolt OSINT használatának, különös tekintettel a járványok kitörésében, felkutatásában és terjedésük megelőzésében. [62]. Kiváltképp akkor fontos ez, amikor ki kell szűrni a hamis adatokat is, hogy a szándékos dezinformáció ne vonjon el fölösleges energiát és erőforrásokat, melyet így a szükséges ellátásra lehet fordítani. [63]



4. Ábra. Az OSINT szakirodalmi forrásainak alakulása a világháló tömeges elterjedésétől napjainkig. Saját szerkesztés. Forrás: ProQuest Central.

Az OSINT témában kiemelten fontosok a közösségi média Youtube felületén található streaming anyagok, melyek nemcsak magát az OSINT-ot mutatják be és értelmezik [64, 65], de annak eszközeiről és hatékony használatukról technikai megoldásokat kínálnak a gyakorlati felhasználók számára, oktatási tanfolyamok keretén belül. [66, 67]

Az OSINT fejlődési ívét vizsgálva, a három korszak szakirodalmát összességében nézve (lásd 4. ábra) kijelenthető, hogy a második – jellemzően még enyhe növekedést mutató – korszakot követően, a szemantikus web (a harmadik) korszakának elején ugyan még stagnáló fejlődés figyelhető meg (az előző korszakhoz képest lényegesen magasabb, de hullámzó). Azonban a korszak második felében a gépi tanulás és a mesterséges intelligencia elterjedésével egy exponenciálisan növekvő, stabil, robbanásszerű fejlődés indul el az OSINT szakirodalmában. Ennek tükrében nem vitatható, hogy az ML és az AI meghatározó lesz a nyílt forrású információszerzés jövőbeni fejlődésében is.

KÖVETKEZTETÉSEK

Az OSINT és előzményeinek áttekintett szakirodalmi forrásai tükrében megállapítható, hogy a nyílt forrású információszerzés jelentős változásokon ment keresztül az évezredek során. Kezdetekben főleg háborús időszakban, az ellenség szándékainak és erőforrásainak feltérképezésére használták. A későbbiekben már békeidőben is szerepet kapott, de pontosabb és hitelesebb információk beszerzése érdekében kiegészült a titkos hírszerzéssel és kémkedéssel. Az állam- és biztonságvédelmi szervek mindenkori feladata, hogy széles körű információszerzéssel és annak teljes eszköztárával elősegítsék a döntéshozatalt a pol-

gárok biztonságának megőrzése érdekében. A 20. század közepén elindult a nyílt információszerzés intézményesítése, melynek következtében az OSINT egyre nagyobb figyelmet kapott. Igazi áttörést az 1990-es évek eleje hozott, amikor megjelent a napjainkban is használt OSINT mozaikszó, változott jelentéstartalma, ezzel együtt a szakirodalma is sokkal nagyobb ütemben fejlődött. Ennek aggregátora egyrészt az információs technológia robbanásszerű fejlődése, másrészt – és ennek sokkal nagyobb szerepe volt – a világháló megjelenése és elterjedése. Ez és az információ volumenének exponenciális bővülése, gyors hozzáférhetősége további jelentésbővülést hozott, kialakultak szakágai, melyeket egymástól elkülönülve használnak. Az OSINT maga már nem pusztán a szabadon elérhető információk gyűjtését jelenti, hanem egy tágabb fogalom, mely egy komplex tevékenységet, annak minden fázisát tartalmazza. A számítógép, a gépi tanulás és a mesterséges intelligencia e tevékenység hatékonyságát növelte, eszközeit tökéletesítette. Immár a polgárok biztonságának különböző aspektusain túl a gazdasági-, üzleti- és a civil szféra egyaránt használja saját érdekei és céljai elérésére. Elmondható, hogy az OSINT behatárolt mindhárom korszakában a biztonsági aspektus a közös jellemző.

A témában napjainkban is megjelenő kutatások, a növekvő szakirodalmi források bizonyítják, hogy az OSINT iránti érdeklődés növekedőben van tekintettel azokra az előnyökre, melyeket minden területen nyújt. Ezek lehetővé teszik a kockázatokra és fenyegetésekre adott valós idejű reakciók generálását a világhálón elérhető adatok, információk és források mennyiségének maximális kihasználásával. Ezek összességzéseként elmondható, hogy az OSINT előtt ígéretes jövő áll különböző alkalmazási területeken. [68] Mindez önmagában is vitathatatlan aktualitást és létjogosultságot ad új tudományágként való aposztrofálásának.

FELHASZNÁLT IRODALOM

[1] R. D. Steele, "Intelligence in The 1990's: Recasting National Security in a Changing World," American Intelligence Journal, vol. 11, no. 3, pp. 29-36, 1990. [Online]. Available: http://www.jstor.org/stable/44326352 (accessed January 06, 2026.)

[2] Y-W. Hwang, I.-Y. Lee, H. Kim, H. Lee, and D. Kim, "Current Status and Security Trend of OSINT," Wireless Communications and Mobile Computing, vol. 2022, no. 1, p. 1290129, 2022/01/01 2022, doi: 10.1155/2022/1290129.

[3] S. Legg and M. Hutter, "A Collection of Definitions of Intelligence," Advances in Artificial General Intelligence: Concepts, Architectures and Algorithms, vol. 157, 07/25 2007.

[4] J. Kis-Benedek, "Az OSINT alkalmazása a diplomáciában," in Gazdaságdiplomácia - Elmélet és gyakorlat felkészülő diplomatáknak, S. G. Nagy and G. Kutasi Eds.: Akadémiai Kiadó, 2020.

[5] V. Scuro, "Open-Source Intelligence (OSINT) for Researchers and Practitioners," Researching a Rigged Game: Digital Approaches to Tracing the Illicit Trade in Cultural Objects, E. Smith and S. Austin, Eds., London: Springer, 2026, pp. 11-28.

[6] Espionage Act of 1917. "Espionage Act of 1917 and Sedition Act of 1918 (1917-1918)." Congress. National Constitutional Center. https://constitutioncenter.org/the-constitution/historic-document-library/detail/espionage-act-of-1917-and-sedition-act-of-1918-1917-1918 (accessed February 03, 2026.)

[7] "2012. évi C. törvény a Büntető Törvénykönyvről." XXIV. fejezet 261 §. https://net.jogtar.hu/jogszabaly?docid=a1200100.tv (accessed February 03, 2026.
[8] R. Mennevée, L'espionnage international en temps de paix -Tome II. (no. 1. k.). Chez l'auteur, 1929.
[9] W. Donovan. (1946) Intelligence: Key to Defense. Life Magazine. 108-121.
[10] R. D. Steele, "National Intelligence and Open Source: From School House to White House," American Intelligence Journal, no. Special Issue, pp. 29-32, 1993.
[11] C. Andrew, The Secret World: A History of Intelligence. New Haven: Yale University Press, 2018.
[12] N. Kent, "The Secret World: A History of Intelligence," The RUSI Journal, vol. 164, no. 1, pp. 86-93, 2019/01/02 2019, doi: 10.1080/03071847.2019.1605039.
[13] R. L. Baker, Deep dive: Exploring the real-world value of opensource intelligence. Indianapolis: John Wiley and Sons, 2023.
[14] L. Block, "The long history of OSINT," Journal of Intelligence History, vol. 23, no. 2, pp. 95-109, 2024/05/03 2024, doi: 10.1080/16161262.2023.2224091.
[15] J. Zhou, "Open-source intelligence and great-power competition under mediatization," (in English), Security Journal, vol. 37, no. 4, pp. 1769-1786, Dec 2024 2024, doi: 10.1057/s41284-024-00446-0.
[16] M. Glassman and M. J. Kang, "Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)," Computers in Human Behavior, vol. 28, pp. 673-682, 03/01 2012, doi: 10.1016/j.chb.2011.11.014.
[17] F. Schaurer and J. Störger, "The Evolution of Open Source Intelligence," The Intelligencer. Journal of U.S. Intelligence Studies, vol. 19, no. 3, pp. 53-56, 2013, doi: 10.3929/ethz-a-006251404.
[18] E. Borges, "What Is Open Source Intelligence (OSINT)?," in Recorded Future Blog vol. 2025.12.12., ed, 2024.
[19] J. Pilch, A hírszerzés és kémkedés története I-III. Franklin Társulat, 1936.
[20] N. P. Nándori, "Szakmatörténeti forrásajánló," Nemzetbiztonsági Szemle, vol. 7, no. 1, pp. 106-110, 2019, doi: 10.32561/nsz.2019.1.8.
[21] G. Ónodi, A hírszerzés története - Ókor, középkor, újkor. Útmutató Kiadó, 1994.
[22] J. Piekalkiewicz, A kémkedés világtörténete I-II. Zrínyi Kiadó, 1997.
[23] J. Boda and K. Regényi, Eds. A hírszerzés története az ókortól napjainkig. Dialóg Campus, 2019.
[24] K. M. Regényi, "OSINT a második generációs internetet megelőző korokban," Nemzetbiztonsági Szemle, vol. 7, no. 2, pp. 32-37, 2019, doi: 10.32561/nsz.2019.2.3.
[25] S. B. Dobrow. "Rise of the Internet and the World Wide Web." EBSCO. https://www.ebsco.com/research-starters/history/rise-internet-and-world-wide-web (accessed February 03, 2026.)
[26] V. Schafer and B. Thierry, "The 90s as a turning decade for Internet and the Web," Internet Histories, vol. 2, pp. 1-5, 12/27 2018, doi: 10.1080/24701475.2018.1521060.
[27] "Internet history of 1990s." Computer History. https://www.computerhistory.org/internethistory/1990s/ (accessed February 03, 2026.)
[28] R. D. Steele and M. Lowenthal, Open Source Intelligence: Executive Overview. OSS Academy, 1998.

[29] North ATlantic Treaty Organzation, Open Source Intelligence Handbook: North ATlantic Treaty Organzation (NATO), 2001.
[30] L. K. Johnson, Ed. Handbook of Intelligence Studies. London: Routledge, 2007.
[31] R. D. Steele, "Open source intelligence," Handbook of Intelligence Studies, L. K. Johnson, Ed.: Routledge, 2007, pp. 129-147.
[32] D. Van Puyvelde and F. Tabárez Rienzi, "The rise of open-source intelligence," European Journal of International Security, pp. 1-15, 2025, doi: 10.1017/eis.2024.61.
[33] H. Williams and I. Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. 2018.
[34] D. Gioe, M. Goodman, and T. Stevens, "Intelligence in the Cyber Era: Evolution or Revolution?" Political Science Quarterly, vol. 135, pp. 191-224, 06/01 2020, doi: 10.1002/polq.13031.
[35] P. Bányász, "A közösségi média, mint a nyílt forrású információszerzés fontos területe," Nemzetbiztonsági Szemle, vol. 3, no. 2, pp. 21-36, 2015.
[36] M. Dihen, "A magyar polgári hírszerzés előtt álló kihívások a 21. század elején," Nemzetbiztonsági Szemle, vol. 8, no. 1, pp. 47-61, 2020, doi: 10.32561/nsz.2020.1.3.
[37] "1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról." https://net.jogtar.hu/jogszabaly?docid=99500125.tv (accessed February 03, 2026.)
[38] Z. Czinner, "Az OSINT határai," Nemzetbiztonsági Szemle, vol. 7, no. 2, p. 1931, 2019, doi: 10.32561/nsz.2019.2.2.
[39] I. Dobák, "OSINT. Gondolatok a kérdéskörhöz," Nemzetbiztonsági Szemle, vol. 7, no. 2, p. 8393, 2019, doi: 10.32561/nsz.2019.2.7.
[40] B. Márton, "A nyílt forrású hírszerzés (OSINT) mint lehetőség a bűncselekmények felderítésében. A rendőrségen belüli önálló OSINT egység koncepciója," Belügyi Szemle, vol. 71, no. 8, pp. 1419-1435, 2023, doi: 10.38146/BSZ.2023.8.
[41] P. Nyeste, "Bűnügyi OSINT," in A bűnügyi hírszerzés kézikönyve, P. Nyeste and F. Szendrei Eds.: Dialóg Campus, 2019, pp. 210-220.
[42] E. Vattai, "A nyílt forrású információszerzés kapcsolata a hadsereggel," Hadmérnök, vol. 18, no. 2, pp. 155-165, 2023, doi: 10.32567/hm.2023.2.10.
[43] I. L. Gál, "Az OSINT (Open Source Intelligence) mint a kémkedés lehetséges elkövetési magatartása," JURA, vol. 20, no. 1, pp. 51-55, 2014.
[44] T. J. Molnár, "Az internetes biztonság és az OSINT összefüggései," Nemzetbiztonsági Szemle, vol. 9, no. 2, pp. 81-94, 2021, doi: 10.32561/nsz.2021.2.6.
[45] I. Solti, "Az OSINT információgyűjtő estközeiről," Nemzetbiztonsági Szemle, vol. 7, no. 2, pp. 3-18, 2019, doi: 10.32561/nsz.2019.2.1.
[46] C. Vida, "Nyílt forrású adatszerzés (OSINT)," in A nemzetbiztonság elmélete a közszolgálatban, I. Resperger Ed.: Dialog Campus, 2018, pp. 133-141.
[47] L. A. Tölgyes. "A szemantikus web története." ITC Global. https://ictglobal.hu/iparagi-megoldasok/a-szemantikus-web-tortenete/ (accessed February 03, 2026.
[48] T. O. Browne, M. Abedin, and M. J. M. Chowdhury, "A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications," International Journal of Information Security, vol. 23, no. 4, pp. 2911-2938, 2024/08/01 2024, doi: 10.1007/s10207-024-00868-2.
[49] J. Černý, "Prompt Engineering: Tactics and Techniques in Open-Source Intelligence," (in English), Journal of Information Warfare, vol. 23, no. 3, pp. 115-135, 2024 2024.

[Online]. Available: https://www.proquest.com/scholarly-journals/prompt-engineering-tactics-techniques-open-source/docview/3115798186/se-2?accountid=32048 (accessed January 06, 2026.)
[50] R. Ghioni, M. Taddeo, and L. Floridi, "Open source intelligence and AI: a systematic review of the GELSI literature," AI & SOCIETY, vol. 39, no. 4, pp. 1827-1842, 2024/08/01 2024, doi: 10.1007/s00146-023-01628-x.
[51] J. Dane and C. Verhoef, "Who's that lady? — Applying open source intelligence in a history context," Endeavour, vol. 48, no. 4, pp. 1-40, 2024/12/01/ 2024, doi: 10.1016/j.endeavour.2024.100967.
[52] I. Szabadföldi, "A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT) - evolúció és kihívások," Nemzetbiztonsági Szemle, vol. 10, no. 1, p. 3051, 2022, doi: 10.32561/nsz.2022.1.3.
[53] J.-J. Oerlemans and S. Langenhuijzen, "Balancing National Security and Privacy: Examining the Use of Commercially Available Information in OSINT Practices," International Journal of Intelligence and CounterIntelligence, vol. 38, no. 2, pp. 579-597, 2025/04/03 2025, doi: 10.1080/08850607.2024.2387850.
[54] J. Andric and M. Terzić, "Intelligence Cycle In The Fight Against Terrorism With Usage Of Osint Data," International Journal of Information and Operations Management Education, vol. 17, pp. 1-16, 05/01 2023.
[55] C. Raluca, "Open Source Intelligence: Opportunities And Challenges" Strategic Impact, no. 74, pp. 95-109, 2020. [Online]. Available: https://www.ceeol.com/search/article-detail?id=884892 (accessed March 03, 2026.)
[56] J. Besenyő, D. G. Barten, H. G. De Cauwer, D. Tin, and A. Gulyás, "A Review of Ambulance Terrorism on the African Continent," Prehospital and Disaster Medicine, vol. 38, no. 2, pp. 237-242, 2023, doi: 10.1017/S1049023X23000213.
[57] J. Besenyő and R. and Shaffer, "Terrorism against healthcare facilities and workers in Africa: An assessment of attack modes, targets and locations," African Security Review, vol. 32, no. 3, pp. 311-331, 2023/07/03 2023, doi: 10.1080/10246029.2023.2213220.
[58] T. Babenko, K. Kolesnikova, O. Abramkina, and Y. Vitulyova, "Automated OSINT Techniques for Digital Asset Discovery and Cyber Risk Assessment," (in English), Computers, vol. 14, no. 10, p. 430, 2025 2025, doi: 10.3390/computers14100430.
[59] L. Ball, G. Ewan, and N. Coull, "Undermining: Social engineering using open source intelligence gathering," in Proceedings of the 4th International Conference on Knowledge Discovery and Information Retrieval. Barcelona, Spain, 2012, pp. 275-280.
[60] K. Z. Christos, "Information Gathering Software OSINT implementation [PhD Thesis]," Thesis, European University of Cyprus, 2023.
[61] E. Dincelli, C. Van Slyke, and A. Yayla, "Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools," Communications of the Association for Information Systems, no. 53, pp. 1052-1071, 2023, doi: 10.17705/1CAIS.05345.
[62] F. Tampu and L. Berek, "A nyílt forrású hírszerzés (OSINT) lehetséges hasznosítása az orvostudomány közegészségügyi-járványügyi szektorában," Orvosi Hetilap, vol. 166, no. 32, pp. 1250–1255, 2025, doi: 10.1556/650.2025.33370.

[63] S. M. Martinez Monterrubio, A. Noain-Sánchez, E. Verdú Pérez, and R. González Crespo, "Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source through OSINT, the verifier tool for official journals," (in eng), Information Sciences, vol. 574, pp. 210-237, Oct 2021, doi: 10.1016/j.ins.2021.05.074.
[64] Biztonsági Akadémia. "Nyílt forrású információszerzés (OSINT) kurzus bevezető." Youtube. https://www.youtube.com/watch?v=SmjuUckJfQE (accessed 2026.01.06.)
[65] OSINT Dojo. "OSINT Introduction: What is Open Source Intelligence?" Youtube. https://www.youtube.com/watch?v=Sa5LbKqCmFI (accessed February 02, 2026.)
[66] Biztonsági Akadémia. "OSINT eszközök és keretrendszer alkalmazása." Youtube. https://www.youtube.com/watch?v=ATjJIPrj1SA (accessed January 06, 2026.)
[67] H. Adams. "Open-Source Intelligence (OSINT) in 5 Hours - Full Course - Learn OSINT!" Youtube. https://www.youtube.com/watch?v=qwA6MmbeGNo (accessed January 06, 2026.)
[68] J. F. Herrera-Cubides, P. A. Gaona-García, and S. Sánchez-Alonso, "Open-Source Intelligence Educational Resources: A Visual Perspective Analysis," Applied Sciences, vol. 10, no. 21, p. 7617, 2020, doi: 10.3390/app10217617

DOI: https://doi.org/10.12700/btsz.2026.8.2.61

THE DEVELOPMENT OF THE LOCKOUT-TAGOUT METHODOLOGY AND ITS POSSIBLE NEXT STAGE

A KIZÁRÁS-KITÁBLÁZÁS MÓDSZERTAN KIALAKULÁSA ÉS LEHETSÉGES KÖVETKEZŐ SZINTJE

MAREK Bence Attila[1] – BRAUN András[2]

Abstract

With the development of industry, machines and occupational safety, humanity has recognized new and new sources of danger, for which it has learned to implement countermeasures. This is how the machines and their dangerous, possibly stored energies were identified, for which the (Lock Out - Tag Out, LOTO) methodology was developed as a countermeasure. LOTO plays a key role in the operation of today's modern and safe factories. However, as technology advances, we need to recognize new ways and opportunities, as the current level of development of the methodology does not differ much from the procedure and toolkit defined by OSHA in 1982. The purpose of the study is to present a possible new way to use LOTO safely.

Keywords

Lock Out - Tag Out, augmented reality, digitalization

Absztrakt

Az ipar, a gépek és ezek mellett a munkavédelem fejlődésével sorra új és új veszélyforrásokat ismert fel az emberiség, melyekre megtanult ellenintézkedéseket végrehajtani. Így kerültek azonosításra a gépek és azok veszélyes, esetleg tárolt energiái, melyekre ellenintézkedésként kialakításra került a kizárás-kitáblázás (Lock Out - Tag Out, röviden LOTO) módszertan. A LOTO kulcsfontosságú szerepet játszik napjaink modern és biztonságos gyárainak működésében. Azonban a technológia fejlődésével fel kell ismernünk az új utakat és lehetőségeket, hiszen a módszertan jelenlegi fejlettségi szintje nem sokban tér el az OSHA által 1982-ben meghatározott eljárástól és eszközkészlettől. A tanulmány célja, hogy bemutasson egy lehetséges új módot a LOTO biztonságos használatára.

Kulcsszavak

Kizárás - Kitáblázás, kiterjesztett valóság, digitalizáció

[1] redder.mb@gmail.com | ORCID: 0009-0004-6028-3134 | Military and Safety Technology Engineer, Occupational Health And Safety Engineer, Certified Security Engineer, Opella Healthcare Hungary Kft. | Had- és biztonságtechnikai mérnök, Munkavédelmi szakmérnök, Okleveles biztonságtechnikai mérnök, Opella Healthcare Hungary Kft.

[2] braun.andras92@stud.uni-obuda.hu | ORCID: 0009-0008-3958-5751 | PhD Student, Doctoral School on Safety and Security Sciences Óbuda University | Doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Napjainkban a munkahelyek többségében megállapítható, hogy sokszínű géppark támogatja a termelés minél hatékonyabb folyamatosságát, valamint annak fejlesztését. Ezen gépek túlnyomó többsége rendelkezik olyan résszel, funkcióval vagy a működéshez szükséges energiával, amelyek az emberek épségére, illetve életére közvetlen veszélyt jelentenek, azaz ezen területek érintése balesetet eredményez. A XX. század végére a baleseti statisztikák már egyértelműen indokolták, hogy a szabályozó szervek fellépjenek az adott korszak egyik legjelentősebb veszélyforrása ellen. A United Auto Workers (UAW) felmérése szerint 1973 és 1995 között a halálos balesetek 20%-ának (414 esetből 83-nak) a kiváltó oka a veszélyes energiaforrások nem megfelelő izolálása volt. Ennek okán 1989-ben kiadták az OSHA 29 CFR 1910.147 előírást, mely már konkrét elvárásokat támasztottak közvetlenül a LOTO rendszer irányába, ezzel az eszköz központi elemévé válva. Ezen szabályok eredményességét igazolandó, hogy az USA területén a legfrissebb, 2025-ös adatok szerint a halálos áldozatok számát (dedikáltan LOTO használatra visszavezetve) közel a felére, 48-re tudta csökkenteni. Miután az USA területén bevált gyakorlattá vált, nemzetközi standard is készült belőle, mely az ISO 14118 számot kapta, témáját tekintve pedig a gépek váratlan indításának megelőzése. Ez a szabvány gyakorlatilag az európai LOTO alapjait foglalja magába:

- váratlan indítás megakadályozása,
- energiaforrások leválasztása,
- ember - gép kapcsolat biztonsága,
- visszaállítás és újraindítás szabályozása.

Magyarországon először az 1993. évi XCIII. törvény fogalmazta meg implicit módon a LOTO igényét: [1]

Azonban maga a gyakorlat az 1980-as évek óta nem sokat változott. Ugyanúgy papíralapon található energiakizárási utasítások alapján helyezik fel a munkavállalók a kizáró eszközöket, valamint papíron vagy digitális formában, de maguk viszik fel, hogy mely lakatokat helyezték fel, vagy mely pontokat zárták ki.

Jelen tanulmány tárgya ezen folyamat részletesebb bemutatása, valamint a folyamat fejlesztésére egy potenciális lehetőség bemutatása, amely használja a 21. század technológiai vívmányait is.

A VESZÉLYES ENERGIA ÉS LOTO, MINT FOGALOM MEGHATÁROZÁSA

Az alapelv kimondja: az energiaforrást fizikailag el kell választani, rögzíteni kell (lock out) és figyelmeztető jelöléssel (tag out) kell ellátni, mielőtt bárki a veszélyzónában munkát végez. Azaz Isolate-Lock-Tag-Verify (leválasztás-lezárás-jelölés-ellenőrzés). [2]

Ahogy az a bevezetésben is említésre került, az eljárás szerves részét képezi az összes, a biztonságot szem előtt tartó termelési szervezet mindennapjainak. A jelenlegi egyik legfrissebb, 2023-as felmérési adatok alapján elmondható, hogy a Brady összesítése szerint 2177 szabályszegésből 190 halálos áldozat volt, melyből 142 elektromos áram általi esetre volt visszavezethető. [3] Másrészről a National Safety Council statisztikái szerint (Nemzeti Biztonsági Tanács - NSC) 48 halálos balesetet mért a LOTO-hoz kapcsolódóan. Ezen számok alapján megállapíthatjuk, hogy a vizsgált évben valahol 49 és 190 fő között lehetnek

az áldozatai olyan baleseteknek, ahol egy megfelelően alkalmazott LOTO eljárás alkalmazása megelőzhette volna a balesetet. [4] Az OSHA 29 CFR 1910.147(b) szerint 7 fő kategóriát különböztetünk meg: elektromos-, mechanikus-, hidraulikus-, pneumatikus-, termikus-, kémiai-, illetve keverék (egyéb) energiák léphetnek fel. [2]

Ezen kategóriákra a gyakorlat és a vonatkozó szabványok alkottak alkategóriákat, melyek közül néhány példa alább látható:

1. Elektromos energia (kockázatok például: áramütés, ívkisülés, váratlan indulás):
    - hálózati feszültség
    - vezérlőáramkörök,
    - elektromagnetika,
    - elektrosztatikus feltöltődés.
2. Mechanikus energia (kockázatok például: beszorulás, zúzódás, amputálás):
    - mozgó alkatrészek,
    - forgó tengelyek,
    - magas nyomás,
    - gravitáció.
3. Hidraulikus energia (kockázatok például: váratlan mozgás, nagy nyomású befecskendezés):
    - nyomás alatt lévő olaj,
    - hidraulikus hengerek,
    - emelőberendezések.
4. Pneumatikus energia (kockázatok például: alkatrész vagy folyadék kilövellése, hirtelen mozgás):
    - sűrített levegő,
    - gáznyomás,
    - vákuumrendszerek.
5. Termikus energia (kockázatok például: égés, fagyás, robbanás):
    - forró felületek,
    - gőzrendszerek,
    - olvadt anyagok,
    - kriogén rendszerek.
6. Kémiai energia (kockázatok például: mérgezés, égés, robbanás):
    - reakcióképes anyagok,
    - savak, lúgok,
    - gyúlékony anyagok,
    - mérgező gázok.

Fontos kiemelni, hogy ezen lista nem található meg összeszedve egy leiratban sem, illetve ISO 12100 szerint a kategóriák hasonlóan, de kicsit eltérve épülnek fel: mechanikus-, elektromos (1. ábra) -, termális-, zaj-, vibráció-, sugárzás-, anyag/kémiai-, ergonómiai-, gépkörnyezetéhez kapcsolódó kockázatok, illetve ezen elemek keveredése. [5] Elmondható, hogy ezen kategorizálás már modernebb, előre mutató és jobban fedi az EGR (ember-gép-rendszer) szempontokat, mint a klasszikus kategóriák.

1. ábra: Kizárás a gyakorlatban, a szerzők szerkesztése

Ha LOTO-ról beszélünk, akkor fontos említeni a Zero Energy State (Energiamentes állapot) [2] fogalmát is, amely a LOTO célja, valamint elvárt eredménye az OSHA szerint: a gép olyan állapotba hozása, amikor minden veszélyes energia megszűnt vagy biztonságos kontroll alatt van, ezért a berendezés nem képes váratlan veszélyes működésre. [2] Ezen állapot elérése mandatoriális a biztonságos munkavégzés érdekében.

Munkavégzés során a tapasztalat azt mutatja, hogy ezen elvek hiánytalan betartása mennyire is fontos: több esetben, régebbi rendszereken telepített kizárási pontok használata esetén nem szűnt meg a veszélyes energia vagy később újra tudott indulni (például: melegvíz vezeték az elzárást követően - órákkal később is forró volt tapintásra). [6]

JOGSZABÁLYI ÉS SZABVÁNYI HÁTTÉR KIALAKULÁSA, FEJLŐDÉSE

Amerikai Egyesült Államok jogszabályi és szabványi rendszere

Az Amerikai Egyesült Államok területén a legfőbb, illetve legelső szabályozó az OSHA volt, amely megalkotta az OSHA 29 CFR 1910.147 [2] előírását a gyakorlati tapasztalatok alapján- Viszont a hatóság előtt az ipar már a szükséges mérnöki gyakorlatot a(z) ANSI/ASSE Z244.1 [7] szabvány formájában (American National Standard Institute - Amerikai Nemzeti Szabványügyi Intézet: ANSI, American Society of Safety Engineers (napjainkban Professionals) - Amerikai Biztonságtechnikai Mérnökök (napjainkban szakemberek) Társasága - ASSE (ASSP)) meghatározta, mely pontos neve Control of Hazardous Energy (Veszélyes Energiák Szabályozása). Az ipar gyorsabban reagált, mint a hatóság, meghatározva ezzel a legjobb gyakorlatot, amit később jogszabályba tudtak emelni. A

megalkotásától mindvégig részletesebb leírást biztosított, mint az OSHA. A legfrissebb verzióját 2024-ben adták ki.

Emellett a későbbiekben egyéb szabványokat is létrehoztak, amelyek specifikusan 1-1 részterülethez nyújtanak részletesebb útmutatást: NFPA 70E Standard for Electrical Safety in the Workplace [8] (Munkahelyi villamos biztonsági szabvány) vagy az ANSI B11-es sorozat, amely a gépbiztonsági szabványokat foglalja magában. Az ANSI szabályozás mellett még fontos megemlíteni a CSA Z460 szabványt is (Canadian Standards Association - Kanadai Szabványügyi Társaság), amely egyaránt épít az ISO 12100 [5] (International Organization for Standardization - Nemzetközi Szabványügyi Szervezet) és az ANSI előírásaira is. [9]

Európa jogszabályi és szabványi rendszere

Az Európai Unió területén alapvetően nem jogszabályokról beszélünk, hanem irányelvekről és harmonizált szabványokról. Érdekesség, hogy az EU részéről az irányelvek nem definiálják közvetlenül a LOTO-t, viszont a mögöttes elv és a tartalmi követelmény megegyezik az OSHA által definiált elvárásokkal. Amint viszont pontosan definiál, az a veszélyes energiák fogalma és a váratlan indítás megelőzése. A LOTO jogszabályi oldala: a 2009/104/EC [10] előírja, hogy a munkaeszközöket úgy kell kialakítani és üzemeltetni, hogy biztosított legyen azok biztonságos leállítása, az energiaforrásoktól történő leválasztása, valamint a karbantartási és javítási tevékenységek során a váratlan indítás és energiafelszabadulás megakadályozása.

Egy másik fontos direktíva a 2006/42/EC [11], azaz a Gépdirektíva. Itt kerül meghatározásra a gépek tervezésének követelményei. Harmonizált szabványként kiemelendő az EN ISO 14118:2018 [12], amely a gépek váratlan elindulásának megakadályozásával foglalkozik. Néhány megemlítendő további szabvány az ISO 13849, amely a gépek biztonsági vezérlésével foglalkozik, illetve az ISO 13850 [13], amely a vészleállítókkal szemben támasztott követelményeket taglalja.

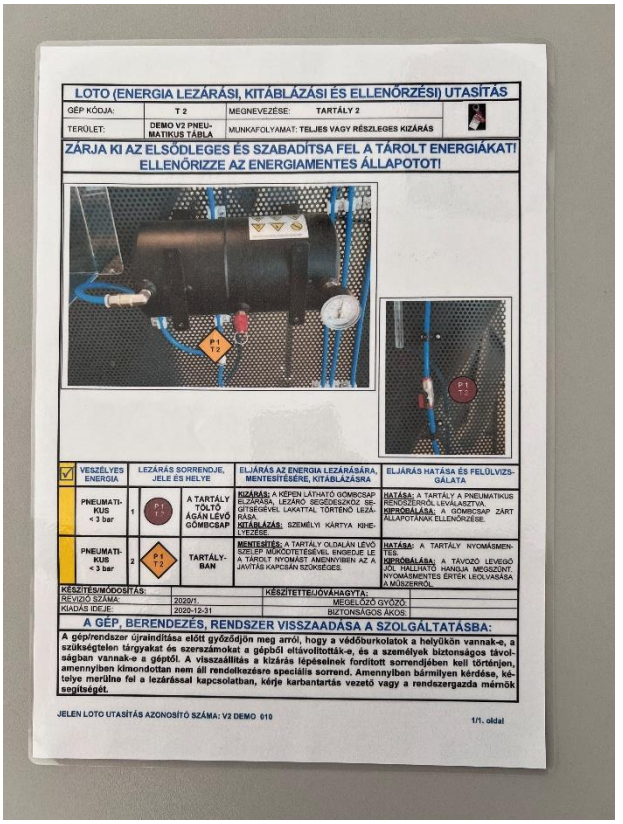
Magyarország jogszabályi és szabványi rendszere

Magyarország szabályozási rendszere e területen az Európai Unió harmonizált jogi és szabványosítási keretrendszeréhez igazodik, amely meghatározza a nemzeti jogszabályok és szabványok kialakítását. Törvényi szinten az 1993. évi XCIII. törvény a munkavédelemről (Mvt.) [1] határozza meg az elvárásokat. Kimondja többek között, hogy alapvető követelmény a biztonságos munkavégzés feltételeinek megteremtése, a veszélyek megszüntetése / csökkentése, illetve meghatározza a kockázatértékelések elvégzésének gyakoriságát, valamint a velük szemben támasztott elvárásokat.

Az Európai Unió direktíváit további jogszabályok ültetik be a gyakorlatba: a 10/2016 (IV. 5.) NGM rendelet [14] a 2009/104/EC direktíva harmonizálása. Előírja a berendezések leállításának követelményét, az energiaforrások leválaszthatóságát és összességében elmondható, hogy ez a LOTO jogi háttere Magyarországon. A gépek forgalomba hozatalára vonatkozóan a 16/2008. (VIII. 30.) NFGM rendelet tekinthető mérvadónak [15], amely a 2006/42/EC hazai jogrendbe történő átültetése és meghatározza a CE megfelelőséghez kapcsolódó alapvető egészségvédelmi és biztonsági követelményeket.

A LOTO RENDSZER ELEMEI

A gyakorlatban nincs egy olyan szabvány vagy leírás, amely a helyes LOTO elemeit összegezné és egyben leírná azt. Azonban a korábban bemutatott szabályozók alapján 12 szükséges lépést különböztetünk meg, melyek nagyságrendileg procedurális és rendszerszintű elemekre oszthatóak. Ezen lépések teljesítése és gyakorlati kivitelezése összességben egy megfelelő biztonságú rendszer fennállását eredményezi.


LOTO (ENERGIA LEZÁRÁSI, KITÁBLÁZÁSI ÉS ELLENŐRZÉSI) UTASÍTÁS

GÉP KÓDJA: T 2 | MEGNEVEZÉSE: TARTÁLY 2

TERÜLET: DEMO V2 PNEUMATIKUS TÁBLA | MUNKAFOLYAMAT: TELJES VAGY RÉSZLEGES KIZÁRÁS

ZÁRJA KI AZ ELSŐDLEGES ÉS SZABADÍTSA FEL A TÁROLT ENERGIÁKAT! ELLENŐRIZZE AZ ENERGIAMENTES ÁLLAPOTOT!

	VESZÉLYES ENERGIA	LEZÁRÁS SORRENDJE, JELE ÉS HELYE		ELJÁRÁS AZ ENERGIA LEZÁRÁSÁRA, MENTESÍTÉSÉRE, KITÁBLÁZÁSRA	ELJÁRÁS HATÁSA ÉS FELÜLVIZSGÁLATA
	PNEUMATIKUS < 3 bar	1	A TARTÁLY TÖLTŐ ÁGÁN LÉVŐ GÖMBCSAP	KIZÁRÁS: A KÉPEN LÁTHATÓ GÖMBCSAP ELZÁRÁSA, LEZÁRÓ SEGÉDESZKÖZ BEGTSÉGÉVEL LAKATTAL TÖRTÉNŐ LEZÁRÁSA. KITÁBLÁZÁS: SZEMÉLYI KÁRTYA KIHELYEZÉSE.	HATÁSA: A TARTÁLY A PNEUMATIKUS RENDSZERRŐL LEVÁLASZTVA. KIPRÓBÁLÁSA: A GÖMBCSAP ZÁRT ÁLLAPOTÁNAK ELLENŐRZÉSE.
	PNEUMATIKUS < 3 bar	2	TARTÁLYBAN	MENTESÍTÉS: A TARTÁLY OLDALÁN LÉVŐ SZELEP MŰKÖDTETÉSÉVEL ENGEDJE LE A TÁROLT NYOMÁST AMENNYIBEN AZ A JAVÍTÁS KAPCSÁN SZÜKSÉGES.	HATÁSA: A TARTÁLY NYOMÁSMENTES. KIPRÓBÁLÁSA: A TÁVOZÓ LEVEGŐ JÓL HALLHATÓ HANGJA MEGSZŰNT. NYOMÁSMENTES ÉRTÉK LEOLVASÁSA A MŰSZERRŐL

KÉSZÍTÉS/MÓDOSÍTÁS:		KÉSZÍTETTE/JÓVÁHAGYTA:	
REVÍZIÓ SZÁMA:	2020/1.	MEGELŐZŐ GYŐZŐ:	
KIADÁS IDEJE:	2020-12-31	BIZTONSÁGOS ÁKOS:	

A GÉP, BERENDEZÉS, RENDSZER VISSZAADÁSA A SZOLGÁLTATÁSBA:

A gép/rendszer újraindítása előtt győződjön meg arról, hogy a védőburkolatok a helyükön vannak-e, a szükségtelen tárgyakat és szerszámokat a gépből eltávolították-e, és a személyek biztonságos távolságban vannak-e a géptől. A visszaállítás a kizárás lépéseinek fordított sorrendjében kell történjen, amennyiben kimondottan nem áll rendelkezésre speciális sorrend. Amennyiben bármilyen kérdése, kételye merülne fel a lezárással kapcsolatban, kérje karbantartás vezető vagy a rendszergazda mérnök segítségét.

JELEN LOTO UTASÍTÁS AZONOSÍTÓ SZÁMA: V2 DEMO 010 1/1. oldal

2. ábra: LOTO ECP példa, a szerzők szerkesztése

Ha LOTO rendszerben gondolkodunk, az első minden esetben az energiaazonosítás. Egyértelműen meg kell határozni, hogy milyen veszélyes energiák vannak és azokat milyen sorban és módon kell kizárni. Az ezt kezelő dokumentációt szokták Energy Control Procedure-nek [2] (Energiakezelési eljárás - ECP - 2. ábra) nevezni, amely dokumentum feladata ennek a meghatározása. Többnyire ezt papíralapon vagy valamilyen dokumentumként szokták a munkavállalók számára biztosítani. Hatékony, azonban fontos megemlíteni azt a veszélyfaktort, hogy nem feltétlen a legfrissebb verzió alapján történik az energiák kizárása, ezáltal fennmaradó energiák maradnak a rendszerben.

3. ábra LOTO lakat példák, a szerzők szerkesztése

A második lépés a leválasztás (Izolálás). Ilyenkor a veszélyes energia leválasztásra, lekapcsolásra kerül, ezáltal kialakul a Zero Energy State alapfeltétele. [2]

A harmadik lépés a kizárás (Lock Out - LO - 3. ábra), amikor a lezáráshoz használt szerelvényre vagy eszközre valamilyen fizikai zárat helyezünk fel, ezáltal megakadályozzuk, hogy valaki esetleg valamely energia visszakapcsolhassa azt. A színeknek nincs szabványban foglalt jelölése, de gyakorlatban jellemzően a piros a személyi lakat (egy személy - egy kulcs) a sárga pedig a csoportos jelölés, amit a csoportvezető helyez fel. [2]

A negyedik lépése a címkézés (Tag Out - TO), amikor figyelmeztető jelöléssel és azonosítóval látjuk el a kizárásunkat, hogy ki, mikor és milyen céllal zárta el az energiaforrást. [2]

Az ötödik lépés a tárolt energia megszüntetése, mely lépésben a maradó energiák kerülnek eltávolításra. A balesetek nagyrésze ennek a lépésnek a végrehajtása közben vagy hiányában történik, amikor már áll a gép, de még energia van jelen. Mindig szem előtt kell tartani, hogy a berendezés nem tekinthető pusztán attól biztonságosnak, hogy az energiaforrásokat leválasztásra kerültek. [2]

Ezen lépést követi az ellenőrzése (Test Out – nem szokták kiírni, de néha feltüntetik egy további TO formájában) az eddigi folyamatoknak, amikor megerősítjük a Zero Energy State fennállását. [2]

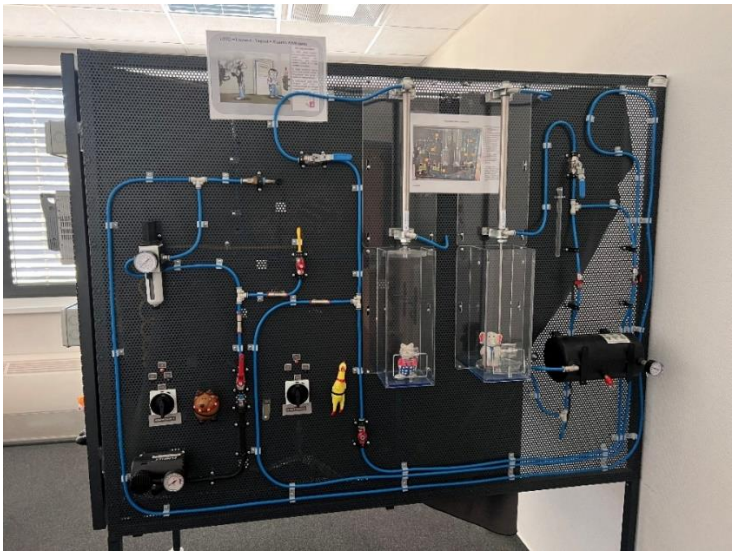
Ezt követően a hetedik lépés a visszaállítás, amely a gép biztonságos elindítását foglalja magában. Nagyon fontos ez a lépés, hogy a veszélyes energiák újraindítása közben ne rongálódjon meg sem a gép, valamint ne alakuljon ki további baleset sem egy esetleges gépsérülés következtében. Ehhez a lépéshez többnyire vissza szoktak hivatkozni az első lépésre, hiszen az ECP-ben meghatározott lépéseket visszakövetve a gép biztonságosan újraindítható. Amennyiben valamilyen okból kifolyóan nem, úgy külön eljárást biztosítanak a visszaállításhoz.[2]

A nyolcadik lépés a csoportos LOTO meghatározása, azaz, hogy hogyan tud több személy egyidejűen dolgozni a berendezésen. Ehhez többnyire már számos eszköz található

a piacon, az egyidőben munkát végzők számával arányosan. Általában egy speciális eszközre minden személy ráhelyez még egy további lakatot. Ezáltal, ameddig az utolsó ember nem végzett a munkával, addig nem lehetséges az adott veszélyes energia visszaállítása (például: vegyi anyagot tartalmazó tartály karbantartásánál a vegyi anyagot szállító szerelvény elzárása). [2]

A következő lépés is nagyon fontos, amely a külsős munkavállalók kezelését foglalja magában. Ha egy cég karbantartási részlege nem fedi le a teljes karbantartást, akkor szoktak igénybe venni alvállalkozókat, akik többnyire nem rendelkeznek ilyen szintű tudással. Ilyen esetben jellemzően dönthet úgy a cég, hogy kioktatja a főbb vállalkozóit, ezáltal önállóan kizárást fognak tudni végezni vagy a karbantartók/mérnökség elvégzi nekik a kizárást, amennyiben a munkavégzésükhöz az indokolt. [2]

A tizedik lépés egy általános probléma kezelését jelenti, amely a műszakváltás. Erre több jó megoldás is létezik, de jellemző példa, amikor a távozó műszak az érkező műszakkal lakatokat cserél, azaz a távozó műszak leveszi a lakatját, az érkező műszak pedig felhelyezi. [2]



4. ábra LOTO gyakorló tábla példa, a szerzők szerkesztése

A tizenegyedik lépés az oktatás és kompetencia. Sok esetben ez a lépés is kulcsfontosságú. Az általunk azonosított legjobb példa a „LOTO gyakorló fal” (4. ábra), ahol a telephelyen előforduló összes kizárás megjelenik egy gyakorló körülmény között, tényleges kockázat nélkül. [2]

Végül az utolsó lépés a rendszer auditja és felülvizsgálata, ahol ellenőrzésre kerül, hogy az előző tizenegy pont mennyire teljesül a gyakorlatban. Ha eltérést észlelünk, akkor azonnal cselekedni kell a megfelelő akciótervek meghozatalával és végrehajtásával. [2]

JAVASLAT A LOTO ELJÁRÁS MODERNIZÁLÁSÁRA

A XXI. század egyik legelterjedtebb vívmánya kétségkívül az okostelefon, amely jellemzően minden korosztály által többé-kevésbé rutinosan használt eszköz lesz, ahogy

haladunk előre z időben. Meglátásunk szerint ez képezhetné a LOTO modernizálásának az alapját. De mi is pontosan a probléma, amire megoldást keresünk? Nos, ez leginkább az emberi természetből adódó veszély, amely a megszokást jelenti. Ha egy folyamatot sokszor, precízen elvégzünk, hajlamosak vagyunk kevésbé az írott dokumentációkra támaszkodni annak végrehajtásához. Cserébe viszont elkezdünk emlékezetből vagy megszokásból dolgozni. Mindennapi életünkből ilyen például a vezetés: ha egy útvonalon 3 évig minden nap autózunk és megszokjuk, sokkal nagyobb eséllyel tévesztünk el egy forgalmi szabály változást, mintha egy új útvonalon mennénk, folyamatosan figyelve a táblákat, felfestéseket és esetleg a forgalmat is. A LOTO esetében ez elsősorban a kizárások felhelyezésére vonatkoztatható.

Amint azt korábban említésre került, napjaink rendszerei főként papír alapú megoldásokat használnak, ahol a karbantartónak kell dokumentálnia és követnie a folyamatot. Itt jönnek képbe az okostelefonok: mindenki zsebében ott vannak, ha pedig nincsenek, már nem jelent súlyos megterhelést, hogy biztosítsanak a szervezetek, munkáltatók egy eszközt a munkavállalóknak. [16]

Az AR technológia rövid bemutatása

Jellemzően, mint presztízs vagy hasznos funkció egyre nagyobb teret nyernek az AR (Kiterjesztett Valóság - Augmented Reality) funkcióval ellátott alkalmazások használata, amely a telefonok kameráján keresztül, a valóságos térben tudnak elhelyezni tárgyakat, objektumokat, melyek 3D-ben jelennek meg. Nagyon egyszerű példa az IKEA alkalmazása, amely számos bútor esetében lehetőséget biztosít számunkra, hogy kameránk segítségével a szobánkba próbáljuk a kiszemelt bútort, hogy hogyan is férne be vagy illeszkedne a már meglévő berendezési tárgyainkhoz. [17]

Emellett fontos kiemelni, hogy a technológiának lehetnek veszélyei is, melyek leginkább az Verify vagy „Test Out" lépésnél jelentkeznek: a szoftver ezt a lépést semmilyen keretek között nem helyettesíti, annak fizikai verifikációja minden helyzetben elsőbbséget képez.

A LOTO AR alkalmazás specifikációja

A mindennapi ipari gyakorlat során a LOTO eljárások alkalmazása gyakori. Ugyanakkor számos kérdés merül fel azok tényleges végrehajtásával kapcsolatban: ki végezte a kizárást, milyen eljárás alapján, megfelelően történt-e a végrehajtás, illetve valóban megvalósult-e a nullaenergia-állapot (Zero Energy State, ZES).

A gyakorlatban megfigyelhető, hogy a biztonságérzet inkább a munkavégző tapasztalatához kötődik, mintsem a folyamat objektív megfelelőségéhez. Ez azonban jelentős kockázatot hordoz, mivel a LOTO hatékonysága nem az egyéni rutinon, hanem a szabványosított és ellenőrizhető végrehajtáson alapul.

E kockázatok csökkentésére került kialakításra egy kiterjesztett valóság (AR) alapú alkalmazás, amely a LOTO folyamat digitalizált támogatását biztosítja. Az alkalmazás az Energy Control Procedure (ECP) dokumentumot digitalizálja és a berendezés (vagy bármely tér, épület, …) 3D modelljén jeleníti meg a kizárási pontokat, lépésről lépésre vezetve a felhasználót a folyamaton.

A folyamat megkezdése a berendezésen elhelyezett QR-kód beolvasásával történik, amely lehetővé teszi a megfelelő eljárás kiválasztását, beleértve a teljes vagy részleges

LOTO végrehajtását. Az alkalmazás ezt követően meghatározott sorrendben vezeti végig a felhasználót az egyes kizárási pontokon.

Minden egyes lépésnél az alkalmazás megjeleníti:

- a szükséges műveletet (pl. adott szerelvény elfordítása),
- a várható hatást (pl. világítás megszűnése),
- valamint az ellenőrzési módot (pl. indítógomb tesztelése).

A kizáró eszköz felhelyezése QR-kód segítségével kerül rögzítésre, amely során az alábbi adatok kerülnek dokumentálásra:

- a felhelyezés időpontja,
- az eszköz egyedi azonosítója,
- a kizárási pont azonosítója,
- a végrehajtó személy neve,
- valamint az alkalmazott eljárás típusa.

A rendszer továbbá képi dokumentációt is rögzít, amely igazolja a fizikai végrehajtást. A folyamat során az alkalmazás automatikusan irányítja a felhasználót a következő kizárási pontra, szükség esetén térképes és képi támogatással. A folyamat lezárásakor a rendszer menti a felhelyezett LOTO eszközöket és biztosítja, hogy a kizárás megszüntetését kizárólag a jogosult személy kezdeményezhesse. Műszakváltás esetén a jogosultságok QR-kód alapú átadással kerülnek továbbításra, amely a rendszer naplójában is rögzítésre kerül. Ilyenkor az átadó telefonján megjelenik egy kód, amit az átvevőnek be kell olvasnia.

Az alkalmazás egyik legnagyobb előnye, hogy egységes és naprakész információt biztosít minden felhasználó számára, ezáltal csökkentve a tapasztalati különbségekből eredő kockázatokat. Emellett biztosítja a folyamat teljes körű dokumentálhatóságát és visszakövethetőségét. További előnyt jelent az oktatási funkció, amely lehetővé teszi a LOTO folyamat gyakorlását fizikai beavatkozás nélkül. Az úgynevezett „training mode” segítségével a felhasználók a kizárási lépéseket szimulált környezetben sajátíthatják el, ami különösen hasznos új munkavállalók képzése során.

Háttérfolyamatok kezelése

A háttérben egy alkalmazáson keresztül tudunk szabályozni, illetve hozzáférni a telefonos kliens minden részéhez: itt adhatunk hozzáférési jogot, férhetünk hozzá a nyilvántartásokhoz, módosíthatjuk az eljárásokat. Az összes itt megvalósult kattintásról egy további naplófile készül, ezáltal nem tud senki sem nyom nélkül módosítani semmit. A felhasználói jogkörök meghatározása a gyáregység feladata.

A bemutatott rendszer jelenleg koncepcionális modellként értelmezhető, amelynek gyakorlati validációja további kutatás tárgyát képezi.

ÖSSZEFOGLALÁS

A tanulmány célja a LOTO módszertan kialakulásának, fejlődésének, szabályozásokban elfoglalt helyének, valamint lehetséges modernizációs irányainak bemutatása. A kutatás alapjául az a meglátás szolgált, hogy a veszélyes energiák nem megfelelő kezelése napjainkban is az egyik legjelentősebb ipari kockázatforrás, különösen karbantartási és esetleges beavatkozási munkák során.

Az ismertetett statisztikák alapján megállapítható, hogy a LOTO rendszer kialakulását súlyos, sok esetben halálos kimenetelű balesetek indokolták, amelyek jelentős része a veszélyes energia nem megfelelő izolálására vagy megszüntetésére vezethető vissza.

A tanulmány részletesen ismerteti a veszélyes energiák fő kategóriáit, valamint bemutatja az OSHA, az ANSI, az ISO és az európai szabályozási rendszerek szerepét a LOTO fejlődésében. Tanulmányunkban ismertettük, hogy bár a modern szabványok és jogszabályok egyértelmű követelményeket fogalmaznak meg a váratlan indítás megakadályozására és az energiaforrások biztonságos leválasztására, maga a gyakorlati végrehajtás sok esetben továbbra is papíralapú vagy erősen emberi rutinra épülő folyamat. Ez különösen azért jelent problémát, mert a LOTO hatékonysága nem az egyéni tapasztalaton, hanem a standardizált, következetesen végrehajtott lépéseken és eljárásokon alapul.

A kutatás egyik fontos része egy tizenkét elemből álló LOTO-modell bemutatása, amely rendszerszinten foglalja össze a biztonságos energiaizolálás legfontosabb lépéseit. A tanulmány külön hangsúlyt fektet a Zero Energy State (ZES) fogalmára, amely a teljes energiamentes állapot elérését jelenti, és amely a biztonságos munkavégzés alapfeltétele.

A szerzők meglátása szerint a jelenlegi LOTO rendszerek egyik legnagyobb kockázata az emberi megszokásból fakad. A hosszú ideje ugyanazon berendezéseken dolgozó munkavállalók hajlamosak lehetnek a dokumentáció helyett rutin alapján végrehajtani a kizárásokat, ami növeli a hibázás lehetőségét, emellett a nyilvántartások vezetése is rendszeresen elmarad. Ennek csökkentésére a tanulmány egy AR alapú digitális LOTO alkalmazás koncepcióját mutatja be, amely képes a hagyományos Energy Control Procedure dokumentumok digitalizálására és interaktív támogatására.

A javasolt rendszer QR-kód alapú azonosítással, 3D modelleken megjelenített kizárási pontokkal, automatikus dokumentációval és auditálható naplózással támogatja a munkavállalókat. A megoldás egyik legnagyobb előnye, hogy a kevésbé tapasztalt dolgozók számára is ugyanazt a szintű ismeretet biztosítja, mint amivel a rutinos karbantartók rendelkeznek. Emellett a rendszer képes dokumentálni a kizárások teljes folyamatát, a felhelyezett lakatok azonosítóit, az időpontokat, valamint a végrehajtó személyeket is. A koncepció további jelentős eleme az oktatási mód, amely lehetőséget biztosít a LOTO folyamatok gyakorlására tényleges energiakizárás nélkül, ezáltal támogatva a kompetenciafejlesztést és az új munkavállalók képzését.

Összességében megállapítható, hogy a LOTO rendszer továbbra is az egyik legfontosabb munkavédelmi eszköz a gépeken és veszélyes energiákkal rendelkező technológiákon, illetve azok környezetében végzett munka tekintetében, azonban a modern ipari környezetben indokolttá vált annak továbbfejlesztése.

A tanulmányban bemutatott AR-alapú megközelítés egy lehetséges jövőbeni irányt mutat be, amely egyszerre növelheti a biztonságot, a dokumentálhatóságot és a folyamatok megbízhatóságát. A technológia továbbá az autonóm karbantartás területén is kulcsfontosságú eszköz lehet a munkáltatók kezében.

FELHASZNÁLT IRODALOM

[1] Wolters Kluwer Hungary Kft, „1993. évi XCIII. törvény a munkavédelemről - Hatályos Jogszabályok Gyűjteménye”. Elérés: 2026. május 6. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99300093.tv

[2] Occupational Safety and Health Administration, *The control of hazardous energy (lockout/tagout)*., 1910.147. [Online]. Elérhető: https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.147
[3] Brady Worldwide, Inc., „Top 10 OSHA Violations for 2025”. [Online]. Elérhető: https://www.bradyid.com/resources/top-10-osha-violations
[4] „NSC Reveals Major Injury, Fatality Events Related to OSHA Top 10 Citations for FY 2025”, szept. 2025.
[5] International Organization for Standardization, *Gépek biztonsága. A kialakítás általános elvei. Kockázatértékelés és kockázatcsökkentés*, ISO 12100:2010., 2010.
[6] S. Dekker, *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems*, 0 kiad. CRC Press, 2016. doi: 10.1201/9781315257396.
[7] American Society of Safety Professionals, *The Control of Hazardous Energy Lockout, Tagout and Alternative Methods*, ANSI/ASSP Z244.1-2024, 2024.
[8] National Fire Protection Association, *Standard for Electrical Safety in the Workplace*, NFPA 70E-2024, 2024.
[9] Canadian Standards Association, *Control of hazardous energy - Lockout and other methods*, 2020.
[10] „Directive No. 2009/104/EC,of the European Parliament and of the Council, of 16 September 2009, concerning the minimum safety and health requirements for the use of work equipment by workers at work | International Labour Organization”. Elérés: 2026. május 7. [Online]. Elérhető: https://www.ilo.org/resource/directive-no-2009104ecof-european-parliament-and-council-16-september-2009
[11] EURÓPAI PARLAMENT, *AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2006/42/EK IRÁNYELVE a gépekről és a 95/16/EK irányelv módosításáról*, 2019. július 26.
[12] International Organization for Standardization, *Gépek biztonsága. A váratlan indítás megelőzése*, ISO 14118:2018, 2018.
[13] International Organization for Standardization, *Gépek biztonsága. Vészleállítás. Tervezési alapelvek*, ISO 13850:2015, 2015.
[14] Wolters Kluwer Hungary Kft, „10/2016. (IV. 5.) NGM rendelet a munkaeszközök és használatuk biztonsági és egészségügyi követelményeinek minimális szintjéről - Hatályos Jogszabályok Gyűjteménye”. Elérés: 2026. május 6. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1600010.ngm
[15] Wolters Kluwer Hungary Kft, „16/2008. (VIII. 30.) NFGM rendelet a gépek biztonsági követelményeiről és megfelelőségének tanúsításáról - Hatályos Jogszabályok Gyűjteménye”. Elérés: 2026. május 6. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a0800016.nfg
[16] J. W. Veile, D. Kiel, J. M. Müller, és K.-I. Voigt, „Lessons learned from Industry 4.0 implementation in the German manufacturing industry”, *J. Manuf. Technol. Manag.*, köt. 31, sz. 5, o. 977–997, aug. 2019, doi: 10.1108/JMTM-08-2018-0270.
[17] G. Sanodia, „The Role of Augmented Reality (AR) and Virtual Reality (VR) in Enhancing Customer Experiences within CRM Systems”, *Turk. J. Comput. Math. Educ. TURCOMAT*, köt. 12, sz. 15, o. 722–738, ápr. 2021, doi: 10.61841/turcomat.v12i15.14750.

DOI: https://doi.org/10.12700/btsz.2026.8.2.73

INTERPRETATION AND MAINTENANCE OF THE EXPLOSION SAFETY CONDITION WITHIN THE SYSTEM OF INSPECTIONS

A ROBBANÁSBIZTONSÁGI ÁLLAPOT ÉRTELMEZÉSE ÉS FENNTARTÁSA A FELÜLVIZSGÁLATOK RENDSZERÉBEN

ZSARNOVSZKI Attila[1] – ELEK Barbara[2]

Abstract

In the system-oriented approach of safety science, explosion safety cannot be interpreted exclusively as a one-time compliance condition, but rather as a technical and organizational state that changes over time. The aim of this paper is to examine to what extent current explosion protection inspection practices are capable of reflecting this dynamic nature of the safety state. The analysis is based on a review of the regulatory and technical framework of explosion protection, as well as an evaluation of the role and limitations of periodic inspections. The results highlight that predominantly static inspection approaches are only partially suitable for assessing temporal state changes and the effects of corrective maintenance activities. Based on these findings, the paper argues that a modern interpretation of explosion safety justifies a stronger consideration of the time dimension and systematic feedback mechanisms within inspection practices.

Keywords

explosion protection, ATEX, inspection, safety science, explosive atmospheres

Absztrakt

A robbanásbiztonság a biztonságtudomány rendszerelvű megközelítésében nem kizárólag egyszeri megfelelőségi állapotként, hanem időben változó műszaki és szervezeti állapotként értelmezhető. A tanulmány célja annak bemutatása, hogy a robbanásvédelmi felülvizsgálatok jelenlegi gyakorlata milyen mértékben képes leképezni ezt a dinamikus állapotjelleget. A vizsgálat a robbanásvédelem szabályozási és műszaki környezetének elemzésére, valamint a felülvizsgálatok szerepének és korlátainak értékelésére épül. Az eredmények rámutatnak arra, hogy a jellemzően statikus szemléletű ellenőrzési megközelítések korlátozottan alkalmasak az időbeli állapotváltozások és a javító tevékenységek hatásának értékelésére. Mindezek alapján a tanulmány amellett érvel, hogy a robbanásbiztonsági állapot korszerű értelmezése indokolja az idődimenzió és a rendszeres visszacsatolás hangsúlyosabb figyelembevételét a felülvizsgálati gyakorlatban.

Kulcsszavak

robbanásvédelem, ATEX, felülvizsgálat, biztonságtudomány, robbanóképes közeg

[1] zsarnovszki.attila@stud.uni-obuda.hu | ORCID: 0009-0001-5337-4212 | PhD student, Óbuda University, Doctoral School on Safety and Security Sciences | PhD hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola

[2] elek.barbara@bgk.uni-obuda.hu | ORCID: 0000-0001-7515-6374 | associate professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Institute of Safety Science and Cybersecurity | egyetemi docens Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Biztonságtudományi és Kibervédelmi Intézet

BEVEZETÉS

A robbanásvédelem műszaki, jogi és szabványi környezete első megközelítésben részletesen szabályozott rendszerként jelenik meg. A potenciálisan robbanásveszélyes térségekben alkalmazott technológiákra, berendezésekre és üzemeltetési gyakorlatokra részletes követelményrendszer vonatkozik. E követelményeket európai irányelvek [1] [2], törvények [3] [4], nemzeti jogszabályok [5] és harmonizált szabványok [6] együttesen határozzák meg. A szabályozási rendszer célja annak biztosítása, hogy a robbanóképes közegek jelenlétében a gyújtóforrások kialakulásának valószínűsége, valamint a robbanások bekövetkezésének kockázata társadalmilag elfogadható szinten maradjon. [7]

A biztonság a biztonságtudomány értelmezésében nem statikus megfelelőségi állapot, hanem dinamikusan változó egyensúlyi állapot, amelyben a veszélyeztető tényezők és az azok kezelésére szolgáló műszaki és szervezeti intézkedések folyamatos kölcsönhatásban állnak egymással. [8] A tanulmány ebből a megközelítésből kiindulva a robbanásbiztonságot nem egyszeri megfelelőségi vagy kizárólag dokumentációs állapotként, hanem időben változó rendszerállapotként értelmezi. A technológiai rendszerek öregedése, az üzemeltetési környezet változása, az emberi beavatkozások, valamint a javítási és karbantartási gyakorlat együttesen folyamatosan alakítják a tényleges robbanásbiztonsági állapotot. [9]

A fentiek ellenére a robbanásvédelem jelenlegi megfelelőségértékelési és felülvizsgálati rendszere a gyakorlatban alapvetően statikus szemléletű. A felülvizsgálatok eredményei jellemzően egy adott időpillanatban rögzített megfelelőségi állapotként jelennek meg, miközben korlátozottan értelmezhető a hibák fennmaradása, az állapotváltozások dinamikája, valamint a javító intézkedések tényleges hatása. A jelenlegi gyakorlatból nagyrészt hiányzik az időbeli állapotváltozások és a javítási folyamatok eredményességének objektív vizsgálata, továbbá jelenleg nem terjedt el egységes módszertan a feltárt hibák súlyosságának, illetve a javításra adható időkeretek meghatározására sem.

A szerző kutatási munkája reagálni kíván a biztonságtudomány említett elméleti kerete és a gyakorlatban kialakult szemléletekre, így eredetileg a robbanásbiztonsági állapot időbeli változásának és az ipari felülvizsgálatok során feltárt hibák dinamikájának empirikus vizsgálatára irányult. A nagyszámú ipari adatbázis elemzése során egyre markánsabban jelentkezett egy alapvető módszertani probléma. A robbanásvédelem jelenlegi felülvizsgálati gyakorlata elsősorban statikus állapotok leírására alkalmas, miközben korlátozott eszközökkel rendelkezik az időbeli állapotváltozások, a hibaperzisztencia, valamint a javítási és karbantartási folyamatok hatékonyságának értelmezésére.

A jelen tanulmány célja ezért nem új műszaki előírások vagy konkrét kvantitatív módszerek részletes bemutatása, hanem egy olyan biztonságtudományi, jogi és műszaki értelmezési keret felállítása, amely megalapozza a robbanásbiztonsági állapot időfüggő vizsgálatának szükségességét. A tanulmány áttekinti a robbanásvédelem szabályozási és műszaki környezetét, a biztonság fogalmának biztonságtudományi értelmezését, a felülvizsgálatok szerepét és korlátait, valamint azokat a módszertani hiányosságokat, amelyek indokolttá teszik a robbanásbiztonsági állapot dinamikus, időben értelmezhető vizsgálatának kialakítását.

A ROBBANÁSVÉDELEM SZABÁLYOZÁSI ÉS MŰSZAKI KÖRNYEZETE

A fejezet célja a robbanásvédelem jogi és műszaki szabályozási környezetének áttekintése, mint a robbanásbiztonsági állapot értelmezésének formális kerete.

A robbanásveszélyes technológiák biztonsági követelményeinek szabályozása az Európai Unióban harmonizált jogi és műszaki keretrendszerben valósul meg. A szabályozás célja annak biztosítása, hogy a potenciálisan robbanóképes közegek jelenlétében alkalmazott technológiák, berendezések és védelmi intézkedések a robbanások kialakulásának és következményeinek kockázatát társadalmilag elfogadható szinten tartsák. [10]

Robbanóképes közeg alatt olyan gáz-, gőz-, köd- vagy por-levegő keveréket értünk, amelyben gyújtóforrás jelenlétében az égés az el nem égett keverék teljes térfogatára önfenntartó módon továbbterjed. Az ilyen közegek az ipar számos területén természetes módon jelen vannak vagy technológiai körülmények között kialakulhatnak, különösen az olaj- és gáziparban, a vegyiparban, a petrolkémiában, a gyógyszergyártásban, az élelmiszeriparban, a gabonatárolás és -feldolgozás területén, a festékgyártásban, valamint egyes korszerű akkumulátorgyártási és finomkémiai technológiákban. [11]

Az európai robbanásvédelmi szabályozási rendszer két alapvető pillére a munkahelyekre vonatkozó ATEX 153 irányelv [1] és a berendezésekre vonatkozó ATEX 114 [2] irányelv. Az ATEX 153 irányelv [1] az üzemeltetők kötelezettségeit, a robbanásveszélyes térségek azonosításának és kockázatkezelésének követelményeit, valamint a munkavállalók biztonságának feltételeit határozza meg, míg az ATEX 114 [2] irányelv a potenciálisan robbanásveszélyes térségekben alkalmazott berendezések és védelmi rendszerek megfelelőségi követelményeit szabályozza.

Jelen kutatás elsődlegesen a potenciálisan robbanásveszélyes ipari környezetek robbanásbiztonsági állapotának értelmezésére fókuszál, és nem terjed ki közvetlenül a robbanóanyag- vagy lőporgyártás speciális technológiai és hadtudományi kérdésköreire. Ugyanakkor a különböző robbanási kockázati rendszerek közötti átjárások és hibrid alkalmazási terek vizsgálata a nemzetközi és hazai szakirodalomban egyre hangsúlyosabban jelenik meg, különösen a robbanóanyag-technológia és a robbanásvédelem metszetében.[12]

A robbanásvédelem gyakorlati megvalósítása nem kizárólag egyetlen jogszabály vagy szabvány alkalmazását jelenti, hanem több szakterület követelményeinek együttes érvényesítését igényli. A robbanásveszélyes térségek biztonságos kialakítása és üzemeltetése [13] egyidejűleg érinti többek között a robbanásvédelem [14], a villamos biztonság [5], a tűzvédelem [4], a munkavédelem [15], a villám- és sztatikus feltöltődés elleni védelem [16], továbbá más szakmák követelményeit is [17]. A robbanásvédelem ezért alapvetően interdiszciplináris műszaki területként értelmezhető, ahol az egyes szakterületek követelményei egymással kölcsönhatásban fejtik ki hatásukat.

A robbanásvédelmi követelmények teljesülésének gyakorlati igazolása döntően harmonizált szabványokon és az azokhoz kapcsolódó műszaki irányelveken keresztül valósul meg. Az európai és magyar szabályozási rendszer formálisan lehetőséget biztosít a szabványoktól vagy műszaki irányelvektől eltérő műszaki megoldások alkalmazására, amennyiben azokkal legalább azonos biztonsági szint igazolható. [18] A magyar szabályozási környezetben az Országos Tűzvédelmi Szabályzat [7] és a kapcsolódó jogszabályi rendelkezések az eltérő műszaki megoldások alkalmazását külön eljáráshoz [19] és a biztonsági szint igazolásához kötik, amelyhez a tervezőnek számításokkal, modellezéssel vagy egyéb

műszaki bizonyítási módszerekkel kell alátámasztania az alkalmazott megoldás egyenértékűségét. [20]

A robbanásvédelem területén ugyanakkor a megfelelő biztonsági szinthez kapcsolódó nominális kockázati célértékek — például az emberi élet elvesztésére, a környezetkárosításra vagy a közszolgáltatások kiesésére vonatkozóan — jellemzően nincsenek explicit módon meghatározva. A harmonizált szabványok ezért elsősorban nem konkrét kockázati szintek számszerű elérését írják elő, hanem olyan műszaki megoldásokat és kialakítási követelményeket határoznak meg, amelyek alkalmazásához megfelelőségi vélelem kapcsolódik. Ebből következően a szabványoktól eltérő robbanásvédelmi megoldások objektív egyenértékűségének igazolása a gyakorlatban jelentős műszaki, jogi és felelősségi kihívást jelenthet. A jelenlegi európai és magyar robbanásvédelmi szabályozási környezet működése ezért a gyakorlatban alapvetően preszkriptív logika mentén értelmezhető: a megfelelő biztonsági állapot elsődleges igazolása a harmonizált szabványokban és kapcsolódó műszaki követelményekben meghatározott előírások teljesítésén keresztül valósul meg. [18]

A jelenlegi szabályozási és szabványi rendszer működése ezért elsődlegesen a megfelelőség igazolására épül. A robbanásvédelmi követelmények teljesülése a gyakorlatban döntően meghatározott műszaki kialakítások, szabványi előírások és felülvizsgálati követelmények teljesítésén keresztül kerül értelmezésre. Ez a megközelítés ugyanakkor alapvetően egy adott időpillanatban értelmezett megfelelőségi állapotból indul ki.

A jelen tanulmány szorosan kapcsolódik a szerző korábbi, robbanásvédelmi felülvizsgálati tapasztalatokra és empirikus adatbázis-elemzésekre épülő kutatásaihoz, amelyek a robbanásbiztonsági állapot értelmezésével, a hibák súlyossági rendszerével, valamint a megfelelőség időbeli változásának vizsgálatával foglalkoztak [21] [22]. A korábbi eredmények rámutattak arra, hogy a robbanásbiztonság nem statikus megfelelőségi állapotként, hanem dinamikusan változó rendszertulajdonságként értelmezhető, amelyet műszaki, szervezeti és üzemeltetési tényezők együttesen alakítanak.

E ponton válik egyértelművé a robbanásvédelmi felülvizsgálati rendszer egyik alapvető korlátja. A robbanásbiztonság — a biztonságtudomány általános értelmezésével összhangban — nem statikus megfelelőségi állapotként, hanem dinamikusan változó egyensúlyi állapotként értelmezhető. Ebben a kontextusban a veszélyeztető tényezők és az azok kezelésére szolgáló műszaki és szervezeti intézkedések folyamatos kölcsönhatásban állnak egymással. Ebből következően a robbanásvédelem nem értelmezhető kizárólag egyszeri megfelelőségi állapotként vagy dokumentációs követelményként. A megfelelő biztonsági szint fenntartása műszaki és biztonságtudományi szempontból elsősorban folyamatos műszaki kontroll, rendszeres felülvizsgálat, valamint a feltárt hiányosságokra visszacsatolt javító és karbantartó tevékenység révén biztosítható, amelynek alkalmazását a vonatkozó jogszabályi és szabványi környezet egyaránt megköveteli.

A robbanásbiztonsági állapot alakulását nem kizárólag a berendezések műszaki állapota, hanem az emberi, szervezeti és üzemeltetési tényezők is érdemben befolyásolhatják. A kritikus infrastruktúrák védelmével foglalkozó kutatások rámutatnak arra, hogy a technológiai rendszerek sérülékenysége nem csupán külső eseményekből, hanem belső szereplők, szervezeti hiányosságok, hibás működési gyakorlatok vagy akár szándékos beavatkozások következtében is kialakulhat. A robbanásbiztonság ezért nem kizárólag statikus műszaki megfelelőségi kérdésként, hanem összetett biztonsági és üzemeltetési rendszerként értelmezhető.[23]

A FELÜLVIZSGÁLATOK SZEREPE A ROBBANÁSBIZTONSÁGI ÁLLAPOT FENNTARTÁSÁBAN

Az elméleti és szabályozási kereteket követően indokolt külön vizsgálni a felülvizsgálatok gyakorlati szerepét a robbanásbiztonsági állapot fenntartásában.

A robbanásvédelmi követelmények teljesülésének biztosítása nem kizárólag a megfelelő tervezési és létesítési állapot kialakítását igényli, hanem annak folyamatos fenntartását is. A potenciálisan robbanásveszélyes térségekben alkalmazott berendezések és védelmi intézkedések műszaki állapota az üzemeltetés során természetes módon változik: az öregedési folyamatok, a környezeti hatások, a mechanikai igénybevételek, a karbantartási és javítási beavatkozások, valamint az emberi tényezők együttesen befolyásolják a robbanásbiztonsági állapot alakulását. [9]

A robbanásveszélyes térségekben alkalmazott berendezések és rendszerek üzembe helyezését megelőzően a vonatkozó jogszabályok és szabványok a villamos biztonsági [5] és robbanásvédelmi követelmények [13] teljes körű ellenőrzését írják elő. Az úgynevezett első (initial) felülvizsgálatok célja annak igazolása, hogy az adott létesítmény, berendezés vagy rendszer a tervezett üzemeltetési körülmények között igazoltan teljesíti a vonatkozó biztonsági követelményeket.

Az első felülvizsgálatok egyben a legmagasabb ellenőrzési mélységet képviselik, amelyek célja a teljes rendszer megfelelőségének lehető legteljesebb körű igazolása.

Ebből következően megfelelő tervezés, kivitelezés és ellenőrzés esetén a technológiai rendszer az üzembe helyezés időpontjában egy olyan robbanásbiztonsági állapotból indul, amelyet az első felülvizsgálatok a vonatkozó követelmények teljesüléseként igazolnak. Az üzemeltetés megkezdését követően azonban a műszaki állapot a rendszer természetéből fakadóan folyamatos változásnak van kitéve, amely megfelelő kontroll és visszacsatolt beavatkozások hiányában a robbanásbiztonsági állapot romlásának irányába hat. A robbanásbiztonság dinamikus állapotjellege ezért indokolttá teszi az ismételt felülvizsgálatok, valamint a visszacsatolt javító és karbantartó tevékenységek alkalmazását.[24]

A robbanásbiztonság megfelelő szintje — a biztonságtudomány általános értelmezésével összhangban — hosszú távon akkor tartható fenn, ha a kialakított műszaki és szervezeti védelmi intézkedések érvényesülését az üzemeltetés teljes életciklusa során rendszeresen ellenőrzik. A feltárt hiányosságokat értékelik, valamint a szükséges javító intézkedéseket visszacsatolt módon végrehajtják. A robbanásvédelmi szabályozási és szabványi környezet ezt a követelményt közvetlen módon is megjeleníti: a potenciálisan robbanásveszélyes térségekben alkalmazott berendezések időszakos felülvizsgálatát és a feltárt hibák javítását egyaránt kötelező elemként kezeli. A felülvizsgálatok szerepe ebben az értelemben túlmutat a formális megfelelőség igazolásán: elsődleges funkciójuk a robbanásbiztonsági állapot monitorozása és a megfelelő biztonsági szint fenntartásának támogatása.

A robbanásvédelmi felülvizsgálatok gyakorlati rendszere mindemellett nem önállóan értelmezhető műszaki tevékenységként jelenik meg. A potenciálisan robbanásveszélyes térségekben alkalmazott villamos berendezések esetében a robbanásvédelmi megfelelőség és a villamos biztonság követelményei közvetlen kölcsönhatásban állnak egymással. A villamos berendezések érintésvédelmi, túláramvédelmi, szigetelési vagy zárlatvédelmi hiányosságai egyidejűleg jelenthetnek életvédelmi, tűzvédelmi és robbanásvédelmi kockázatot is.

A robbanásvédelmi felülvizsgálatok és a villamos biztonsági felülvizsgálatok kapcsolatát a magyar szabályozási környezet közvetlen módon is megjeleníti. A 40/2017. (XII. 4.) NGM rendelet [5] hatálya kiterjed a potenciálisan robbanásveszélyes térségekben alkalmazott villamos berendezésekre is, amelyek esetében a jogszabály a villamos biztonsági követelmények ellenőrzését szigorított feltételek mellett kezeli. A rendelet a robbanásveszélyes térségekben alkalmazott villamos berendezések esetében az általános feszültséghatároktól eltérően alacsonyabb feszültségszinteken is kötelezővé teszi a villamos biztonsági felülvizsgálatokat. Továbbá meghatározza az ismétlődő felülvizsgálatok ciklusidejét is.

A robbanásveszélyes térségekben alkalmazott villamos berendezések felülvizsgálatára és karbantartására vonatkozó részletes műszaki követelményeket az MSZ EN IEC 60079-17 szabvány [13] határozza meg. A szabvány az első (initial), időszakos és folyamatos felügyeleti jellegű felülvizsgálatok rendszerét egyaránt szabályozza, amelynek célja a robbanásvédelmi követelmények teljesülésének fenntartása az üzemeltetés teljes életciklusa során.

A villamos biztonsági és robbanásvédelmi követelmények ezért nem egymástól független rendszerekként, hanem egymással közvetlen kölcsönhatásban álló biztonsági követelményekként jelennek meg. A villamos eredetű gyújtóforrások kialakulásának lehetősége, valamint az azok megelőzésére szolgáló védelmi intézkedések megfelelősége egyidejűleg hordoz villamos biztonsági, tűzvédelmi és robbanásvédelmi jelentőséget.

Ebből következően a robbanásvédelmi és villamos biztonsági felülvizsgálatok egymástól elkülönült időben vagy tartalommal történő értelmezése műszaki, biztonságtudományi és szabályozási szempontból is korlátozottan értelmezhető, mivel a robbanásbiztonsági állapot értékelése a villamos eredetű gyújtóforrások kialakulásának lehetőségétől és az azok megelőzésére szolgáló védelmi intézkedések tényleges érvényesülésétől nem választható el.

A robbanásbiztonsági állapot megfelelő értékelésének alapvető feltétele a vizsgálatok teljessége és tételessége. A robbanásvédelmi és villamos biztonsági követelmények teljesülése minden egyes érintett berendezésre, védelmi elemre és kialakítási részletre egyedileg értelmezendő, ezért a felülvizsgálatok rendszere alapvetően tételes ellenőrzési logikára épül. A vonatkozó jogszabályi és szabványi környezet az érintett berendezések és védelmi intézkedések egyedi megfelelőségének ellenőrzését követeli meg. Ebből következően a reprezentatív mintavételen vagy részleges állapotértékelésen alapuló megközelítések a robbanásvédelmi felülvizsgálatok rendszerlogikájával korlátozottan egyeztethetők össze.

A vizsgálatok teljességének követelménye a gyakorlatban számos esetben üzemeltetési, technológiai vagy hozzáférési nehézségekbe ütközhet, különösen üzemelő berendezések, magasban elhelyezett szerelvények vagy nehezen hozzáférhető kialakítások esetén. Ezek a körülmények másrészről nem szüntetik meg a felülvizsgálatok tételes és teljes körű végrehajtásának követelményét, hanem olyan szervezési, üzemeltetési vagy ismételt vizsgálati intézkedéseket tesznek szükségessé, amelyek révén az érintett berendezések megfelelősége egyedileg ellenőrizhetővé válik.

A robbanásbiztonsági állapot értékelése ezért számos esetben nem korlátozható kizárólag dokumentációs vagy szemrevételezéses megfelelőség-ellenőrzésre.

A robbanásvédelmi felülvizsgálatok eredményeihez kapcsolódó javítási kötelezettség szintén a biztonsági állapot fenntartásának részét képezi. A 40/2017. (XII. 4.) NGM rendelet [5] a feltárt hiányosságok esetében előírja a javításra vonatkozó írásos intézkedések

és javítási határidők meghatározását, amelyhez közvetlen jogkövetkezmények is kapcsolódnak. Amennyiben a feltárt hiányosság a meghatározott időkereten belül nem kerül megszüntetésre, a berendezés üzemeltetése nem tartható fenn.

A javításra adható időkeretek meghatározása ezért a robbanásbiztonsági állapot fenntartásának egyik központi jelentőségű eleme. A jelenlegi szabályozási és szabványi környezet — a javítási kötelezettség és az időkeretek alkalmazásának előírása mellett — nem határoz meg egységes, objektív és ismételhető mérnöki módszertant a feltárt hibák súlyosságának, a javítási prioritásoknak vagy a javításra adható idő meghatározásának támogatására.

A javítási időkeretek meghatározása ezért a gyakorlatban a felülvizsgáló és az üzemeltető közös műszaki és üzemeltetési mérlegelésén alapul. Ennek során egyidejűleg szükséges figyelembe venni a feltárt hiba jellegét, a robbanásbiztonsági kockázatot, a technológiai környezetet, valamint a javítás tényleges műszaki és szervezési lehetőségeit. A jelenlegi rendszer korlátozott eszközöket biztosít annak objektív értékelésére, hogy az adott robbanásbiztonsági állapot időben milyen mértékben változik, a feltárt hibák milyen arányban maradnak fenn, illetve a végrehajtott javító intézkedések milyen hatást gyakorolnak a biztonsági állapot alakulására. [5]

A felülvizsgálatok ezért számos esetben elsősorban statikus állapotképet rögzítenek, miközben korlátozottan értelmezhető a hibák időbeli fennmaradása, az állapotváltozások dinamikája, valamint a javító intézkedések tényleges hatása.

A ROBBANÁSVÉDELMI FELÜLVIZSGÁLATOK GYAKORLATI KORLÁTAI

A következőkben a robbanásvédelmi felülvizsgálatok gyakorlati végrehajtása során jelentkező korlátok kerülnek bemutatásra.

A robbanásvédelmi és villamos biztonsági felülvizsgálatok szabályozási és szabványi rendszere alapvetően teljes körű és tételes ellenőrzési logikára épül. A gyakorlati végrehajtás során számos olyan üzemeltetési, technológiai és szervezési körülmény jelenhet meg, amely a vizsgálatok tényleges végrehajtását jelentősen befolyásolja.

A potenciálisan robbanásveszélyes térségekben alkalmazott berendezések egy része folyamatos technológiai üzemben működik. Egyes berendezések kizárólag leállított állapotban vizsgálhatók, míg más esetekben a hozzáférhetőség korlátozott magasban történő telepítés, technológiai beépítettség vagy egyéb üzemeltetési körülmények miatt. A gyakorlatban ezért rendszeresen előfordulnak olyan helyzetek, amikor egy adott berendezés vagy kialakítási részlet vizsgálata az adott időpontban nem hajtható végre teljeskörűen.

Ezek a körülmények azonban nem oldják fel a felülvizsgálatok tételes végrehajtásának követelményét. A robbanásvédelmi megfelelőség ugyanis minden egyes érintett berendezésre és védelmi intézkedésre egyedileg értelmezendő, amelyből következően a tényleges állapot is kizárólag egyedi vizsgálatok útján értékelhető. Az olyan gyakorlati megjelölések, mint például az „üzemben volt”, „nem hozzáférhető”, „magasan telepített”, vagy „vizsgálatkor nem ellenőrizhető” önmagukban nem feltétlenül biztosítanak elegendő alapot a megfelelőség egyértelmű igazolásához. Mindezek olyan állapotot jelölnek, amelyben a tényleges robbanásbiztonsági állapot részben vagy egészben ismeretlen marad.

A robbanásvédelmi állapot megfelelő értékelése ezért számos esetben nem korlátozható kizárólag dokumentációs vagy szemrevételezéses megfelelőség-ellenőrzésre. A

tényleges műszaki állapot értelmezése sok esetben részletes helyszíni ellenőrzést, megbontást, működési körülmények közötti vizsgálatot, valamint ismételt vagy külön szervezett ellenőrzési tevékenységet igényelhet. A vizsgálatok teljességének biztosítása ezért nem kizárólag műszaki, hanem egyidejűleg szervezési és üzemeltetési feladat is.

A gyakorlati korlátok következtében a gyakorlatban kialakulhat olyan helyzet, amelyben a dokumentált megfelelőség és a tényleges robbanásbiztonsági állapot egymástól részben eltér. A felülvizsgálati dokumentáció ilyen esetekben elsősorban a rendelkezésre álló vizsgálati körülmények között értékelhető állapotot tükrözi, miközben a teljes robbanásbiztonsági állapot egy része nem, vagy csak korlátozottan ismert. Ez különösen jelentős kockázatot hordozhat olyan rendszerek esetében, ahol a védelmi intézkedések megfelelősége jellemzően részletes műszaki ellenőrzéssel értelmezhető.

A robbanásvédelmi felülvizsgálatok gyakorlata ezért nem kizárólag a megfelelőség dokumentálásának kérdése, hanem egyidejűleg annak problémája is, hogy a tényleges robbanásbiztonsági állapotról milyen mélységű és megbízhatóságú információ áll rendelkezésre az adott időpillanatban.

A ROBBANÁSBIZTONSÁGI ÁLLAPOT IDŐBELI ÉRTELMEZÉSÉNEK KORLÁTAI

A robbanásvédelmi felülvizsgálatok jelenlegi gyakorlata alapvetően időszakosan rögzített állapotképek formájában jeleníti meg a robbanásbiztonsági megfelelőséget. A felülvizsgálati jegyzőkönyvek jellemzően az adott vizsgálati időpontban feltárt hibákat, hiányosságokat és megfelelőségi állapotokat dokumentálják, miközben korlátozottan értelmezhető a robbanásbiztonsági állapot időbeli változása, valamint a feltárt hibák fennmaradásának dinamikája.

A jelenlegi gyakorlatban alkalmazott megfelelőségi kategóriák — például a „megfelelt”, „nem megfelelt”, „súlyos hiba” vagy „karbantartandó” jellegű minősítések — elsősorban statikus állapotértékelést tesznek lehetővé. A kategóriák mindemellett önmagukban korlátozott információt hordoznak arról, hogy az adott hiányosság milyen mértékben befolyásolja a teljes robbanásbiztonsági állapotot, illetve annak időbeli alakulását.

A robbanásvédelmi felülvizsgálatok során feltárt hibák súlyosságának értelmezése jelenleg jelentős mértékben szakmai mérlegelésen alapul. A vonatkozó jogszabályi és szabványi környezet részletes műszaki követelményeket fogalmaz meg a megfelelőségre vonatkozóan, ezzel együtt korlátozottan állnak rendelkezésre olyan egységes módszertani eszközök, amelyek objektív és ismételhető módon támogatnák a feltárt hiányosságok súlyosságának összehasonlítható értékelését. Ebből következően ugyanazon hibatípus különböző felülvizsgálatok vagy különböző szakmai gyakorlatok során eltérő súlyossági megítélés alá eshet.

A robbanásbiztonsági állapot időbeli értelmezése nem azonosítható közvetlen módon a klasszikus kockázatértékelési módszerek alkalmazásával. A probléma elsődlegesen nem a robbanási esemény bekövetkezési valószínűségének és következményeinek számszerű meghatározása. A probléma a jogszabályi és szabványi követelményekhez viszonyított robbanásbiztonsági állapot, annak változása, valamint a feltárt hibák fennmaradásának időbeli értelmezése. A zónabesorolásból, a hibák jellegéből vagy a potenciális gyújtóforrás-

képződés lehetőségéből fakadó szempontok természetesen hordoznak biztonsági jelentőségű információkat, a vizsgálat célja azonban nem klasszikus kockázatszámítás, hanem a robbanásbiztonsági állapot és annak időbeli alakulásának értelmezhetősége.

A jelenlegi felülvizsgálati rendszer további korlátja, hogy a hibák fennmaradásának és ismételt előfordulásának időbeli értelmezése jellemzően nem válik a megfelelőségértékelés közvetlen részévé. A felülvizsgálati jegyzőkönyvek alapvetően az adott időpontban fennálló állapotot rögzítik, miközben korlátozottan követhető, hogy egy adott hiányosság milyen időtartamon keresztül marad fenn, milyen gyakorisággal tér vissza, illetve a végrehajtott javító intézkedések milyen tartós hatást gyakorolnak a robbanásbiztonsági állapotra.

A robbanásbiztonsági állapot időbeli értelmezésének korlátozottsága különösen jelentős a javítási időkeretek meghatározása szempontjából. A javításra adható idő meghatározása ugyanis nem kizárólag az adott időpillanatban fennálló állapot értékelését igényli, hanem annak mérlegelését is, hogy a feltárt hiányosság a robbanásbiztonsági állapot időbeli alakulását milyen módon befolyásolja. Ennek ellenére jelenleg korlátozottan állnak rendelkezésre olyan objektív eszközök, amelyek a robbanásbiztonsági állapot változásának dinamikáját, a hibák fennmaradását vagy a javítási intézkedések eredményességét időben értelmezhető módon támogatnák.

Ebből következően a jelenlegi felülvizsgálati gyakorlat számos esetben elsősorban a megfelelőség aktuális állapotának dokumentálását teszi lehetővé, miközben korlátozott információ áll rendelkezésre arról, hogy a robbanásbiztonsági állapot milyen irányban és milyen ütemben változik az üzemeltetés során.

AZ IDŐBELI ÁLLAPOTÉRTELMEZÉS SZEREPE A ROBBANÁSVÉDELEMBEN

A robbanásbiztonsági állapot dinamikus jellegéből következően az idődimenzió figyelembevétele nem opcionális elem, hanem az értelmezés egyik alapfeltétele.

A robbanásbiztonsági állapot dinamikus jellegéből következően a biztonsági szint fenntartása nem kizárólag az aktuális megfelelőségi állapot értékelését, hanem annak időbeli változásának értelmezését is szükségessé teszi. A jelenlegi felülvizsgálati rendszer elsősorban időszakosan rögzített állapotképeket biztosít, miközben korlátozottan értelmezhető, hogy az adott robbanásbiztonsági állapot milyen irányban és milyen ütemben változik az üzemeltetés során.

A feltárt hiányosságok fennmaradása, ismételt előfordulása vagy hosszú időn keresztül történő jelenléte önmagában is lényeges információt hordozhat a robbanásbiztonsági állapot alakulásáról. Egy adott hiba ismételt megjelenése vagy több felülvizsgálati cikluson keresztül történő fennmaradása nem kizárólag műszaki problémára utalhat, hanem az üzemeltetési, karbantartási vagy szervezeti folyamatok működéséről is információt hordozhat. Hasonló módon a hibák számának, jellegének vagy súlyosságának időbeli változása szintén alkalmas lehet a robbanásbiztonsági állapot alakulásának közvetett értelmezésére.

A javításra adható időkeretek meghatározása szintén olyan terület, ahol az idődimenzió értelmezése különös jelentőséggel bír. A javítási döntések ugyanis nem kizárólag az adott időpontban fennálló megfelelőségi állapotra épülnek, hanem arra a feltételezésre is, hogy az adott hiányosság milyen módon befolyásolhatja a robbanásbiztonsági állapot későbbi alakulását. Ennek ellenére a jelenlegi gyakorlat korlátozott objektív eszközt biztosít

a robbanásbiztonsági állapot időbeli változásának vagy a javító intézkedések tényleges eredményességének értékelésére.

A robbanásvédelmi felülvizsgálatok során keletkező nagymennyiségű műszaki adat lehetőséget teremthet olyan időfüggő állapotértelmezési megközelítések kialakítására, amelyek túlmutatnak az egyszeri megfelelőségértékelés logikáján. Az ismételt felülvizsgálatok eredményeinek összehasonlító elemzése lehetőséget adhat többek között a hibák fennmaradásának, az állapotváltozások dinamikájának, valamint a javító és karbantartó tevékenységek hatásának értelmezésére.

Mindez nem a klasszikus robbanási kockázat számszerű meghatározását célozza, hanem a robbanásbiztonsági állapot időbeli értelmezhetőségének javítását, valamint a felülvizsgálati és üzemeltetési döntések objektívebb támogatását. Az időfüggő állapotértelmezési megközelítések ezért hozzájárulhatnak a robbanásbiztonsági állapot fenntartásának tudatosabb és visszacsatoltabb műszaki gyakorlatához.

A jelenlegi felülvizsgálati gyakorlat korlátai következtében korlátozottan ismert, hogy a robbanásbiztonsági állapot időben milyen természetű változásokat mutat, a feltárt hiányosságok milyen arányban és időtartamon keresztül maradnak fenn, valamint a javító és karbantartó intézkedések milyen tényleges hatást gyakorolnak a biztonsági állapot alakulására. Ebből következően a robbanásvédelmi szabályozási és felülvizsgálati rendszer gyakorlati érvényesülésének hatásossága is csak korlátozottan értelmezhető időbeli összefüggéseiben.

Az időfüggő állapotértelmezési megközelítések ezért nem kizárólag részletesebb műszaki állapotképet tehetnek lehetővé, hanem hozzájárulhatnak a robbanásbiztonsági állapot alakulásának pontosabb megértéséhez, valamint a javító, karbantartó és üzemeltetési gyakorlatok tudatosabb visszacsatolásához és fejlesztéséhez is.

ÖSSZEFOGLALÁS

Az összefoglalás a tanulmány főbb megállapításait és azok biztonságtudományi jelentőségét foglalja össze.

A robbanásbiztonság fogalma a gyakorlatban nem értelmezhető egyetlen statikus, időtől független állapotként. A műszaki rendszerek, az üzemeltetési környezet, a szervezeti működés, valamint az emberi tényezők együttesen folyamatosan változó állapotot hoznak létre, amelynek biztonsági szintje időben természetes módon módosul. A biztonság így nem pusztán egy adott időpillanatban fennálló megfelelőség, hanem egy dinamikusan fenntartandó rendszerállapot.

A biztonságtudomány humán- és társadalomtudományi megközelítései rámutatnak arra, hogy a biztonság nem kizárólag műszaki kategória, hanem társadalmi normákhoz, szervezeti működéshez, együttműködéshez, kommunikációhoz és alkalmazkodási folyamatokhoz is kapcsolódó jelenség. A társadalmi és szervezeti normák szerepe a robbanásvédelem területén is egyértelműen megjelenik: a szabványok, a felülvizsgálati rendszerek, a karbantartási gyakorlatok és az üzemeltetési fegyelem együttesen alakítják a tényleges robbanásbiztonsági állapotot.

A vizsgálatok arra is rámutatnak, hogy a formális megfelelőség és a tényleges biztonság nem minden esetben esik egybe. A szabványi megfelelőség megléte önmagában nem garantálja, hogy egy rendszer robbanásbiztonsági szempontból hosszú távon is megfelelő állapotban marad. A hibák fennmaradása, az ismétlődő hiányosságok, valamint a javítások

elmaradása vagy késedelme fokozatos állapotromláshoz vezethet, még akkor is, ha a rendszer alapvető technológiai funkcióját továbbra is képes ellátni.

Mindezek alapján a robbanásvédelem korszerű értelmezése indokolja az idődimenzió és az állapotváltozások figyelembevételét. A felülvizsgálatok eredményei nem csupán egy adott időpillanat megfelelőségét írják le, hanem alkalmasak lehetnek a robbanásbiztonsági állapot időbeli alakulásának, romlási tendenciáinak és a beavatkozások hatékonyságának értelmezésére is. Ez egyúttal indokolja olyan módszertani megközelítések alkalmazását, amelyek a robbanásbiztonságot nem statikus megfelelőségi kategóriaként, hanem folyamatosan változó, monitorozható és értékelhető rendszerállapotként kezelik.

FELHASZNÁLT IRODALOM

[1] EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA, *1999/92/EK irányelv, a robbanásveszélyes légkör kockázatának kitett munkavállalók biztonságának és egészségvédelmének javítására vonatkozó minimumkövetelményekről*. 2000.

[2] EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA, *2014/34/EU irányelv, a robbanásveszélyes légkörben való használatra szánt felszerelésekre és védelmi rendszerekre vonatkozó tagállami jogszabályok harmonizációjáról (átdolgozás)*. 2016.

[3] Országgyűlés, *1993. évi XCIII. törvény a munkavédelemről*. 2026.

[4] Országgyűlés, *1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról*. 2026.

[5] Nemzetgazdasági Miniszter, *40/2017. (XII. 4.) NGM rendelet az összekötő és felhasználói berendezésekről, valamint a potenciálisan robbanásveszélyes közegben működő villamos berendezésekről és védelmi rendszerekről*. 2026.

[6] EURÓPAI BIZOTTSÁG, *2022/1668 EU végrehajtási határozat, a robbanásveszélyes légkörben való használatra szánt felszerelésekre és védelmi rendszerekre vonatkozóan a 2014/34/EU európai parlamenti és tanácsi irányelv támogatása céljából kidolgozott harmonizált szabványokról*. 2022.

[7] Belügyminisztérium, *54/2014 BM rendelet az Országos Tűzvédelmi Szabályzatról*. 2025.

[8] C. Kollár, „A BIZTONSÁG FONTOSABB FOGALMAI”, *Biztonságtudományi Szemle*, sz. 2025. VII. évf. 1. szám, márc. 2025, doi: https://doi.org/10.12700/btsz.2025.7.1.15.

[9] J. Geng, S. Muré, M. Demichela, és G. Baldissone, „ATEX-HOF Methodology: Innovation Driven by Human and Organizational Factors (HOF) in Explosive Atmosphere Risk Assessment”, *Safety 2020*, köt. 6, sz. 1, o. 21, 2020, doi: https://doi.org/10.3390/safety6010005.

[10] A. Adriana és S. Burian, „Dynamics of the standardization process for explosive atmospheres”, előadás MATEC Web of Conferences, 2024. [Online]. Elérhető: https://doi.org/10.1051/matecconf/202438900052

[11] T. Csaszar, S. Burian, C. Colda, és E. Ghicioi, „Practical aspects regarding the evaluation of explosion protected equipment”, előadás MATEC Web of Conferences, 2021. [Online]. Elérhető: https://doi.org/10.1051/matecconf/202134201011

[12] M. Leitner, „Technológiai üzemállapotok figyelembevétele robbanásvédelmi kockázatértékelés során”, in *Mérnöki Szimpózium a Bánkin*, in ATT60. , Óbudai Egyetem, 2023, o. 308-313. [Online]. Elérhető: http://bgk.uni-obuda.hu/esb

[13] MAGYAR SZABVÁNYÜGYI TESTÜLET, „MSZ EN 60079-17 Robbanóképes közegek 17. rész: Villamos berendezések felülvizsgálata és karbantartása (IEC 60079-17:2024)”. 2024.
[14] OTSZ, *TvMI 13.5:2025.02.01. Tűzvédelmi Műszaki Irányelv, Robbanás elleni védelem*. 2025. [Online]. Elérhető: https://www.katasztrofavedelem.hu/application/uploads/documents/2024-12/84966.pdf
[15] FMM–ESZCSM, *3/2003. (III. 11.) FMM–ESZCSM együttes rendelet a potenciálisan robbanásveszélyes környezetben levő munkahelyek minimális munkavédelmi követelményeiről*. 2008.
[16] OTSZ, *TvMI 7.7.:2026.02.01. Tűzvédelmi Műszaki Irányelv, Villamos berendezések, villámvédelem és elektrosztatikus feltöltődés elleni védelem*. 2026. [Online]. Elérhető: https://www.katasztrofavedelem.hu/application/uploads/documents/2025-12/86701.pdf
[17] MAGYAR SZABVÁNYÜGYI TESTÜLET, „MSZ EN 1127-1:2019 Robbanóképes közegek. Robbanásmegelőzés és robbanásvédelem. 1. rész. Alapelvek és módszertan”. 2019.
[18] Magyar Szabványügyi Testület, „Tévhitek és tények”. [Online]. Elérhető: https://www.mszt.hu/hu-hu/tevhitek-es-tenyek
[19] Országgyűlés, *259/2011. (XII. 7.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról*. 2025.
[20] Országgyűlés, *489/2017. (XII. 29.) Korm. rendelet a tűzvédelmi hatósági eljárások általános és különös szabályairól*. 2024.
[21] A. Zsarnovszki és B. Elek, „Changes in the Safety Level of Potentially Explosive Industrial Technologies in Practice”, *PCS Science 2023*, o. 57–69, 2023.
[22] A. Zsarnovszki és B. Elek, „ROBBANÁSVESZÉLYES IPARI TECHNOLÓGIÁK BIZTONSÁGI KÖVETELMÉNYEINEK ÉRVÉNYESÜLÉSE A GYAKORLATBAN”, *Biztonságtudományi Szemle*, sz. 2024. VI. évf. 4. szám, o. 127-142., 2024, doi: https://doi.org/10.12700/btsz.2024.6.4.127.
[23] N. Daruka, „Critical Infrastructure Risks from Sabotage”, in Critical Infrastructure Protection: Advanced Technologies for Crisis Prevention and Response. Dordrecht: Springer Netherlands, 2025, o. 129–139.
[24] L. Moldovan, „Considerations regarding the inspection of equipment designed for use in potentially explosive atmospheres”, előadás MATEC Web of Conferences, 2021. [Online]. Elérhető: https://doi.org/10.1051/matecconf/202134204002

DOI: https://doi.org/10.12700/btsz.2026.8.2.85

CURRENT CHALLENGES OF HUNGARIANISM (FROM THE CHANGE OF REGIME TO THE PRESENT DAY)

A HUNGARIZMUS AKTUÁLIS KIHÍVÁSAI (A RENDSZERVÁLTÁSTÓL NAPJAINKIG)

BOROSS Zsigmond Attila[1]

Abstract

Following the regime change, Hungarism reemerged in Hungary, with several sizable organizations forming and two attempts made to seize power. These attempts were successfully prevented thanks to the diligent investigative work of national security experts, saving the lives of multiple public figures, although the general public remains largely unaware of the threat. This period is particularly associated with István Győrkös, Albert Szabó, and György Ekrem Kemál, while in the new millennium, in the absence of charismatic leadership, only smaller Hungarist organizations continue to operate, with Diána Bácsfi being the only widely recognized name among the public. The flexible application of Hungarist ideology –overt or covert – can still be observed during periods of societal crisis. Rival intelligence services sought to exploit these groups to disrupt social stability. A crucial objective for national security and law enforcement agencies is to strengthen societal security awareness, enabling the timely recognition of potential threats.

Keywords

Hungarism, Violence, Attempts to seize power, Counter-extremism, Societal security, Security awareness

Absztrakt

A rendszerváltást követően újjáéledt a hungarizmus Magyarországon. Több jelentős létszámú szervezet alakult, és két alkalommal megkísérelték átvenni a hatalmat is. A nemzetbiztonsági szakemberek sikeres felderítőmunkája révén sikerült mindezt megakadályozni. Több közszereplő ennek köszönheti az életét, ugyanis kivégzésüket tervezték. Ezek veszélyességével a közvélemény nincs tisztában. Győrkös István, Szabó Albert és Ekrem Kemál György neve fémjelzi ezt az időszakot. Az új évezredben – karizmatikus vezető hiányában – csak kisebb létszámú hungarista szervezetek működnek. A közvélemény számára szinte csak Bácsfi Diána neve mond valamit. A hungarista ideológia – nyílt vagy leplezett – rugalmas felhasználásával, alkalmazásával találkozhatunk válságjelenségek idején. Ellenérdekelt titkosszolgálatok fel akarták használni ezeket a szervezeteket a társadalmi béke megbontására. A nemzetbiztonsági, rendvédelmi szervek, célja kell, hogy legyen – a veszély időben történő felismerése végett – a társadalom biztonságtudatosságának erősítése.

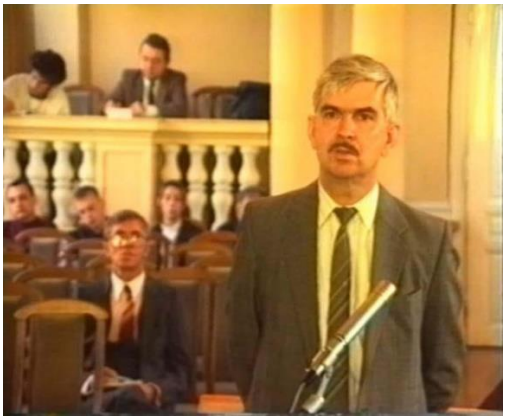
Kulcsszavak

hungarizmus, erőszak, hatalomátvételi törekvések, extrémizmus-elhárítás, társadalombiztonság, biztonságtudatosság

[1] attila.zsigmond.boross@vih.gov.hu | ORCID: 0000-0001-7941-9194 | Senior Government Counsellor, Defence Administration Office| hivatali főtanácsos, Védelmi Igazgatási Hivatal

BEVEZETÉS

Az előző rész a hungarizmus kialakulását, eszméjét és hatalomra jutását mutatta be. Láthattuk, hogy Szálasiék halála után itthon szinte eltűnt, viszont az emigrációban a felszínen áramlott a nemzetiszocializmus magyar gyakorlata. A rendszerváltás idején megvalósuló politikai pluralizmus tulajdonképpen zöld utat adott a demokrácia felszámolásában érdekelt erők újjáélesztésének is. A múlt és „jelen" közötti kapcsolatot – az első hungarista puccskísérletnél exponálódott – Bosnyák Imre jelenítette meg legkézzelfoghatóbban. A rendszerváltást követő évtized átmenetiségét az előzőekben már bemutatott Győrkös István kiteljesedése, valamint további – nemegyszer önjelölt – hungarista vezetők színrelépése jellemezte.



1. ábra: Győrkös István (Forrás: https://magyarnarancs.hu/riport/s-bajtars-101675)

A cselekvéskényszer új, valós program nélküli, egyre jelentéktelenebb szervezetek „pillanatnyi" feltűnését hozza magával. A közvélemény alig érzékelte, hogy mindeközben két hatalomátvételi kísérlet és egy rendőrgyilkosság is köthető a hazai hungarista erőkhöz.

A publikációban felhasznált forrásmunkák között a tudományos hátterű művek szerepelnek a felhasznált irodalom listájában, míg az idézett propagandaanyagoknak helyet adó kiadványok megjelölése pusztán zárójelben szerepel.

GYŐRKÖS ISTVÁN HATALOMÁTVÉTELI TÖREKVÉSE – 1992

Miként korábbi tanulmányomban már szerepelt [1], „a Gottfried Küssel nevéhez kapcsolódó osztrák neonáci puccskísérlet felderítése során a külföldi hatóságok azonosították a magyar nemzetiszocialista vezető személyét és militáns szerepvállalását, így a magyar társszervekhez fordultak. Mivel Győrkös már látókörbe került az előző években, kizárólag az ellenőrzését kellett szorosabbra vonni. A nehezen kiismerhető, ötletszerűségei által vezetett hungarista vezető kontrollja a nemzetbiztonsági szakma tapasztaltabb munkatársainak bevonását igényelte. [2]

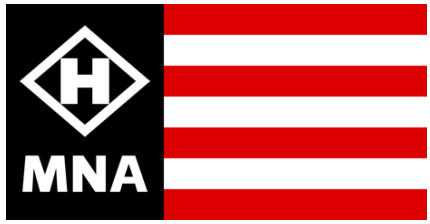
Győrkös tényleges veszélyességét tükrözte, hogy a Nemzetbiztonsági Hivatal és a Katonai Biztonsági Hivatal együttes feljelentésére az Országos Rendőr-főkapitányság 1992 januárjában nyomozást rendelt el a régi Büntető Törvénykönyv egy új törvényi tényállása [3] alapján, *„az alkotmányos rend erőszakos megváltoztatása"* alapos gyanúja miatt Győr-

kös István és hat társa ellen. Győrkös lakásán házkutatást tartottak, ahol egy szovjet gyártmányú karabélyt, 500 lőszert, katonai felszerelést és jelentős mennyiségű nemzetiszocialista, hungarista propagandaanyagot foglaltak le. [1] [4] [5] [6] [7]

A vizsgálatot segítette az I. rendű vádlott vallomása, nyílt politikai véleményvállalása, miszerint: „*Mindig nemzetiszocialista gondolkodású voltam. Hittem és hiszek a nemzetiszocializmus nemzetfelemelő erejében. Vártam a rendszerváltást, úgy gondolva, hogy a demokratikus változások következtében szabadon, legálisan lehetőségem nyílik arra, hogy ezért az eszméért valamit tehessek. Célomat legálisan, becsületesen akartam megvalósítani, de erre a rendszerváltás utáni események nem adtak lehetőséget. Azok a diszkriminatív alkotmánycikkelyek, amelyek oly jellemzőek a sztálini típusú alkotmányokra, nem változtak, továbbra sem nyílt lehetőség a legális munkára. Sok tépelődés után, mert fel tudtam mérni annak a lépésnek a következményét, amit meg akartam tenni, elhatároztam, hogy tőlem telhetően elkövetek mindent annak érdekében, hogy a nemzetiszocialista gondolat legális lehetőséget kapjon a létezésére. Tudtam és vallom, hogy ez csak törvényes keretek között, a demokrácia játékszabályainak betartásával lehetséges, ezért ennek a küzdelemnek az alapfeltételévé a felvilágosító propagandamunkát tettem.”* [1] [8]

Fontosnak tartottam, és ma is fontosnak tartom kiemelni, hogy „a vizsgálat lefolytatása során megváltozott a bűncselekmény minősítése. A nehezen bizonyítható államellenes bűncselekménnyel szemben a kisebb társadalmi veszélyességű, közösség elleni izgatás bűntett [9] elkövetésének alapos gyanúja erősödött meg, ezért az őrizetbe vétel után három nappal már szabadlábra is helyezték a gyanúsítottakat. A nyomozás megállapította, hogy Győrkös három fiával, egy unokaöccsével, valamint a család két barátjával illegálisan alapította meg a Magyar Nemzetiszocialista Akciócsoportokat. Tevékenységük profilját (a bíróság értelmezése és indoklása szerint) az Amerikai Egyesült Államokban, az NSDAP/AO (a lincolni székhelyű szervezet neve: Nemzetiszocialista Német Munkáspárt/Külföldi Újjáépítési Tagozata) által előállított kiadványok, röplapok terjesztése, plakátok kiragasztása jelentette. Ítéletében a Győri Városi Bíróság Győrkös István elsőrendű vádlottat bűnösnek találta lőfegyverrel és lőszerrel való visszaélés, valamint közösség elleni izgatás vádpontokban, ezért egy év börtönbüntetésre ítélte, amelynek végrehajtását ötévi próbaidőre felfüggesztette. A többi vádlott ennél is enyhébb büntetést kapott.” [1]

Mindezeket követően alapította meg Győrkös a Magyar Nemzeti Arcvonalat, a következő negyed évszázad legjelentősebb militáns hungarista szervezetét.



2.ábra: a Magyar Nemzeti Arcvonal jelképe

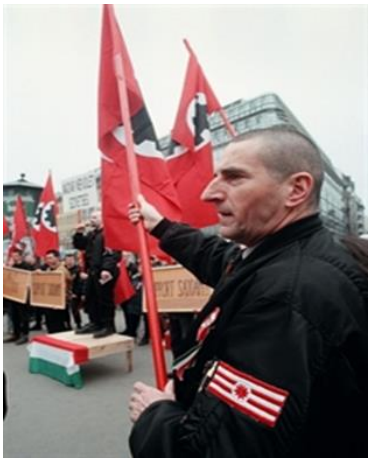
MAGYAR NÉPJÓLÉTI SZÖVETSÉG

Mintegy, a közvélemény felrázása céljából lépett a politikai küzdőtér emelvényére 1993-ban Szabó Albert. Az addig felszín alatt működő, tevékenykedő nemzetiszocialista szervezetek ekkor vállaltak először hangos, demonstratív közszereplést. Szabó Albert a

nyolcvanas évek közepén hagyta el hazánkat, és Ausztráliában telepedett le. Évek során egyre erősebb kapcsolatot alakított ki az ottani politizáló magyarsággal, köztük főként a hungarizmust valló, korosodó nyilas aktivistákkal. Részt vett a politikai, vallási témájú rendezvényeken. Hallgatóból fokozatosan szervező lett. 1993 elején tért haza, de politikai ellenfelei (elsősorban Csurka István és a MIÉP), volt ideiglenes szövetségesei (MNA) szinte egyből támadták, provokátort gyanítva személyében. A heves bírálatok mögött húzódik az a tény, hogy Szabó igyekezett elhallgatni életének azon szakaszát, amelyet Ausztrália után és a hazaérkezés előtt Izraelben töltött el... Ellenfelei szerint fellépése, képviselt nézetei alapján jelentős jogi szankciókat érdemelt volna, amelyek elmaradása miatt a hatalom és a „provokátor" közötti kapcsolatot látták bizonyítva.

Tény, hogy direkt szerepvállalása, mind külsőségeiben, mind megfogalmazott elveiben, céljaiban, bátrabban azonosult a hungarista elődökkel, mint riválisai. Közérthető, programja leegyszerűsített, ellenségképe világos volt, mindezek hatására szimpatikus lett a „nacionalista" fiatalság számára. Győrköstől eltérően, programjának kiindulópontja nem egy összetett idea, hanem a nemzet volt. Az összes gondolatot e fogalom és a megvalósítandó célok köré szervezte.

1993-ban megalakította a már nevében is figyelemfelkeltő Világnemzeti Népuralmista Pártot. Aktivistái és maga Szabó is a harmincas évek militarista hangulatát tükröző ruházatát öltötték fel: sötét (általában) szürke ing, fekete nyakkendő, fekete nadrág, esetleg „antant-szíj". Szimbólumként megjelent az un. sumér csillag, amely Árpád-sávok közepén kapott helyet. Az új, összetett jelkép egyben zászlóvá és karszalag-motívummá is vált. A demonstrációk során az egyenruhás aktivisták lobogókkal, politikai témájú tablókkal vonultak fel. Jellemzően egyközpontú, Szabó Albert által képviselt szervezet volt. A nyilas elődök feltétlen elismerése, a jelképek és a program nyílt felvállalása 1994-ben a párt feloszlatásához vezetett.



3.ábra: Szabó Albert (karján a Világnemzeti Népuralmista Párt, zászlóján a Magyar Népjóléti Szövetség jelképe) (Forrás: http://plajbasz.blogspot.com/p/magyar-naci-kronologia.html)

Az év tavaszán Szabó is részt vett a Magyarországi Hungarista Mozgalom megalakításában. Ezután új szervezetet is létrehozott, Magyar Népjóléti Szövetség (MNSZ) néven, amellyel a célja a még közérthetőbb, a lakosság számára elfogadhatóbb gondolatok megfo-

galmazása volt. E szellemben alkottak új jelképet, melyen piros alapon, fehér körben ábrázolt, fekete fogaskerék található. A választott szimbólummal Szabó és az MNSZ kifejezte a korábban is kimutatott vonzódását a hungarizmuson túl általában a nemzetiszocialista ideológia, szervezetek irányába. A fogaskerék közérthetősége, valamint a forgalmas közlekedési pontokon megtartott „lakossági fórumok" a mindennapos kapcsolat, a kontaktus kiszélesítését szorgalmazták.

Bár e szervezet is eszmeiségének kizárólagosságát hangoztatta, a sorozatos jogi súrlódások, esetleges taktikázás miatt, demonstratív jogkövető magatartás volt megfigyelhető részükről. Ideológiájában a hungarizmuson kívül, illetve arra épülve a nemzetiszocializmus aktualizált módozata, az un. szociálnacionalizmus szerepelt. Témájuk fontos részét képezte az őstörténet-kutatásokon, okkult tudományokon alapuló Magyar Hit képviselete, népszerűsítése. A magyarázatok során elsődlegesen itt kaptak teret a rasszista, antiszemita nézetek. Mindenesetre elmondható, hogy az 1990-es évek közepén Szabó és szervezete, az MNSZ rendelkezett a legkiterjedtebb, legszervezettebb országos bázissal és támogatói körrel hungarista vonalon. Látványos visszaszorulását kompromittálódása, illetve a többször már kilátásba helyezett jogi szankciók érvényesítése eredményezte.

SZABÓ ALBERT PERE

Az 1993-ban hazatért Szabó Albert politikai szereplését a kezdetektől fogva nagy érdeklődéssel figyelte a közvélemény, ugyanis minden megnyilvánulása magában hordozta a jogi szankcionálás lehetőségét. Az általa létrehozott Világnemzeti Népuralmista Párt valószínűleg a külföldről érkező támogatások érdekében igyekezett mindig reflektorfényben sütkérezni. A megtartott sajtótájékoztatók és „történelmi előadások" azonban számos ponton felvetették a jogsértés megvalósítását.

A közösség elleni izgatás (régi Btk. 269. §), valamint az önkényuralmi jelkép használatának (régi Btk. 269/B. §) megvalósítása fogalmazódott meg cselekményei kapcsán, azonban az eljárás során a Magyar Köztársaság Legfelsőbb Bírósága másodfokon a vádlottat felmentette. [10] Figyelmet érdemel, hogy a védelem leginkább az Alkotmánybíróság nagyfokú önállóságáról tanúskodó, liberális jogértelmezésére építhetett. Így fordulhatott elő, hogy tulajdonképpen az ideológiai/politikai ellenfélre támaszkodva kerülhetett ki győztesen az eljárás alól a hungarista párt vezetője.

Mint az elsőfokú bíróság is kifejtette, valamely nemzetiségre, vagy fajra tett lealacsonyító kifejezések akkor büntethetők csak, ha gyűlöletre uszításban jelentkeznek. Az Alkotmánybíróság időközben hatályon kívül helyezte a Btk. 269. § (2.) bekezdését: *„Aki nagy nyilvánosság előtt a magyar nemzetet, valamely nemzetiséget, népet, felekezetet vagy fajt sértő vagy lealacsonyító kifejezést használ, vagy más ilyen cselekményt követ el, vétség miatt /.../ büntetendő."*

Az elsőfokú bíróság állásfoglalását minden valószínűség szerint az Alkotmánybíróság ez ügyben megfogalmazott, véleménynyilvánítás kérdésében alkotott álláspontja határozta meg: *„E szabadság az olyan gondolatokat, információkat, elveket és nézeteket is megilleti, amelyek sértőek, meghökkentőek, vagy aggodalmat keltenek."* [11]

Az akkor hatályos Btk. a közösség elleni izgatást a köznyugalom elleni bűncselekmények között helyezte el. A 269 § (1.) bekezdés értelmében:

„Aki nagy nyilvánosság előtt

a) a magyar nemzet vagy valamely nemzetiség,

b) valamely nép, felekezet vagy faj, továbbá a lakosság egyes csoportjai ellen gyűlöletre uszít, büntettet követ el."

Tehát, a bűncselekmény gyanúját felvető magatartás elkövetésének időpontjában a tényállás szerint az uszítás, mint veszélyeztetés-kérdés fennállásának bizonyítása volt a döntő. Az uszításnak azonban nagyobb nyilvánosság előtt kell megtörténnie, amit a népes hallgatóság, illetve a jelenlévő újságírók biztosítottak. A bíróság a gyűlöletre uszítás értelmezésénél továbbra is az Alkotmánybíróság véleményében kifejtetteket [12] vette figyelembe. Mivel Szabó Albert a „történelmi előadásai" során a zsidóságot „pusztán" negatív jelzőkkel illette, de kárt okozó tevékenységre, aktív gyűlöletre nem hívott fel, illetve mivel a Btk. 269. § (2.) bekezdését ekkorra hatályon kívül helyezék, e vádakat ejtették.

Az eljárás során az önkényuralmi jelképek használata (régi Btk. 269/B. §) is megfogalmazódott. E jelképeket a védelem szerint pusztán a „történelmi előadás" szemléltetőeszközeként használták fel, így azok önálló szerepét megkérdőjelezték. Az ominózus nyilaskereszt fénymásolt kiadványon jelent meg, így fekete színével különbözött az eredeti, zöld ábrázolástól. Ráadásul az ábra Szálasi Ferenc 1944. október 15-i hadparancsán szerepelt, így az ezt tartalmazó Út és Cél című lap, közszemlére kitett oldalát már történelmi dokumentumként értelmezték.

A felmentő ítélet 1996. október 30-án emelkedett jogerőre. A sors játéka, hogy Szabó ellen az 1996. október 23-i közszereplése miatt Csurka István, a MIÉP elnöke eljárást indítványozott, mivel a Btk. 269. paragrafusában megfogalmazott tényállást ezúttal is megvalósítottnak vélte. A lefolytatott tárgyaláson Szabó Albertet egy év szabadságvesztésre ítélték, melyet három évre felfüggesztettek.

EKREM KEMÁL GYÖRGY PUCCSKÍSÉRLETE 1997-BEN

Az extrémizmus – terrorizmus összefüggéseit vizsgálva sikerült korábban kimutatnom, hogy a „rendszerváltást követően kialakuló magyarországi politikai extrémizmust kétarcúság jellemezte. A társadalom irányába a kezdeti időben – idealisztikusan – propagandával közelítettek, amely azonban hatástalan maradt, ezért céljaik elérését fegyverszerzés és erőszakos akciók végrehajtására révén tervezték. Győrkös mellett Ekrem Kemál György is ezt a vonalat képviselte.

4.ábra: Ekrem Kemál György
(Forrás: https://hu.wikipedia.org/wiki/Ekrem-Kem%C3%A1l_Gy%C3%B6rgy)

Az 1990-es évek közepétől egyre gyakrabban követtek el robbantásos cselekményeket az országban. Ezeket nem lehet általánosan terrortevékenységként értelmezni, ugyanis az érintettek rendszerint a bűnözői csoportok konfrontálódó tagjai közül kerültek ki. A média által részletesen megjelenített figyelmeztetések és leszámolások mindennapossá váltak, megemelve ezzel a társadalom ingerküszöbét. A Magyar Szocialista Párt és a Szabad Demokraták Szövetsége két-két pártirodája ellen elkövetett csőbombás merényletek így mérsékelt visszhangot keltettek.

- 1997. február 9-én a XIV. kerület Rákosfalva park 1-5. szám alatt lévő szolgáltatóház bejáratánál csőbomba robbant, minek következtében megrongálódott az épületben lévő MSZP-iroda bejárata.
- 1997. március 10-én a tűzszerészeknek sikerült a beállított időpont előtt két perccel hatástalanítani a csőbombát az SZDSZ XVI. kerület Köztársaság utca 6-8. szám alatti irodájának ablakában.
- 1997. április 21-én házilag készített, kisebb erejű pokolgép robbant Újpesten, az MSZP irodájának bejáratánál.
- 1997. június 15-én a tűzszerészek hatástalanítani tudták azt a csőbombát, amelyet az SZDSZ XV. kerületi irodájánál helyeztek el. [13]

A modus operandi, valamint az üzenetként a helyszínen közzétett jelképek egy félreértelmezett nemzeti radikalizmust követő személyi körre utaltak. A Nemzetbiztonsági Hivatal és a Rendőrség mintegy kétéves felderítését, nyomozását követően a Rendőrség az Országos Baleseti Intézet kórboncnokát gyanúsította meg a cselekmények elkövetésével. J. Géza egy orvos ismerősétől vegyszereket akart beszerezni a robbanószerkezetekhez. (Figyelmet érdemel, hogy már ebben az időben az Országos Baleseti Intézetben – J. Géza közelében – dolgozott az a Bartha Tibor főorvos, aki a Securitate ügynökeként az 1980-as években benősült a Tőkés családba, csak azért, hogy – Stelian fedőnéven – jelenthessen Tőkés Lászlóról. Vajon milyen célból települt át Magyarországra?) Ugyancsak fontos momentumnak számított, hogy regisztrált kapcsolatban állt a hazai extrémizmus egyik meghatározó alakjával, Ekrem Kemál Györggyel is. [14] A házkutatás során egy élesítés nélküli csőbombát, öt félkész pokolgépet, egy géppisztolyt lőszerekkel, valamint egy „Terrorizmus" című, illetve egyéb robbantási szakkönyveket talált a rendőrség J. Géza lakásán, illetve munkahelyén. Rejtekhelyként az egyik hullakamra szolgált. [15] A bizonyítás során igazságügyi szakértők ellentmondó szakvéleményt adtak a felhasznált és a gyanúsítottnál fellelt csőbombák azonos eredetének lehetősége kapcsán, így az ítélet kizárólag azok birtoklását szankcionálta – a nehezebben bizonyítható – terrorcselekmény elkövetése helyett.

A csőbombás támadássorozat értelmezéséhez elengedhetetlen a motivációs háttér vizsgálata. Azokban a napokban Ekrem Kemál György és „testőre", Rácz János ellen intézkedéseket készített elő a Rendőrség (ismét csak a Nemzetbiztonsági Hivatal információi alapján). Bár a sajtó [15] magányos elkövetőről tudósított a csőbombás akciók vonatkozásában, az egy időben zajló események és a kimutatható személyes kapcsolatok alapján az egymástól függetlenül tálalt események logikai lánca – valamint egy többszereplős csoport tevékenysége – rajzolódik ki. [16] A J. Géza barátjának számító és Ekrem szűk környezetében feltűnő, személyvédelmi felelősként fellépő Rácz Jánost ugyanis betörés közben tetten érte a rendőrség, aki azonban fegyverhasználat segítségével elmenekült a helyszínről és lakása felé vette az irányt. Hazafelé tartva szembesült azzal, hogy – iratait elhagyta és – a

Kálvin tér környéki otthona körül jelentős rendőri erőket vontak össze, ezért a nyílt utcán fejbe lőtte magát. A lakásán tartott házkutatás során a Központi Bűnüldözői Igazgatóság munkatársai hungarista kiadványok mellett fegyvereket találtak. [15]

Későbbi vádirat szerint tehát, amikor megkezdődött a csőbombás merényletsorozat, akkor Ekrem Kemál György az alkotmányos rend megdöntését készítette elő szűk körben." [13] A félig török származású Ekrem Kemál György (1946-2009) életét alapvetően befolyásolta, hogy édesapját, az '56-os Széna téri hőst, Ekrem Kemált 1957-ben kivégezték, így számára az állam mindenkori ellenséggé vált.

Ekremet 1994-ben – Győrkös István és Szabó Albert társaságában – a Magyarországi Hungarista Mozgalom (HM) társelnökének nevezték ki. A lakásán titkosszolgálati eszközökkel rögzített beszélgetések, továbbá az elsőrendű vádlott levelei, felhívásai, sajtónyilatkozatai, illetve a tanúvallomások bizonyítják, hogy a HM passzivitásával szembesülve, bizonyítási kényszerétől hajtva 1996-ban létrehozta a „Kommunizmus Üldözötteinek Szövetségét (KÜSZ), melynek célja az alkotmányos rend erőszakos, fegyveres megdöntése volt. [17] Még az elsőfokú ítélet szerint sem merült fel soha a vádlottban, hogy eszmerendszerét a demokrácia keretei között valósítsa meg. A meghatározó nemzetiszocialisták szembesültek ugyanis azzal, hogy céljaikat csak részben tudják elérni, ezért az erőszak alkalmazása, mint reális eszköz volt jelen képzetükben. Ezt azonban már nem propagálták." [13] A várt politikai eredmények elmaradása 1997-re erőszakos eszközök alkalmazására ösztökélte a minimális számú követővel bíró „vezetőt".

Illuzórikus elképzeléseire jellemző, hogy azt tervezte, követőivel ráépül az akkor zajló METÉSZ (Mezőgazdasági Termelők Érdekvédelmi Szövetsége) tüntetésekre. Mivel a gazdálkodók nehézgépekkel vonultak fel, Ekrem folyamatosan kampányolt közöttük Budapest blokád alá vétele érdekében. Tervei szerint elfoglalták volna a rádiót, és felkérték volna Göncz Árpád akkori köztársasági elnököt, hogy vezesse a felkelőket a Horn-kormány megdöntésére. A KÜSZ ezt követően hajtotta volna végre a rendőrség és a hadsereg lefegyverzését, a határok lezárását és a numerus clausushoz hasonló törvények megalkotását.

Ekrem nem tervezte békésnek a folyamatot – az apja kivégzése iránti bosszúvágytól és személyes ellenszenvétől fűtve – több személy likvidálását is célul tűzte ki. A „halállistára" így került Berecz János (MSZMP), Horn Gyula (MSZP) és Pető Iván (SZDSZ) politikusok mellé Vitray Tamás sportriporter is. [17]

Tanulságként az olvasók figyelmébe ajánlottam és ajánlom ma is, hogy a „konkrét előkészületek miatt 1997 tavaszán eljárás alá vont Ekrem-Kemál György volt az egyetlen, akit a rendszerváltás után alkotmányos rend elleni fegyveres szervezkedés kísérlete miatt – 2001-ben – öt év próbaidőre felfüggesztett kétéves szabadságvesztésre ítéltek (amelyet egy évre mérsékelt a Legfelsőbb Bíróság). *„Magyarország erős ország, amely megengedheti és meg is kell engednie magának, hogy Ekrem Kemál Györggyel szemben ne a megtorlás, hanem a figyelmeztetés, a megelőzés eszközeit alkalmazza"* – az ítélet szerint." [13] [18]

Figyelmet érdemel, miszerint az államellenes cselekmény elkövetőjével szemben megfogalmazott – elnéző – szemléletű ítéletében a bíróság olyan szempontokat vett figyelembe, minthogy, Ekrem apja 1956-os mártír volt, valamint, hogy csak szűk körben tervezgette a hatalomátvételt. [19] Az enyhe bírósági ítéletek hatására a társadalomban nem tudatosult, hogy a rendszerváltást követően is két alkalommal készítettek elő hatalomátvételt a hungaristák, amelyhez fegyvereket halmoztak fel, és az életellenes erőszakcselekményektől sem riadtak volna vissza.

KISCSOPORTOS FOGLALKOZÁSOK

A 2004-2005-ben aktív Magyar Jövő Csoport Bácsfi Diána vezetésével jött létre. Külsőségeiben, témájában a Szabó Albert-féle vonalat követte. Közterületi fórumaik mellett Churchill városligeti szobrának vörös festékkel történő leöntése és a Budakeszi úton kihelyezett Ságvári emléktábla megrongálása fűződik a nevükhöz. A közvélemény éles reakciója kiváltotta a nemzetiszocialista irányzat más szervezeteinek gyanakvását, akik Bácsfiban – Szabó követőjeként – szintén provokátort láttak. A magyar őstörténettől az ezotéria világáig elkalandozó, mintegy tíz nyelven beszélő Bácsfi a Kard-Kereszt-Korona Szövetség által a tradicionalitással is kapcsolatba került. A Szálasit is magába foglaló vezérkultusz közös platformot teremtett az ultrajobboldali szervezet, valamint a nemzetiszocialista Bácsfi között.

5.ábra: Bácsfi Diána, a Magyar Jövő Csoport vezetője
(Forrás: https://24.hu/poszt-itt/2012/02/13/naci-az-mtv-ben/)

Nemzeti Őrsereg 2007-ben alakult. Tevékenységének elkülönült profilja nehezen értelmezhető. A Magyar Gárdával szoros szövetségben álló szervezet zöldinges tagjai karszalagjaikkal a leventemozgalom és a nyilas pártszolgálatos közötti átmenetet testesítették meg. A főként Észak-Kelet-Magyarországon aktív szervezet (alapvetően Szabolcs-Szatmár-Bereg megyében) legjelentősebb sajtónyilvánosságra a 2008-as szlovákiai (Királyhelmec) demonstrációval tett szert, amikor is a helyi hatóság őrizetbe vette és később kiutasította 28 egyenruhás tagjukat.

6.ábra: Nemzeti Őrsereg (Forrás: https://kuruc.info/r/6/56792)

A Pax Hungarica Mozgalom (2008 – 2017) szintén felvállalta a hungarizmust külsőségeiben, Domokos Endre János, Németberta Péter és Lantos János vezetésével. Jelenlétük a nemzetiszocialista szervezésű rendezvényeken (pl. Becsület napja) általános volt, viszont az ő fellépésük sem tudta dinamizálni a hazai – egyre inkább szűkülő – hungarista bázist.

7.ábra: Pax Hungarica Mozgalom (Forrás: http://www.katolikus-honlap.hu/0904/magyar.htm)

Külsőségeiben kevésbé, viszont céljait tekintve jelen volt a hungarizmus még a 2006-os Kossuth téri demonstrációsorozaton is. A Forradalmi Nemzeti Bizottmány több radikális és extrém vezető aktivistát is közös platform alá szervezett. Így küzdött együtt Toroczkai Lászlóval például Ekrem Kemál György is, akinek azonban érdemi szerep ekkor már jutott.

A másik legjelentősebb Kossuth téri szervezet, a Magyar Nemzeti Bizottság 2006 vezető szervezői, ideológusai között megtaláljuk Halász Józsefet, a Pajzs Szövetség vezetőjét. (A szervezet megnevezése megegyezik a japán tradicionalitás egy meghatározó alakja, fanatikus mártírja, Misima Jukio szervezetének nevével.) A Pajzs Szövetség 2006. október 15-én – a nyilas hatalomátvétel évfordulóján – deklarálta politikai programját, amely a Szálasi által létrehozott Nemzet Akaratának Pártja (NAP) korporációs állam-és társadalomszervezési téziseit képviselte.

8.ábra: A Pajzs Szövetség jelképe

A hazai nemzetiszocialista ideológia és szervezetrendszer kiépültségét tükrözi, hogy szubkulturális szintig hatott a kisugárzása. Ennek egyik fontos intézménye volt a Gede

Testvérek Bt., amely propagandaanyagok kiadásával foglalkozik 1994 óta. A hungarista emigráció egyik legjelentősebb bázisán, Ausztráliában élő Gede Tibor és a magyar fővárosban az üzletet működtető Gede Sándor könyvkiadásra szakosodott. A „hiánypótló" ideológiai kiadványok mellett a könyvesbolt által biztosított találkozási lehetőség is növelte népszerűségüket a mozgalomban.

Tompó László irodalomtörténészként vette át Tudós-Takács János (teológus, filozófus) szellemi örökségét a hazai nemzetiszocialista bázis ideológiai pallérozása területén. A két világháború közötti fajvédő, népi írói és politikai katolicizmus elveit hangoztató Tompó tulajdonképpen hungarista propaganda-felelősként működik. Publicisztikái a Kuruc.info, Hunhir, Szittyakürt oldalain olvashatók.

Az írásnak nem témája az összes militáns, erőszakkész szervezet bemutatása. Kizárólag azokra koncentrál, amelyek működése a hungarista eszmékre hivatkozva zajlik/zajlott. Így maradt ki például a Magyar Gárda, a Betyársereg a Véderő és a Légió Hungária is.

RENDŐRHALÁL

2016. szeptember 24-én Budapesten, a Teréz körút 4. előtt házilag készített robbanószerkezet okozott súlyos, életveszélyes sérülést egy rendőrjárőr két tagjának. A nagy erőkkel folytatott nyomozással párhuzamosan a Rendőrség ellenőrzés alá vonta a hazai militáns szervezetek aktivistáit is. A házkutatások eredményeként MNA tagoknál éles lőfegyvereket, lőszereket és robbanóanyagot foglaltak le.

Miként azt korábbi elemzésben bemutattam, a „Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI) 2016. október 26-án nyílt nyomozási eljárás részeként házkutatást kezdeményezett Győrkös István bőnyi ingatlanában. A bűnügyi munka keretében végrehajtott intézkedés feltehetően mellőzte a nemzetbiztonsági aspektusú kockázatelemzést. Az extrémizmus- és terrorelhárítás szakmai szemlélete elengedhetetlennek tartotta volna ugyanis megvizsgálni azt a folyamatot, amelyben Győrkös István 1999 óta tartó elszigetelődésen ment át. Mint láttuk, a politikai kapcsolatkeresésében még a szélsőbaloldali Magyar Munkáspártig [20] is eljutott egyik fia, ifj. Győrkös István személyes szerepvállalása révén. Szervezete tagsága számára mindez már nem volt elfogadható, ezért a többség 2012-ben a „puccsot" végrehajtva egy párhuzamos MNA-t hozott létre. Szintén nem tudták elfogadni egyre nyíltabb oroszpártiságát, amely a propagandától GRU tagokkal tartott közös airsoft kiképzésekig vált ismertté.

Újabb, immár a magánélet, a család szintjére begyűrűző veszteséget jelentett számára, hogy a következő évben elhunyt az egyik fia, Győrkös Csaba.

A számára szellemi példát, elitet megjelenítő ultrajobboldal egyik legjelentősebb francia képviselője, Dominique Venner szintén ebben az időszakban öngyilkos lett (a melegházasságok franciaországi legalizálása, Európa iszlamizációja miatt) a Notre Dame oltáránál, így tiltakozva teátrálisan a tradicionális értékek pusztulása miatt, és elutasítva mindezzel az általuk illegitimnek tekintett modern állammal és annak intézményeivel való bármiféle együttműködést. Győrkös értékvesztesége így a mozgalmi területtől a szellemi szintig emelkedett rövid idő leforgása alatt.

Az MNA idős vezetője az illegális bevándorlás tömegessé válása idején a „migráns csürhe" [21] elleni fellépést sürgette, viszont ezzel párhuzamosan számára is a fenyegetettség-tudat jelentős erősödését eredményezte, hogy állandóan szembesülhetett az illegális migráció propagált veszélyével. Az idős, militarizmus iránt vonzódó – fegyvermester fia,

Győrkös Kolos révén valószínűleg éles lőfegyvert birtokló – kiábrándult, teljesen befelé forduló fanatikus hungarista vezetőt fent ismertetett előzmények után keresték fel a KR NNI munkatársai 2016. október 26-án. (Az eset tragikusan példázza, hogy milyen eltérő kockázat kapcsolódik egy – a rendőrség által rendszeresen eljárás alá vonható – erőszakos bűnelkövetőhöz, illetve egy nemzetbiztonsági kockázatot jelentő, fanatikus, extrém aktivistához. A bőnyi tragédia a váratlanság számlájára írt felkészületlenség – és intézkedési anomáliák – eredménye. Mindez szemlélteti a nemzetbiztonsági kockázatra adott bűnügyes válaszlépések korlátait, kudarcát.)

Győrkös István az életútja, mozgalmi szerepe és militáns szemlélete alapján joggal kerülhetett a hazai katonai és polgári nemzetbiztonsági szolgálatok, rendvédelmi szervek látókörébe. Személyének, illetve a hozzá fűződő kockázatok értékelésének korlátait jelenheti azonban, ha annak során kizárólag egy félreértékelt aspektus (például bűnügyi) válik meghatározóvá, miként az történhetett a tragikus eseményt megelőzően. Mivel a tényleges szélsőjobboldalt képviselő, tradicionalitás kizárólagosságát hirdető ultrajobboldal elutasítja a modern állam összes intézményrendszerét, Győrkös a szent hit védelmezőjeként fellépő keresztes vitéz, vagy a japán szamuráj példáját követve – beszűkült realitásérzékéből fakadva – elképzelhetetlennek tartotta fegyvere átadását…(Az 1960-as években három alkalommal is irodalmi Nobel-díjra jelölt Misima Jukio 1970-ben erőszakos hatalomátvételt kísérelt meg a követőiből létrehozott félkatonai szervezetre – a Pajzs Szövetségre – támaszkodva. Kudarcával szembesülve rituális öngyilkosságot követett el. Misima személye és példája a Győrkös által csodált ultrajobboldal fundamentalista szemléletének egyik legszemléletesebb megnyilvánulása.)” [1]

Fontosnak tartom azonban megemlíteni, hogy a fogvatartottal 2023-ban készített interjúsorozat során a büntetését töltő Győrkös István következetesen tagadta, hogy ő lőtt volna Pálvölgyi Péter rendőr őrnagyra. Ártatlansága szemléltetésére egy könyv is készült, amely bizonyítási elemeket tartalmaz. [22]

9.ábra: A fogvatartott Győrkös István (a szerző felvétele)

ÖSSZEFOGLALÁS

A hungarizmus és Szálasi Ferenc személye a hazai nemzetiszocialista, valamint rasszista elkötelezettségű személyek és szervezetek számára a legáltalánosabb hivatkozási lehetőség, azonban az összetett történelmi és ideológiai háttérrel, ellentmondásaival általában nincsenek tisztában jelenkori követői. De, mint látható, nem az eszmei letisztultság, vagy a bázis nagysága határozza meg az aktuális hungarista fenyegetéshez kapcsolódó kockázat mértékét.

A történelmi előzmények áttekintése, megismerése és értelmezése többrétegű tapasztalat levonására nyújt lehetőséget. Elsődlegesen az ismeretek bővítése iránt elvárható igényesség kielégítését szolgálhatja, másodsorban azonban a jövő kihívásainak eredményes megválaszolását is támogathatja. Mert bár változnak azok az eszközök és felületek, amelyeken az extrémizmus megnyilvánul, az emberi viselkedés alapvető törvényszerűségei általános érvényűek. A hungarizmus ideológiája mentén megfigyelhető radikalizáció folyamata így egy karizmatikus vezető és már néhány követő esetében is államellenes és terrorcselekmények lehetőségét vetíti előre. A hatáskörrel és illetékességgel bíró rendvédelmi szervek számára a megfelelő jelzőrendszer kialakítása, valamit a keletkezett információk szakszerű elemzése és értékelése jelenthet feladatot a vázolt, nemzetbiztonsági súlyú kockázatok hatékony elhárításában. A társadalom, közvélemény részéről, illetve irányába pedig elengedhetetlen a biztonságtudatosság erősítése.

FELHASZNÁLT IRODALOM

[1] Zs. A. Boross, „Győrkös István, mint a rendvédelem folyamatos célszemélye," *Belügyi Szemle*, no. 6, 108–118, 2018.
[2] Zs. A. Boross, „Humán faktor. Az emberi tényező szerepe az extrémizmus-elhárítás kérdéskörében," *Nemzetbiztonsági Szemle*, no. 2, pp. 139–159, 2014.
[5] F. Dávid, „Nemzeti biztonság és nemzetbiztonság a stratégiaalkotásban," *Nemzetbiztonsági Szemle*, no. 2, pp. 5–22, 2017.
[6] F. Dávid, „Az új évezred nemzetbiztonsági feladatellátásának súlypontjai," *Nemzetbiztonsági Szemle*, no. 1, pp. 213–216, 2015.
[7] F. Dávid, „Biztonságpolitikai hangsúlyok a polgári nemzetbiztonsági szférában 2001 és 2010 között," *Hadtudomány*, no. 1–2, pp. 62–76, 2013.
[8] *Köztársaság*, no. 15, p. 33, 1993.
[10] *Magyartudat*, no. 1, p. 8, 1997.
[13] Zs. A. Boross, „Extrémizmus – terrorizmus (, avagy a politikai szélsőség útja a terrorcselekményig Magyarországon)," *Terror& Elhárítás*, no. 1, pp. 1–19, 2013.
[14] *www.origo.hu/itthon/19990823arendorseg.html.*
[15] *http://www.hetek.hu/belfold/199908/maganyos_farkas_volt_a_parthazak_robbantoja.*
[16] *https://index.hu/belfold/2009/06/14/meghalt_ekrem-kemal_gyorgy/:*
[17] *http://www.origo.hu/itthon/20000320nem.html:*
[18] *http://www.origo.hu/itthon/20010524felfuggesztett.html:*
[19] *http://www.jogiforum.hu/hirek/1121:*
[20] *http://nol.hu/belfold/20121124-hungaristak_es_kommunistak-1348363.*
[21] Dezső András, Munk Veronika: A „migráns csürhe" ellen szervezkedett a rendőrgyilkos. Link: *https://index.hu/belfold/2016/10/26/gyorkos_istvan_portre/*

[22] I. Győrkös, *Kereszttűzben.* Budapest: Világ Magyarsága Kiadó, 2021.

JOGSZABÁLYOK

[3] Az 1978. évi IV. törvény a (régi) Büntető Törvénykönyvről (rBtk.) 139. § (2) bekezdés szerinti alkotmányos rend erőszakos megváltoztatására irányuló előkészület bűntett 1989. évi XXV. törvény 3. §-ával megállapított szövege
[4] 1995. évi CXXV. törvény
[9] Btk. 269. § b) pont szerinti közösség elleni izgatás
[11] 36/1994. (VI.24.) Alkotmánybírósági határozat
[12] 30/1992. (05.26.) Alkotmánybírósági határozat

DOI: https://doi.org/10.12700/btsz.2026.8.2.99

ARTIFICIAL INTELLIGENCE AND USER PROFILING: OVERVIEW AND RISKS

MESTERSÉGES INTELLIGENCIA ÉS FELHASZNÁLÓI PROFILALKOTÁS: HELYZETKÉP ÉS KOCKÁZATOK

BOKROS Anna Dóra[1]

Abstract

The study reviews the current state of AI-based user profiling, the major related events, and the regulatory environment, with particular attention to legislative gray areas, user awareness, and the possibilities for targeted manipulation inherent in the technology. It highlights that user profiling, based on the analysis of data collected across various digital systems, can be used not only for cybersecurity or marketing purposes, but also for optimizing attacks and targeted opinion manipulation. Furthermore, it draws attention to the role of behavioral biometric data processing in user profiling, the composition of users' digital footprints, and the shortcomings and dark patterns used in informing users about the handling of their data.

Keywords

user profiling, targeted opinion manipulation, AI regulation, AI-driven profiling, user digital awareness, GDPR, anonymization, dark patterns

Absztrakt

A tanulmány áttekinti a mesterséges intelligencia szerepét a felhasználói profilalkotásban, a kapcsolódó jelentősebb eseményeket és az európai szabályozási környezetet, különös tekintettel a jogalkotói szürke zónákra, valamint a felhasználók tudatosságára és a technológiában rejlő célzott manipulációs lehetőségekre. Rávilágít, hogy a felhasználói profilalkotás során gyűjtött adatok elemzése által nyert adatok a kiberbiztonsági, vagy marketingcélú felhasználás mellett akár támadások optimalizálására, célzott véleménybefolyásolásra is. Felhívja a figyelmet továbbá a viselkedés alapú biometrikus adatok kezelésének felhasználói profilalkotásban betöltött szerepére és a felhasználók digitális lábnyomának összetételére, valamint a felhasználók tájékoztatásában alkalmazott hiányosságokra, sötét mintázatokra.

Kulcsszavak

felhasználói profilalkotás, véleménybefolyásolás, MI rendelet, MI vezérelt profilalkotás, felhasználók digitális tudatossága, GDPR, anonimizálás, sötét mintázatok

[1] bokrosdora@gmail.com | ORCID: 0009-0001-8436-5626 | Had-és biztonságtechnikai mérnök, Okleveles biztonságtechnikai mérnök | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely | Military and Security Engineer, Certified Security Engineer | Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Artificial Intelligence Workshop

A FELHASZNÁLÓI PROFILOK ADATÖSSZETÉTELE

A felhasználói profilalkotás gazdasági és politikai jelentősége

A felhasználói profil a felhasználók, vagy felhasználói csoportok eszköz, demográfiai és viselkedési adatainak, preferenciáinak gyűjteménye és az azokból feldolgozás során nyert következtetések, melyek nagy pontossággal leírják a felhasználók interakcióit a vizsgált alannyal kapcsolatban. A profilalkotás magában foglalja a felhasználók egy adott szoftver, szolgáltatás, platform vagy egyéb termékkel kapcsolatos interakcióhoz kötődő adatainak gyűjtését, elemzését és egyéb adataihoz való társítását, melyet különböző ágazatok használnak fel, első sorban személyre szabott felhasználói élmény tervezésére, termékfejlesztésre, valamint hatékony marketingstratégiák kialakítására. A felhasználói viselkedés monitorozásának piacát nem könnyű egységes piacként definiálni, mivel egymást átfedő analitikai rétegek ökoszisztémája, ugyanakkor globális értékét 2025-ben hozzávetőleg 3.1 milliárd USD-re becsülték, mely 2026 első felére 3,61 milliárdra növekedett, emellett egyes előrejelzések alapján 2031-re 7,65 milliárdra, [1] mások szerint 2030-ra 13,6 milliárd USD-re fog nőni. [2] Több ezer szolgáltató kínál jelenleg marketing célú felhasználói profilalkotásra szolgáló termékeket az egyszerű adatelemző eszközöktől a komplex valós időben frissülő platformokig, azonban bizonyos felmérések szerint a piac hozzávetőleg 44%-át 8-10 vállalat teszi ki – mint például a Google, IBM, Oracle vagy SAS. [3] A növekedés többek között annak az igénynek köszönhető, hogy a szervezetek a statikus adatokon túlmutatóan a kontextust is számításba kívánják venni, melyhez a hiányzó láncszem a felhasználói viselkedés. Az az iparág bővülésében kulcsfontosságú tényező az ügyfelek vásárlási szokásainak és viselkedésének megértésének egyre növekvő szükségessége, valamint az olyan fejlett technológiák megjelenése, mint a mesterséges intelligencia (MI), a gépi tanulás (ML) és az üzleti folyamatok automatizálása. [4]

Az MI fejlődése és elterjedése mellett 2020-as évek másik meghatározó eseménye, hogy a COVID-19 járvány következtében az emberek élettere jelentős mértékben a digitális platformok és online ökoszisztémák irányába tolódott el. Ez felgyorsította a digitalizáció elterjedését az élet szinte minden területén, jelentős hatás gyakorolva a munkaszervezésre, oktatásra, vásárlási szokásokra, kapcsolattartásra, miközben előre látható és előre nem látható lehetőségek, kihívások is megjelentek. [5]

A fejlődés másik fő ösztönzőereje a világban jelenleg zajló fegyveres konfliktusok hatására kibontakozó fejlesztési verseny. A mesterséges intelligencia kettős felhasználású technológia. Alkalmazása mindent felgyorsít – a döntéshozatalt, az eszkalációs ciklusokat, a detektálást és a támadásokat is. A célpontokról gyűjtött és következtetett információk minőségének javulása hatására a felderítéstől a megsemmisítésig tartó folyamat jelentősen lecsökkenthető. A felhasználók profilozása során felhalmozott és elemzett adatok nem csupán a marketingszakemberek számára képviselnek hatalmas értéket, hanem kibervédelmi, bűnüldözési, politikai stratégiai jelentőséggel is bírnak. Olyan eszközök, amelyek korábban csak a kormányokra vagy világvezető vállalatokra korlátozódtak, kisebb csoportok vagy egyének számára is elérhetővé válnak. Ugyanakkor szükséges kiemelni, hogy ettől nem lesz automatikusan előnyös vagy veszélyes a technológia. Ugyanakkor – mint minden úttörő technológia esetén – jelenleg számos technikai, jogi, etikai, edukációs szürke zóna alakult ki, melyeknek lehetnek jelentős negatív hatásai ártó szándékú felhasználás, visszaélés esetén, és mely lehetőségekre szükséges kiemelt figyelmet fordítani.

A felhasználói profilalkotás mai formájához vezető út

A profilalkotás évszázados múltra visszatekintő interdiszciplináris terület. Jóval az iparosodás előtti időkre visszanyúló első formájának tekinthető a kereskedők közvetlen kapcsolata vásárlóikkal, akiknek ismerték preferenciáit, fizetési megbízhatóságát, családi hátterét. A XIX. század végén a postai rendelésre és katalógusértékesítésre épülő vállalkozások gyűjtötték az ügyfelek rendelések során megadott adatait, melyekhez demográfiai adatokat kezdtek társítani, hogy szegmentált ügyfélcsoportokat hozhassanak létre. A feldolgozás papír alapon történt matematikai módszerekkel.

A XX. század elején jelentős előrelépés jelentett a számítási kapacitás növekedésében a Herman Hollerith által kifejlesztett lyukkártya-rendszer. Az 1950-es évektől a pszichológia nagyobb szerepet kapott az ügyfélprofilozásban, melynek úttörője, Ernest Dichter pszichológus és marketingkutató interjúk, projektív tesztek és csoportbeszélgetések révén próbálta feltárni a vásárlók tudattalan indítékait. Számításba vett olyan személyiség és viselkedésbeli tényezőket mint a vágyak, félelmek, identitás, társadalmi státusz kifejezése. [6] Az 1960-as évektől megjelentek a központosított nyilvántartások, melyek a különböző szervezetek ügyfeleik hitelképességére, vásárlási szokásaira, előfizetéseire, tulajdonukban álló ingóságaikra, becsült háztartási jövedelmükre vonatkozó adatokat is társítottak az eddigiekhez.

A személyi számítógépek kora magával hozta a széleskörű felhasználói adatok decentralizált gyűjtésének és feldolgozásának új eszközeit. Az 1980–1990-es években a relációs adatbázisok megjelenésével a vállalatok elkezdték rendszerezni és tárolni az ügyféladatokat. Ekkor vált lehetővé a vásárlási előzmények és tranzakciók követése, ami jelentős előrelépést hozott a profilozásban. A személyi számítógépek elterjedésével nagyobb teret nyert a közvetlenül a felhasználók által önkéntes, explicit hozzájárulás révén megadott adatok kezelése, amelyek tipikusan regisztrációs folyamatok, kérdőívek, vagy ügyfélszolgálati interakciók során keletkeznek. Megjelentek továbbá az ügyfélkapcsolat-kezelő rendszerek, például az Oracle Siebel CRM, amelyek segítségével a vállalatok célzottabb marketingtevékenységet tudtak folytatni. A hangsúly a demográfiai adatok helyett egyre inkább a viselkedési adatokra helyeződött át.

A 1990-es évek közepétől az internet elterjedésével megjelentek a HTTP sütik, amelyek lehetővé tették a felhasználók online tevékenységének dinamikusabb követését. A különböző digitális termékek, szolgáltatások, felületek használata során automatikusan generálódó eszköz- és technikai adatok, mellett a weboldalak rögzíteni kezdték a felhasználók oldalmegtekintéseit, kattintási útvonalait és munkamenetbeli viselkedését, ami megalapozta az online viselkedésen alapuló profilozást. Az olyan cégek, mint a DoubleClick, úttörő szerepet játszottak a hirdetési célú adatgyűjtésben.

A 2000-es évek végére a vezető technológiai platformok, mint a Google és a Facebook (2021 óta Meta), hatalmas mennyiségű, több munkameneten és eszközön átívelő adatot kezdtek felhalmozni a felhasználóikról. Egyre nagyobb szerepet kaptak az érdeklődési körökre épülő célzott hirdetések. A 2010-es években az okostelefonok és a mobilapplikációk, főként közösségi média felületek elterjedése még tovább bővítette az adatgyűjtés lehetőségeit, így a profilozás egyre nagyobb mértékben támaszkodott a felhasználók kapcsolati hálózatára, online viselkedésre, alkalmazáshasználatra, közzétett tartalmakra, vélemények és reakciók valós idejű elemzésére.

A 2010-es évek végétől a 2020-as évek elejéig a Big Data és a gépi tanulás vált meghatározóvá. A profilok ekkor már folyamatosan frissülő, valószínűségi alapú rendszerekké váltak, amelyeket előrejelzések készítésére használtak.

Az MI eszközök segítségével lehetővé vált a nagy mennyiségű gyűjtött adat dinamikus, akár valós idejű elemzése és a profilok felhasználó specifikus hiper-perszonalizációja a korábban jellemző statikus demográfiai adatok elemzésén túllépve. Ezek alapján dinamikus következtetéseket lehet levonni a felhasználók hangulatára, véleményére, személyiségjegyeire, jövőbeli vásárlási hajlandóságára, egyéb döntéseire vonatkozóan is. A prediktív analízis többek között olyan módszereket használ, mint a viselkedési adat klaszterezés, trendelemzés, adaptív tanulási algoritmusok, érzelmi bevonódás mértékének mérése nyelv-feldolgozás (NLP) segítségével, vagy szolgáltatáselhagyási szándék észlelése. Az így nyert inferált adatok egyaránt felhasználhatók az online tér biztonságosabbá tételére például csalásmegelőzés céljából, szélsőséges csoportok formálódásának és aktivitásának felismerésére, ugyanakkor politikai kampánytevékenységre, hamis vagy torzított információ célzott, csoport- vagy egyénspecifikus terjesztésére is. [7] Ezt jól szemlélteti a 2018-as Facebook–Cambridge Analytica botrány, mely során a brit politikai elemző vállalat egy ártatlannak tűnő alkalmazáson keresztül hozzávetőleg 87 millió Facebook felhasználó adatait gyűjtötte össze tudomásuk és hozzájárulásuk nélkül, majd ezeket pszichográfiai profilalkotásra és célzott politikai befolyásolásra használták, többek között a 2016-os amerikai elnökválasztási kampány során. [8] Az olyan eszközök fejlődésén túlmenően, mint a webes adatkinyerés (web scraping), adatösszekapcsolás (data linking), vagy a nyelvi tanulási modellek által elemzett felhasználói tartalmak mellett az MI alapú chat applikációk további adatgyűjtési lehetőségeket és adatvédelmi kihívásokat hoztak magukkal.

Az MI fejlődése magával hozta a felhasználók élete több aspektusának gyökeres változását, valamint edukációs hiányosságokat is. Így az MI chatbot felhasználók jelentős része amellett, hogy a munkahelyi korlátozások ellenére napi feladatai egy részét végeztetik el a chatbotokkal, gyakran adnak meg személyes adatot, vagy rájuk utaló információt, illetve egészségügyi állapotukra vonatkozó tanácsot, diagnózist kérő lekérdezéseket visznek be, emellett egyre nő azok száma, akik pszichológiai segítséget kérnek a chatbotoktól, vagy a társas kapcsolataikat helyettesítik mesterséges intelligenciával, jelentős adatvédelmi kockázatnak téve ki magukat. Csak az elmúlt évben több MI chat prompt szivárgással kapcsolatos eset kapott nyilvánosságot. 2025 augusztusában a Google több ezer megosztott ChatGPT beszélgetést indexelt, így azok kereshetővé és nyilvánosan hozzáférhetővé váltak. Az indexelt oldalak teljes csevegési előzményeket tartalmaztak – beleértve az érzékeny, privát és korlátozott terjesztésre szánt adatokat is. [9] Egy másik esetben 2025 szeptemberében a Google Search Console lekérdezései között esetenként 300 karakternél hosszabb ChatGPT felhasználói lekérdezések is megjelentek, melyeknél több esetben a felhasználók magánéleti helyzetüket fejtették ki az applikációnak. [10] Az rendszerek, mint a ChatGPT, képesek felhasználói adatok kinyerésére és osztályozására az interakcióik alapján. Az OpenAI szerint a felhasználóknak továbbra is joguk van elutasítani az adataik felhasználását a modell fejlesztéséhez, viszont rendszeresen kritika éri a szervezetet a nem kellőképpen transzparens adatkezelési gyakorlatok miatt. [11] [12]

A viselkedésalapú adatok egy speciális kategóriáját képzik az olyan biometrikus adatok, mint a kattintások, érintések, görgetések, billentyűleütések ritmusa, képernyő mé-

reteihez viszonyított helyzete, nyomáserőssége, lenyomás ideje, bizonyos esetekben beszédhang elemzése, illetve egyéb viselhető okoseszközök által gyűjtött egészségügyi adatok, mint például a szívverés vagy járásdinamika. Mivel a viselkedésalapú biometrikus adatok feldolgozása a folyamatosan zajlik a háttérben és nem igényli a felhasználó aktív közreműködését, valamint nem az emberi test időben állandó fizikai attribútumainak rögzítésén alapul, elfogadottsága magasabb a felhasználók körében. [13] A felhasználói profilalkotás során gyűjtött adattípusok csoportosítását az 1. táblázat részletezi.

Fő kategória	Alkategória	Adattípus	Példák
Elsődleges adatokp	Felhasználó által megadott (aktív)	Regisztrációs és személyes adatok	név, e-mail, telefonszám, lakcím, életkor
			regisztráció, vásárlás, ügyfélszolgálati kommunikáció
		Közzétett tartalom	hozzászólás, üzenet, blogbejegyzés, kép-, video-, hangfelvétel, chatbot prompt
	Automatikusan gyűjtött (passzív)	Aktivitással kapcsolatos adatok	böngészési előzmények, keresések, vásárlási, applikációhasználati mintázatok, interakciók
		Technikai és eszközadatok	IP-cím, böngésző, operációs rendszer, eszközazonosítók, nyelvi beállítások, képernyőméret
		Szenzor- és biometrikus adatok	billentyűleütés, kurzormozgás, érintés, járásdinamika
		Helyadatok	GPS, földrajzi hely, mozgásadatok, helyalapú aktivitás
		Külső forrásból származó adatok	nyilvántartások, harmadik felektől vásárolt adatok,
Másodlagos adatok	Következtetett	Pszichológiai jellemzők	személyiségjegyek, hangulat
		Egészségügyi állapot	fizikai vagy mentális állapotra utaló következtetések
		Gazdasági helyzet	jövedelem, hitelképesség
		Demográfiai és társadalmi jellemzők	vallás, ideológia, politikai nézetek
		Preferenciák és érdeklődés	termékpreferenciák, érdeklődési kör
		Viselkedési mintázatok	szokások, rutinok
		Prediktív adatok	döntések, jövőbeli viselkedés előrejelzése

1. táblázat: A felhasználói profilok adatösszetétele, saját szerkesztés

A felhasználói profilalkotás társadalmi kockázatai

Az MI eszközök legújabb változatait övező jelentősebb biztonsági kihívások közé tartozik a félrevezető információk széleskörű vagy célzott terjesztése, a személyes adatok védelmének nehezebbé válása és a tömeges megfigyelés lehetősége. Mindezek a felhaszná-

lói adatok elemzésével nyert átfogó kép segítségével még célzottabbá, pontosabbá, személyre szabottabbá tehetők. Az Anthropic AI fejlesztő vállalat és a Pentagon közt kibontakozó helyzet kapcsán egy 2026.03.06-án közölt videointerjúban [14] Dean Ball a Trump adminisztráció korábbi vezető MI szakpolitikai tanácsadója kifejtette, hogy jogi szempontból a felhasználók eszközeinek kormányzati szervek által történő közvetlen megfigyelése jogellenes cselekedet, ugyanakkor a harmadik felektől vásárolt adatkészletek elemzése nem feltétlenül számít megfigyelési tevékenységnek a jelenlegi USA-beli jogszabályi környezetben.

A technológia emellett megkönnyíti a deepfake tartalmak gyorsabb és meggyőzőbb előállítását, valamint az MI generált tartalmakhoz szükséges bemeneti információk könnyen szennyezhetők (data poisoning), így az MI eszközök, kiemelten a chatbotok a különböző promptokra torzított információt generálhatnak, amely befolyásolhat akár választásokat, vagy aláásható az emberek azon képességét, hogy megbízzanak bármilyen információban, potenciálisan destabilizálva a társadalmakat. [15] Több kutatás született az AI eszközök, chatbotok téves információterjesztéséről, melyet jól szemléltet a Nature 2026. április 07-i cikkében közölt 2024-es kutatás, mely során a Göteborgi egyetem kutatói megalkottak egy fiktív betegséget, hogy teszteljék az MI chatbotokat. A fiktív kórképet leíró információkat első körben egy blogbejegyzésben, majd 2 tudományos publikációban tették közzé. A „csapda cikkek" számos árulkodó jelet tartalmaztak, emellett konkrétan közölték is, hogy „ez az egész tanulmány kitalált". Ennek ellenére a cikkek közlése után, az információ elkezdett megjelenni a leggyakrabban használt LLM chatbotok kimenetében. 2024. április 13-án a Microsoft Bing Copilotja, valamint a Google Geminije, majd 2024. április 27-én a Perplexity AI, majd később a hónap folyamán az OpenAI ChatGPT-je valódinak jelezte a kitalált kórképet a felhasználók felé és tanácsolta nekik, hogy forduljanak orvoshoz. Ezen az ártatlannak tűnő figyelemfelhívó kísérleten túlmutatva az utóbbi években számtalan cikk és kutatás született arról, hogy az MI chat applikációk képesek befolyásolni a felhasználóik politikai nézeteit, valamint hogy mely politikai jelöltekre szavazzanak. Egy a Nature-ben 2025. december 04-én publikált kutatás résztvevőit arra kérték, hogy beszélgessenek olyan nyelvi modellel melyet a kutatók a 2024-es amerikai, a 2025-ös kanadai és a 2025-ös lengyel választások kontextusában különböző jelöltjeinek támogatására tanítottak be. A beszélgetés közvetlen eredményeként 1,52 és 10% közötti volt a választók véleményének változása. [16] Egy másik, a Science folyóiratban publikált kutatás 77 000 brit résztvevő véleményváltozásait vizsgálta, akik 700 különböző politikai vonatkozású kérdésben léptek interakcióba az MI chatbotokkal. A legoptimálisabb modell a résztvevők hozzávetőleg 25%-ának véleményét képes volt megváltoztatni a vizsgált politikai kérdésekben. [17] Ezek a véleménybefolyásolásra irányuló törekvések a dinamikusan változó felhasználói profilok következtetett adataival kombinálva magukban hordozzák a felhasználóra szabott véleménybuborékok és célzott manipuláció vagy mentális állapot befolyásolásának kockázatát.

ADATVÉDELMI KIHÍVÁSOK

A felhasználói profilokra vonatkozó főbb szabályzási kísérletek

A különböző országok különböző megközelítést alkalmaznak a személyes adatok védelmére és a mesterséges intelligencia alkalmazására vonatkozóan. Az Egyesült Álla-

mok, mint az egyik „MI nagyhatalom” a technológia szabályozása tekintetében decentralizált, iparág ösztönző megközelítést részesít előnyben, amely a fejlesztés ösztönzésére összpontosít az átfogó szövetségi korlátozások helyett. [18] Kína hasonlóan ösztönzi a fejlődést, viszont konkrét tiltásokat és irányelveket fogalmaz meg például az MI generált tartalmak jelölésére, vagy az MI modellek tanításához használt bemeneti adatoknál alkalmazandó elővigyázatosságra vonatkozóan. [19] Az Európai Unió ezzel szemben nagyobb hangsúlyt fektet a személyiségi jogi, etikai, versenyegyenlőséget támogató mesterséges intelligencia szabályozásra, valamint konkrét tiltásokat fogalmaz meg.

Az Európai Unió területén belül a legmeghatározóbb adatvédelmi és MI vonatkozású rendelkezések az EU 2016/679 rendelete (továbbiakban GDPR) [20] és az EU 2024/1689 rendelete (továbbiakban MI rendelet) [21]. A felhasználó profil, mint fogalom megjelenik továbbá az EU 2022/2065 rendeletben (továbbiakban: Digitális szolgáltatásokról szóló rendelet) [22], valamint az EU 2023/2854 rendeletében (továbbiakban: Adatrendelet) [23]. Azonban az MI rendelet, az Adatrendelet és a Digitális szolgáltatásokról szóló rendelet is a GDPR 4. cikk 4. pont szerinti definícióra hivatkozik, mely szerint a profilalkotás a „*személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják*”. Ebben az értelmezésben a profilalkotás fogalmába a gyűjtött adatok személyazonossággal való egyértelmű összekapcsolása tartozik, különös tekintettel, ha az így gyűjtött adott személyhez köthető adatok, vagy az azokból levonható következtetések adott személy megítélésére hatással lehetnek, ezek miatt negatív diszkrimináció, faji, világnézeti, egyéb orientációra vonatkozó hátrányos megkülönböztetés érheti. A GDPR 22. cikke szabályozza a személyazonosságához köthető profilalkotáson alapuló automatizált döntéshozatalt is (például hitelkérelem elutasítása, dinamikus árképzés, automatikus HR szűrés vagy ügyfélkizárás). Emellett fontosabb profilalkotásra vonatkozó elemei a 13–14. cikkben definiált tájékoztatási kötelezettség, a 21. cikkben kifejtett 4. cikk értelmezése szerinti profilalkotás elleni tiltakozási jog, és a 35. cikk által megfogalmazott adatvédelmi hatásvizsgálat alkalmazása.

Magyar jogszabályi környezetben a 2011. évi CXII. törvényben jelenik meg a profilalkotás definíciója, szintén a GDPR-beli megfogalmazást alkalmazva. Szintén kitér az adatkezelés alanyával szembeni tájékoztatási kötelezettségre (17§ (2)) akkor is, ha az adatkezelő harmadik országbeli (25/E.§). [24] A 17/HU WP251rev.01 NAIH iránymutatása közérthetően összefoglalja a profilalkotás három elemét: „*valamilyen formájú automatizált kezelésnek kell lennie; személyes adatok tekintetében kell végezni; és a profilalkotás célja egy természetes személy személyes jellemzőinek értékelése*.” [25]

Az MI rendeletben megjelenik a biometrikus és viselkedési adatok kezelése, az érzelemfelismerés, valamint ezek és egyéb természetes személyekkel összefüggésbe hozható inputok alapján következtetések levonása is. A rendelet ezeket is első sorban személyiségi jogi szempontból vizsgálja, kiemelten azokra a felhasználási területekre, ahol kiegyenlítetlen hatalmi viszonyok állhatnak fenn és az adatkezelés alanyára az MI rendszer által levont következtetések negatív következménnyel járhatnak (például munkahely, oktatási, egészségügyi intézmények, igazságszolgáltatás bizonyos aspektusai).

Marketingcélú profilalkotás esetén a korlátozások nem egyértelműek

A marketingcélú profilalkotás jelenleg nem rendelkezik egységes, általánosan elfogadott definícióval. Ez a fajta profilalkotás általában nem természetes személyként vizsgálja a felhasználókat, személyazonosságuk nem kerül explicit módon azonosításra. Ennek ellenére a teljes anonimizálás meglehetősen ritka a gyakorlatban, emellett anyagi érdek fűződik a fogyasztói preferenciák lehető legpontosabb feltérképezéséhez. A vállalatok adatkezelés során többnyire egyedi azonosítót (például sütiazonosító vagy eszközazonosító) alkalmaznak. Így a felhasználói paraméterek és interakció továbbra is nyomon követhető tényleges személyazonosítás nélkül. Ugyanakkor az alkalmazáshasználati adatkészletek kinyerése, vagy megosztása továbbra is jelentős adatvédelmi kockázatot jelent. Egy a Helsinki egyetem kutatói által 2022-ben végzett kutatás szerint számos tanulmány kimutatta, hogy a felhasználók azonosíthatók vagy újraazonosíthatók az anonimizált adatkészletekből az alkalmazáshasználati szokásaik alapján. Az elemzett kutatások alapján egy 46 726 résztvevőt magába foglaló vizsgálat során az akkori 500 legnépszerűbb alkalmazás használata által a felhasználók 99,67%-ánál egyedi alkalmazás-aláírást lehetett létrehozni. Egy nagyobb, 1,37 millió kínai felhasználóból álló adatkészletet elemzése alapján mindössze 4 alkalmazás használata által a felhasználók 88%-át lehetséges egyedileg azonosítani. [26]

Sötét mintázatok alkalmazása a felhasználók tájékoztatásában

A sütik elfogadására vonatkozó bannerek és az adatvédelmi irányelvek kontextusában a sötét mintázatok olyan felhasználói felület-kialakítások vagy kommunikációs gyakorlatok, amelyeket szándékosan úgy alakítottak ki, hogy befolyásolják, nyomást gyakoroljanak, összezavarják vagy manipulálják a felhasználókat, hogy hozzájáruljanak az olyan adatgyűjtési, -követési vagy -megosztási gyakorlatokhoz, amelyeket megfelelő tájékoztatás és egyértelmű választási lehetőségek esetén elutasítanának. Ha feltételezzük, hogy a felhasználói adatok többségének kezelése explicit, önkéntes hozzájárulásuk alapján történik, akkor is figyelembe kell venni az alábbi döntéseiket befolyásoló tényezőket.

Az EU jogszabályi környezete egyértelműen definiálja a felhasználók tájékoztatására vonatkozó paramétereket, a nem megfelelő tájékoztatást komoly bírságokkal szankcionálja. Azonban a gyakorlatban a tájékoztatás minősége és az adatkezelés jogszerűsége gyakran elmarad az elvárásoktól. Egy 2012-es felmérés szerint egy felhasználónak körülbelül 76 napba telne elolvasni azon adatkezelési tájékoztatókat, melyekkel egy év alatt találkozik. [27] Egy 50000 adatkezelési tájékoztatót vizsgáló 2021-es elemzés szerint egy adatkezelési tájékoztató hossza 4000 szó terjedelmű, emellett az átlagos felhasználók számára gyakran nehezen értelmezhető jogi nyelvezettel íródnak. [28] Egy 2024-es felmérés szerint a vizsgált felhasználók körülbelül 0,5%-a nyitotta meg az adatkezelési tájékoztatókat. A tanulmányban vizsgált dokumentumok már átlagosan 7400 szó hosszúságúak voltak. [29]

A GDPR rendelkezése szerint hozzájárulásnak tájékoztatáson alapulónak, konkrétnak és önkéntesnek kell lennie. Ezzel szemben számos weboldal nem ad választási lehetőséget sem, kizárólag egy felugró ablakban tájékoztat, hogy az adott oldal sütiket használ, kezeli a felhasználó adatait. A sütik elfogadására vonatkozó bannerek gyakran alkalmaznak GDPR rendelkezéseket sértő módszereket a grafikus kialakítás, szövegezés, vagy választási lehetőségek láthatósága terén. A felhasználó kognitív kifáradására, érzéketlenedésére alapozva túlterhelő mennyiségű egyesével kiválasztandó kategóriára bontják a hozzájárulást,

elrejtik a visszautasítás opciót, kiemelik a minden süti elfogadására irányuló lehetőséget, előre bejelölik az összes kezelni kívánt sütikategóriát, vagy félreértelmezhető, esetleg megtévesztő módon ábrázolják az elfogadást és elutasítást jelző gombokat. A sütik elutasítását indokolatlanul hosszú, következetlen vagy nehezen átlátható folyamatok nehezítik, miközben az adatkezelés elfogadása egyszerű és gyors marad. Ezzel párhuzamosan a rendszerek gyakran alkalmaznak túlzott egyszerűsítést, személyre szabást és célzott javaslatokat, amelyek a kívánt döntési útvonalat intuitívabbnak és relevánsabbnak tüntetik fel. Ezek mellett a felhasználói profilalkotás segítségével felületek folyamatosan adaptálódnak a változó felhasználói szokásokhoz a kívánt adatkezelési eredmények elérése érdekében. [30] Egyre gyakrabban megjelenik a sütik elutasítási lehetőségének fizetési fal mögé helyezése is, ahol a felhasználó választhat, hogy előfizet, vagy beleegyezik az adatkezelésbe a „jobb felhasználói élmény" érdekében.

A szabályozás gyakorlati korlátai

Olyan non-profit szervezetek, mint a NYOB a sötét mintázatok alkalmazása kapcsán közel 10000 európai weboldalt vizsgált felül nem megfelelő gyakorlataik kapcsán, mely eredményeként több mint 500 vállalat kapott írásbeli figyelmeztetést 2021 tavaszáig. A jogsértések 42%-át 30 napon belül remediálták, viszont a vizsgált vállalatok 82%-ánál alkalmazott gyakorlatok továbbra is sértik a GDPR-t. Ennek megfelelően további 422 panasz került benyújtásra 10 adatvédelmi hatósághoz. [31] A Meta részére az utóbbi években több jelentős adatvédelmi vonatkozású bírság került kiszabásra, melyek közül a legismertebb a 2023 májusi 1,2 milliárd euró összegű bírságot eredményező adatátviteli szabálysértés, melyet a felhasználói adatok az Európia Unióból az USA-ba továbbítása eredményezett. [32] Majd további nagy nyilvánossággal járó bírságokat kaptak felhasználókat célzó webes adatkinyerés miatt 2022-ben, a felhasználói jelszavak egyszerű szöveg alapú tárolásáért 2024 szeptemberében, valamint egyéb nem megfelelő jelszókezelési gyakorlatok miatt 2024 decemberében. Ugyan a 2023-as eset korábban példátlan mértékű bírságot eredményezett, számításba kell venni, hogy a vállalat teljes piaci értékét a 2023 májusában több mint 520 milliárd, jelenleg 2026 májusában pedig 1,5-1,6 trillió dollárra becsülik. [33] A megfelelő jogi és technológiai kontrollok implementálásának és betartatásának legjelentősebb akadályai a fejlődés rendkívül gyors üteme, valamint az egyre nagyobb számú digitális szolgáltató egyidejű jelenléte és az adatvédelmi incidensek kivizsgálási ideje, valamint a bírság és remediálás megállapításához vezető idő hossza. Emellett a kontrollok érvényesítése gyakran gazdasági vagy politikai érdekbe ütközik. Jól szemlélteti ezen kezdeményezések akadályait az MI technológiákról szóló kommunikáció ellentmondásos hatása is. Hetente jelennek meg különböző médiumokban a keresőoptimalizált, hangzatos főcímek az emberiséget elpusztító mesterséges intelligenciáról szóló elméletekről és találgatásokról. Az ilyen típusú kommunikáció viszont paradox módon erősíti a technológiai óriásvállalatok pozícióját, és akadályozza a mesterséges intelligencia által jelenleg okozott negatív társadalmi hatások hatékony szabályozását, ahogy a *Nature* 2023 júniusában megjelent cikkében összegzett szakértői vélemények is alátámasztják [34]. Ezen értelmezés szerint a mesterséges intelligencia, „tökéletes fegyverként" való ábrázolása táplálja a nemzetek közötti fejlesztési versenyt az előnyszerzés és a lehető leghatékonyabb MI eszközök saját irányításuk

alá vonása érdekében. Ezáltal ösztönzi a beruházásokat és akadályozza az iparág szabályozását célzó kezdeményezéseket, valamint lehetővé teszi, hogy nagyvállalati vezetők szűk csoportjai befolyásolják azokat.

ÖSSZEFOGLALÁS

A profilalkotásnak különböző definíciói léteznek ágazattól, felhasználási módtól függően. A felhasználókról gyűjtött adatok elemzésével létrehozott profilok használhatók többek között kibervédelmi anomáliadetektálásra, szervezeti munkafolyamat optimalizálása, vagy ügyfélinterakciók elemzésére, termékfejlesztés és üzleti stratégiai döntések elősegítése céljából. A profilalkotás során gyűjtött hatalmas mennyiségű adat önmagában is jelentős értéket képvisel mind gazdasági, mind biztonsági szempontból. Ezen felül az utóbbi években a digitalizáció terjedése, és a mesterséges intelligencia forradalma új dimenziót nyitott a felhasználói adatok feldolgozásában, mely hatására az eddig emberi léptékkel belátható időn belül feldolgozhatatlan mennyiségű adatból struktúrált, akár valós időben változó, nagy pontosságú kép alakítható ki a vizsgált felhasználókról, így akár jövőbeli döntéseik is előrejelezhetővé válhatnak. A felhasználói profilalkotás fejlődése nyilvánvaló előnyei mellett számos új biztonsági kihívást magával hozott, mivel a marketingcélú felhasználás mellett akár kifinomult kibertámadásokhoz, vagy politikai véleménybefolyásoláshoz is felhasználható. A kockázatok mitigálása érdekében a különböző országok jogalkotói megkísérelték szabályozni a felhasználókról gyűjthető adatok felhasználási és kezelési módjait, igyekezve lépést tartani a fejlődéssel. A szabályozói kontrollkörnyezet kialakításában azonban jelentős kihívást okoz a gazdasági érdekek és a felhasználók jogainak érvényesítése közötti érdekellentét. Ennek eredményeként számos szabályozói szürke zóna alakult ki a felhasználói profilalkotás szabályozása terén, továbbá a gyors ütemű technológiai fejlődés gyakran meghaladja a jogalkotók alkalmazkodásának ütemét. A Európai Unió mesterséges intelligencia alapú felhasználói profilalkotásra vonatkozó szabályozási környezete jelenleg nem rendelkeznek egyértelműen a marketikg célból létrehozott felhasználói profilok adattartalmáról és felhasználásuk korlátozásáról. A magas bírságok ellenére a felhasználói adatok kezelésére vonatkoztató tájékoztatás, adatkezelési gyakorlatok gyakran nem kellőképpen transzparensek, valamint a szabálytalan gyakorlat beazonosításától annak szankcionálásáig és részleges vagy teljes mitigálásig akár évek is eltelhetnek. Emellett a felhasználói profilkészítésben rejlő anyagi előnyök messze túlmutatnak a büntetések mértékén. Ezért szükséges a felhasználók megfelelő edukációja online aktivitásuk lehetséges következményeit, digitális lábnyomuk összetételét, adatvédelmi jogaik érvényesítési lehetőségeit illetően, és a manipulációs technikák felismerése terén. Valamint a vállalatok és nemzetek vezetőinek nagyobb hangsúlyt kell helyezniük az állampolgárok digitális biztonságtudatossági oktatására, a digitális lábnyom adatösszetételére és a kockázatarányos felkészülés érdekében számításba kell venniük azokat a szcenáriókat, amikor ezen adatok felhasználása ellenséges vagy manipulatív szándékkal történik.

FELHASZNÁLT IRODALOM

[1] Mordor Intelligence, “User Activity Monitoring Market - Growth, Trends, COVID-19 Impact, and Forecasts,” Mordor Intelligence, Elérés: https://www.mordorintelligence.com/industry-reports/user-activity-monitoring-market

[2] Strategic Market Research, "Behavior Analytics Market," Strategic Market Research, 2025. Okt. Elérés: https://www.strategicmarketresearch.com/market-report/behavior-analytics-market
[3] Market Growth Reports, "Customer Analytics Market Report," Market Growth Reports, 2026. Jan. Elérés: https://www.marketgrowthreports.com/market-reports/customer-analytics-market-114920
[4] Intellect Markets, "Customer Behavior Analytics Market," Intellect Markets, Elérés: https://intellectmarkets.com/report/customer-behavior-analytics-market
[5] J. Amankwah-Amoah, Z. Khan, G. Wood, and G. Knight, "COVID-19 and Digitalization: The Great Acceleration," Journal of Business Research, 2021. Nov. Elérés: https://www.sciencedirect.com/science/article/pii/S0148296321005725?via%3Dihub
[6] "How Ernest Dichter Brought Psychology to Business," *Psychology Today*, 2022. Ápr. Elérés: https://www.psychologytoday.com/us/blog/psychology-yesterday/202204/how-ernest-dichter-brought-psychology-business
[7] S. C. Matz, M. Kosinski, G. Nave, and D. J. Stillwell, "Psychological targeting as an effective approach to digital mass persuasion," *Proceedings of the National Academy of Sciences*, 2017. Nov. https://www.pnas.org/doi/10.1073/pnas.1710966114
[8] "The Cambridge Analytica scandal and what it teaches us," *University of Greater Manchester Blog*. 2021. Ápr. 19, Elérés: https://greatermanchester.ac.uk/blogs/the-cambridge-analytica-scandal-and-what-it-teaches-us
[9] A. Alifar, "Exposed: Google is indexing private AI conversations — here's what you should know," *DEV Community*, 2025. Júl. Elérés: https://dev.to/alifar/exposed-google-is-indexing-private-ai-conversations-heres-what-you-should-know-37m5
[10] "The Old Rules Are Dead," *Quantable*. Elérés: https://www.quantable.com/ai/the-old-rules-are-dead/
[11] V. Kumar and M. Lata, "AI chatbots: security and privacy challenges," *International Journal of Electronic Security and Digital Forensics*, vol. 17, pp. 776–797, 2025. Jan, Elérés: https://www.researchgate.net/publication/387605688_ai_chatbots_security_and_privacy_challenges
[12] F. Bulut Kartal and E. Yildirim, "AI profiling poses growing threat to privacy and national security," *Anadolu Agency*, 2025. Júl. 10, Elérés: https://www.aa.com.tr/en/artificial-intelligence/ai-profiling-poses-growing-threat-to-privacy-and-national-security/3627228
[13] C. L. Miltgen, A. Popovič, and T. Oliveira, "Determinants of end-user acceptance of biometrics: Integrating the 'Big 3' of technology acceptance with privacy context," *Decision Support Systems*, vol. 56, no. 1, pp. 103–114, 2013. Dec. Elérés: https://www.sciencedirect.com/science/article/abs/pii/S0167923613001267.
[14] Ezra Klein, Dean Ball, „*Why the Pentagon Wants to Destroy Anthropic*" 2026. Márc. 6. Elérés: https://www.youtube.com/watch?v=xc97F2CFBOY
[15] D. Matthews, "Scientists invented a fake disease. AI told people it was real," Nature, 2026. Ápr. 7, Elérés: https://www.nature.com/articles/d41586-026-01100-y
[16] H. Lin, G. Czarnek, B. Lewis, J. P. White, A. J. Berinsky, T. Costello, G. Pennycook, and D. G. Rand, "Persuading voters using human–artificial intelligence dialogues," Nature, 2025. Dec. 4, Elérés: https://www.nature.com/articles/s41586-025-09771-9

[17] M. V. Gómez, "Programs like ChatGPT can change the opinion of one in four voters," El País, 2025. Dec. 4, Elérés: https://english.elpais.com/technology/2025-12-04/programs-like-chatgpt-can-change-the-opinion-of-one-in-four-voters.html
[18] The White House, "National Policy Framework for Artificial Intelligence: Legislative Recommendations," 2026. Mar. Elérés: https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-national-policy-framework-for-artificial-intelligence-legislative-recommendations.pdf
[19] CMS Expert Guides, "AI laws and regulation in China." Elérés: https://cms.law/en/int/expert-guides/ai-regulation-scanner/china
[25] National Authority for Data Protection and Freedom of Information (NAIH), "Irány-mutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához," Elérés: https://www.naih.hu/files/wp251rev01_hu.pdf
[26] T. Li, "Smartphone App Usage Analysis: Datasets, Methods, and Applications," *IEEE*, 2022. Elérés: https://helda.helsinki.fi/server/api/core/bitstreams/54d45a59-3295-4c63-a28f-1e5ff33ec903/content
[27] A. C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," *The Atlantic*, 2012. Mar. 1, Elérés: https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/
[28] De Montfort University Leicester, "Study shows privacy policies are longer and harder to understand in 2021," 2022. Febr. Elérés: https://www.dmu.ac.uk/about-dmu/news/2022/february/study-shows-privacy-policies-are-longer-and-harder-to-understand-in-2021.aspx
[29] Linklaters, "Who reads privacy notices? And why do we have them?" *Digilinks Blog*, 2024. Szept. 26, Elérés: https://www.linklaters.com/insights/blogs/digilinks/2024/september/uk---who-reads-privacy-notices-and-why-do-we-have-them
[30] A. Mathur, M. Kshirsagar, and J. Mayer, "Dark design patterns: An end-user perspective," *Human Technology*, vol. 16, no. 2, pp. 170–199, 2020. Aug. Elérés: https://www.researchgate.net/publication/346663816_dark_design_patterns_an_end-user_perspective
[31] noyb – European Center for Digital Rights, "noyb files 422 formal GDPR complaints on nerve-wrecking 'Cookie Banners'," 2021. Aug. 10, Elérés: https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners
[32] European Data Protection Board (EDPB), "1.2 billion euro fine for Facebook as a result of EDPB binding decision," 2023. Máj. 22, Elérés: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en
[33] CompaniesMarketCap, "Market capitalization of Meta Platforms (Facebook) (META)." Elérés: https://companiesmarketcap.com/meta-platforms/marketcap/#google_vignette
[34] *Nature*, "Stop talking about tomorrow's AI doomsday when AI poses risks today," 2023. Jún. 27, Elérés: https://www.nature.com/articles/d41586-023-02094-7

JOGSZABÁLYOK

[20] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet – GDPR), *Official Journal of the European Union*, 2016. Ápr. 27, Elérés: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679

[21] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályokról (Mesterséges Intelligencia Rendelet), *Official Journal of the European Union*, 2024. Jún. 13, Elérés: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R1689

[22] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló rendelet – DSA),” *Official Journal of the European Union*, 2022. Okt. 19, Elérés: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/hun

[23] Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete az adatokhoz való méltányos hozzáférésről és felhasználásról (adatmegosztási rendelet – Data Act), *Official Journal of the European Union*, 2023. Dec. 13, Elérés: https://eur-lex.europa.eu/eli/reg/2023/2854/oj?locale=hu

[24] Magyarország Országgyűlése, 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról Elérés: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv

DOI: https://doi.org/10.12700/btsz.2026.8.2.113

THE ROLE OF THE EU AI ACT IN MITIGATING OCCUPATIONAL PSYCHOSOCIAL RISKS

AZ EU AI ACT SZEREPE A MUNKAHELYI PSZICHOSZOCIÁLIS KOCKÁZATOK MÉRSÉKLÉSÉBEN

GÁBOR Edina[1] – NÉGYESI Imre[2]

Abstract

The workplace expansion of artificial intelligence and algorithmic management, alongside efficiency enhancement, generates new and intensifying psychosocial risks, cognitive overload, isolation, information deficit, and lack of control in the digital work environment. The present study comprehensively examines how the European Union's Artificial Intelligence Act (EU AI Act) contributes to the management of these modern occupational safety challenges. Although the AI Act is primarily an internal market and product safety legislation, the research demonstrates its indirect occupational safety significance along a four-dimensional analytical model. The study reveals how the mechanisms required by the regulation, particularly the definition of prohibited AI practices, transparency requirements, the mandate for human oversight, the employee information obligation, and the right to an explanation of individual decisions, create proactive guarantees.

Keywords

artificial intelligence, occupational health and safety, psychosocial risks, EU AI Act, algorithmic management

Absztrakt

A mesterséges intelligencia és az algoritmikus menedzsment munkahelyi térnyerése a hatékonyságnövelés mellett új és erősödő pszichoszociális kockázatokat, kognitív túlterheltséget, izolációt, információs deficitet és kontrollhiányt generál a digitális munkakörnyezetben. Jelen tanulmány átfogóan vizsgálja, hogy az Európai Unió mesterséges intelligenciáról szóló rendelete (EU AI Act) miként járul hozzá ezen modern munkavédelmi kihívások kezeléséhez. Bár az AI Act elsődlegesen belső piaci és termékbiztonsági jogszabály, a kutatás egy négydimenziós elemzési modell mentén bizonyítja annak közvetett munkavédelmi jelentőségét. A tanulmány feltárja, hogy a rendelet által megkövetelt mechanizmusok, különösen a tiltott MI-gyakorlatok meghatározása, az átláthatósági követelmények, az emberi felügyelet előírása, a munkavállalói tájékoztatási kötelezettség és az egyedi döntések magyarázatához való jog hogyan teremtenek proaktív garanciákat.

Kulcsszavak

mesterséges intelligencia, munkavédelem, pszichoszociális kockázatok, EU AI Act, algoritmikus menedzsment

[1]gabor.edina@phd.uni-obuda.hu | ORCID: 0009-0009-0421-0252 | PhD student, Doctoral School on Safety and Security Sciences, Obuda University | doktorandusz hallgató, Biztonságtudományi Doktori Iskola, Óbudai Egyetem
[2]negyesi.imre@uni-nke.hu | ORCID: 0000-0003-1144-1912 | Head of department, Ludovika University of Public Service| tanszékvezető, Nemzeti Közszolgálati Egyetem

BEVEZETÉS

A negyedik ipari forradalom technológiai vívmányai, a mesterséges intelligencia, a felhőalapú szolgáltatások és az okoseszközök ma már nem csupán elszigetelt informatikai eszközökként, hanem egymással szorosan összekapcsolódó, komplex rendszerekként strukturálják át a munka világát. E technológiák integrációja új típusú szervezeti és vezetési gyakorlatokat hozott létre. Miközben a feladatkiosztás, a teljesítményértékelés és a munkafolyamatok adatvezérelt, automatizált irányítása soha nem látott hatékonyságnövelést és folyamatoptimalizálást tesz lehetővé a vállalatok számára, egyúttal alapjaiban formálja át a munkavállalói kontrollviszonyokat. E változások nyomán a munkahelyi környezetben a klasszikus fizikai és kémiai ártalmak mellett új és felerősödő pszichoszociális kockázatok jelentek meg.

A munkahelyi pszichoszociális kockázatok munkavédelmi szabályozásának fejlődéstörténetét és hazai jogi keretrendszerét egy korábbi tanulmányom már átfogóan elemezte [1]. Az említett kutatás rámutatott arra, hogy a munkahelyi mentális egészségvédelem jogi és intézményi háttere folyamatosan adaptálódik a változó munkakörnyezethez. Ezt az elméleti alapot folytatva, a digitalizáció munkaszervezésre gyakorolt hatásait vizsgálva, kutatásunk során azonosítottuk és rendszereztük a digitális munkakörnyezet specifikus pszichoszociális kockázatait. E kutatás négy fő dimenziót: a túlterheltséget, az izolációt, az információs deficitet és a kontrollhiányt tárta fel, amelyek komplex rendszerszintű kihívást jelentenek a modern munkavégzés során [2].

Tovább vizsgálva munkahelyi pszichoszociális kockázatok kezelésének lehetőségeit, jelen tanulmány fókuszában az Európai Unió mesterséges intelligenciáról szóló rendelete, az (EU) 2024/1689 rendelete áll. A kutatás azt a szabályozási metszéspontot vizsgálja, ahol a hagyományos munkavédelem, az alapjogvédelem és az új technológiaszabályozás összekapcsolódik. A tanulmány alaptézise, hogy bár az AI Act nem hagyományos értelemben vett munkavédelmi jogszabály, hanem elsődlegesen belső piaci, termékbiztonsági és alapjogvédelmi logikára épülő uniós rendelet, egyes mechanizmusai közvetett, ám fontos munkavédelmi jelentőséggel bírnak.

Jelen tanulmány jogszabályi és koncepcionális elemzésként arra vállalkozik, hogy feltárja, hogy az AI Act horizontális, kockázatalapú megközelítése miként képes kiegészíteni a klasszikus munkavédelmi szabályozást a digitális munkakörnyezetben. Célkitűzése annak bemutatása, hogy a rendelet specifikus előírásai már az MI-rendszerek tervezési, fejlesztési, forgalomba hozatali és működtetési szakaszában olyan technikai és szervezeti garanciákat követelnek meg, amelyek proaktívan támogatják a pszichoszociális kockázatok kezelését. A tanulmány a korábban lefektetett négydimenziós modell mentén részletesen elemzi, hogy az EU AI Act és specifikus részei a tiltott MI-gyakorlatok meghatározása (5. cikk), az átláthatósági követelmények (13. cikk), az emberi felügyeletre vonatkozó szabályok (14. cikk), a munkavállalói tájékoztatás (26. cikk), az alapjogvédelmi hatásvizsgálat (27. cikk), valamint az egyedi döntések magyarázatához való jog (86. cikk) hogyan járulhatnak hozzá a munkahelyi technostressz, a kognitív túlterheltség, az információs aszimmetria és a kontrollhiány célzott mérsékléséhez. [3]

A MESTERSÉGES INTELLIGENCIA MUNKAHELYI ALKALMAZÁSÁNAK ALAPJOGI KORLÁTAI

A huszonegyedik században a gépi tanulás, a mesterséges neurális hálózatok, a prediktív analitika és más adatvezérelt megoldások munkahelyi alkalmazása új típusú szervezeti és vezetési gyakorlatokat hozott létre. E folyamat egyik fontos megjelenési formája az algoritmikus menedzsment, amelynek során a feladatkiosztás, a munkaidő-beosztás, a teljesítményértékelés, a toborzás vagy akár a munkavállalói viselkedés monitorozása részben vagy egészben algoritmikus rendszerek támogatásával történik. Ez a vállalatok számára hatékonysági és döntéstámogatási előnyöket kínálhat, ugyanakkor a munkavállalók szempontjából átalakíthatja a munkahelyi elvárásokat, a kontrollviszonyokat és a pszichoszociális terhelést. [4] [5]

Az Európai Unió jogfejlődésében és szociális modelljében központi jelentőségű az a normatív alapelv, hogy a gazdasági fejlődés és a technológiai innováció nem értelmezhető az emberi méltóság, az alapvető jogok, valamint a munkavállalók egészségének és biztonságának védelmétől függetlenül. A mesterséges intelligencia munkahelyi alkalmazása ezért nem pusztán technológiai vagy gazdasági kérdés, hanem alapjogi, munkavédelmi és szervezeti felelősségi dimenzióval is rendelkezik. Az uniós jogi keretrendszer több szinten is rögzíti azokat az alapelveket, amelyekhez a munkahelyi technológiahasználatnak igazodnia kell.

Ennek egyik kiindulópontja az Európai Unió Alapjogi Chartája, amelynek 31. cikke a tisztességes és igazságos munkafeltételekről rendelkezik. A cikk kimondja, hogy minden munkavállalónak joga van az egészségét, biztonságát és méltóságát tiszteletben tartó munkafeltételekhez.[6] Ez a rendelkezés a digitális munkakörnyezetben is értelmezhető, mivel a munkavállalói méltóság nemcsak a fizikai munkakörnyezetre, hanem az adatvezérelt megfigyelésre, az algoritmikus értékelésre és az automatizált döntéstámogatásra is kiterjeszthető. A munkahelyi MI-rendszerek alkalmazása különösen akkor vethet fel alapjogi kérdéseket, ha a munkavállaló nem érti az őt érintő döntések logikáját, nincs érdemi lehetősége a döntések megkérdőjelezésére, vagy a technológiai rendszer aránytalan beavatkozást jelent a magánszférájába és szakmai autonómiájába.

Az Alapjogi Charta mellett a Szociális Jogok Európai Pillére is fontos szakpolitikai hivatkozási keretet jelent. (1. ábra) A 10. alapelv az egészséges, biztonságos és megfelelően alakított munkakörnyezethez, valamint a személyes adatok foglalkoztatással összefüggő védelméhez kapcsolódik. Fontos hangsúlyozni, hogy a Szociális Jogok Európai Pillére nem klasszikus értelemben vett, közvetlenül alkalmazandó jogszabály, hanem szakpolitikai és normatív irányú. Ennek ellenére releváns a digitális munkakörnyezet értelmezésében, mert összekapcsolja a munkahelyi egészségvédelmet, a munkakörnyezet emberhez igazítását és a foglalkoztatási adatok védelmét.[7]

A szabályozási mechanizmusok uniós jogi alapját részben az Európai Unió működéséről szóló szerződés 153. cikke adja.[9] Ez a rendelkezés lehetővé teszi, hogy az Unió támogassa és kiegészítse a tagállamok tevékenységét többek között a munkakörnyezet javítása, valamint a munkavállalók egészségének és biztonságának védelme területén. Ebből nem következik, hogy minden technológiai innováció automatikusan munkavédelmi szabályozási tárgy lenne, de az uniós alapjogi és munkavédelmi keretrendszer alapján a munkahelyi technológiahasználat nem választható el a munkavállalói jólét és biztonság kérdésétől.

Ebben az összefüggésben értelmezhető az AI Act is, amely nem munkavédelmi jogszabályként, hanem a mesterségesintelligencia-rendszerekre vonatkozó horizontális uniós szabályozásként teremthet új kapcsolódási pontokat a pszichoszociális kockázatok megelőzéséhez.

1. Ábra: A szociális jogok európai pillérének 20 alapelve [8]

ELMÉLETI KERETRENDSZER, A DIGITÁLIS MUNKAKÖRNYEZET PSZICHOSZOCIÁLIS KOCKÁZATAI

A felhőalapú rendszerek, az okoseszközök, az Internet of Things megoldások, a robusztus mennyiségű adatok elemzése és a mesterséges intelligencia alkalmazása ma már nem csupán különálló technológiai újításokként, hanem egymással szorosan összekapcsolódó, komplex rendszerként értelmezendők a biztonságtudomány fókuszában is. Ezek a technológiák olyan új, sokszor az Ipar 4.0 keretein belül megvalósuló platformalapú és algoritmikus munkahelyi helyzeteket hoznak létre, amelyekben a pszichoszociális kockázatok gyakran nem elszigetelten, hanem egymással és a technológiai infrastruktúrával összekapcsolódva jelennek meg. [10] [11]

Az EU-OSHA 2025-ös reprezentatív OSH Pulse jelentése empirikusan is alátámasztja, hogy a digitalizáció és az algoritmikus menedzsment széleskörű munkahelyi elterjedése szorosan összefügg a pszichoszociális kockázatok jelen tanulmányban vizsgált négy dimenziójával. Bár e technológiák önmagukban nem determinálnak pszichoszociális ártalmat, a felmérés adatai alapján az automatizált feladatkiosztás, a folyamatos monitorozás és az algoritmikus teljesítményértékelés szignifikánsan növelheti a munkavállalók kognitív túlterheltségét (a válaszadók 48%-ánál a szoftver diktálja a munkatempót), a társas izolációt (30%), a szakmai autonómia csökkenéséből fakadó kontrollhiányt (16-19%), valamint a rendszerek átláthatatlanságából eredő információs deficitet. Ezek az összefüggések egyértelművé teszik, hogy az MI-alapú munkahelyi rendszerek bevezetése nem szűkíthető le technológiai vagy hatékonysági kérdéssé; a sikeres integráció és az egészséges munkakörnyezet megőrzésének elengedhetetlen feltétele a célzott, munkavédelmi fókuszú pszichoszociális kockázatértékelés és a munkavállalók érdemi bevonása. [12]

A digitális munkakörnyezet elméleti keretrendszerének vizsgálatakor kiemelten figyelembe venni az algoritmikus vállalatirányítás munkahelyi egészségre és biztonságra gyakorolt hatásait. A Time to build a European digital ecosystem című európai szakpolitikai jelentés szerint a mesterséges intelligencia munkahelyi integrációja átalakítja a munkáltató és a munkavállaló közötti erőviszonyokat, és adataszimmetriát hozhat létre [13]. Az automatizált feladatelosztás, a folyamatos digitális megfigyelés és az átláthatatlan algoritmikus teljesítményértékelés a munkavállalói autonómia csökkenéséhez, kognitív túlterheléshez, valamint a szociális párbeszéd gyengüléséhez vezethet. Ez indokolja az olyan transzparenciát és emberi felügyeletet előíró szabályozási eszközök vizsgálatát, mint az AI Act [13].

A digitális munkakörnyezet pszichoszociális kockázatainak feltárására a tanulmány a korábbi kutatásban részletesen alátámasztott, négydimenziós modellt alkalmaz. [2] Ezek a gyakorlatban szorosan összefonódó dimenziók, a túlterheltség, az izoláció, az információs deficit és a kontrollhiány fogják át a legfőbb pszichoszociális kockázati kihívásokat. A túlterheltség az MI-rendszerek által diktált fokozott munkatempóból és a folyamatos, invazív monitorozásból fakadó kognitív-érzelmi technostresszt jelenti, míg az izoláció a platform- és távmunka során elmaradó spontán interakciókat és a társas támogatás erózióját írja le. Az információs deficit a „fekete doboz" jellegű, többlépcsős algoritmikus döntéshozatal átláthatatlanságából eredő bizonytalanságot és szervezeti igazságtalanságérzetet jelöli. Végül a kontrollhiány a munkavállalói autonómia csökkenésére utal, amikor a dolgozó érdemi ráhatás vagy emberi felülvizsgálati lehetőség nélkül kénytelen alávetni magát az automatizált feladatkiosztásnak és teljesítményértékelésnek.

A tanulmány a továbbiakban ezen a négydimenziós keretrendszeren keresztül vizsgálja, hogy az Európai Unió mesterséges intelligenciáról szóló rendelete miként reflektál a fenti kockázatokra. Bár az AI Act nem hagyományos értelemben vett munkavédelmi jogszabály, a modell segít azonosítani, hogy a rendelet egyes mechanizmusai hogyan kapcsolódnak a munkavállalói pszichoszociális jólléthez. A vizsgálat rávilágít, hogy a jogszabály specifikus rendelkezései, különösen a tiltott gyakorlatok meghatározása, az átláthatósági követelmények és az emberi felügyelet előírása már a technológia tervezési és alkalmazási szakaszában olyan irányítási garanciákat követelnek meg, amelyek közvetett és fontos módon egészítik ki a klasszikus munkavédelmi szabályozást a pszichoszociális kockázatok megelőzésében.

A KOCKÁZATOK CSÖKKENTÉSE AZ AI ACT MECHANIZMUSAIN KERESZTÜL

Az Európai Unió mesterséges intelligenciára vonatkozó szabályozása a digitális technológiák biztonságos, átlátható és alapjogokat tiszteletben tartó alkalmazását kívánja biztosítani, miközben egységes keretet teremt az MI-rendszerek fejlesztésére, forgalomba hozatalára és használatára. A mesterséges intelligenciáról szóló rendelet kockázatalapú megközelítést alkalmaz. Tiltott MI-gyakorlatokat határoz meg, részletes kötelezettségeket ír elő a magas kockázatú MI-rendszerekre, külön átláthatósági követelményeket kapcsol bizonyos rendszerekhez, míg a minimális vagy nem jelentős kockázatú rendszerek esetében nem állapít meg hasonló szigorú kötelezettségeket. A foglalkoztatás, a munkavállalói irányítás és az önfoglalkoztatás területe a rendelet III. mellékletében különösen érzékeny alkalmazási területként jelenik meg, mivel több ilyen célú MI-rendszer magas kockázatú besorolást kap. Ez arra utal, hogy az uniós jogalkotó felismerte: a munkahelyi MI-rendszerek

nem pusztán technológiai eszközök, hanem a munkáltató és a munkavállaló közötti döntési, információs és kontrollviszonyokat is alakítják. [3]

A kognitív túlterheltség és a technostressz csökkentése

A kognitív és pszichés túlterheltség egyik lehetséges forrása a munkahelyi érzelemfelismerő rendszerek és biometrikus megfigyelési technológiák alkalmazása. Amennyiben egy MI-rendszer arckifejezések, hanglejtés, hangszín, mozgásminták vagy más fiziológiai és viselkedési jelek alapján következtet a munkavállaló érzelmi állapotára, stressz-szintjére, elkötelezettségére vagy figyelmi állapotára, az a munkavállaló számára fokozott megfigyeltségérzetet és teljesítménynyomást eredményezhet. Ez a hatás különösen akkor jelent pszichoszociális kockázatot, ha a rendszer működése nem átlátható, a munkavállaló nem ismeri az értékelési logikát, vagy nincs érdemi lehetősége a technológiai döntések vitatására. [14]

Az AI Act 5. cikke a tiltott MI-gyakorlatok körében külön rendelkezik az érzelemfelismerő rendszerekről. A rendelet tiltja olyan MI-rendszerek forgalomba hozatalát, üzembe helyezését vagy használatát, amelyek természetes személyek érzelmeire következtetnek munkahelyi vagy oktatási intézményi környezetben, kivéve, ha az alkalmazás orvosi vagy biztonsági okból történik. Ez a rendelkezés közvetlenül nem pszichoszociális kockázatértékelési szabály, mégis releváns a munkahelyi pszichoszociális kockázatok szempontjából, mert korlátozza azokat az MI-alkalmazásokat, amelyek a munkavállalók érzelmi állapotának invazív és nehezen ellenőrizhető monitorozására irányulhatnak.

A munkahelyi MI-rendszerek szélesebb körében az AI Act III. melléklete több foglalkoztatással, munkavállalói irányítással és önfoglalkoztatással kapcsolatos alkalmazást magas kockázatúként nevesít. Ide tartozhatnak például a toborzásra és kiválasztásra, a munkafeltételeket érintő döntésekre, az előléptetésre vagy a munkaviszony megszüntetésére, továbbá a feladatkiosztásra, valamint a teljesítmény és viselkedés értékelésére használt rendszerek. Ez nem jelenti azt, hogy minden HR-célú szoftver automatikusan magas kockázatú lenne, de a rendelet egyértelműen különös figyelmet fordít azokra az MI-rendszerekre, amelyek a munkavállalók lehetőségeit, értékelését vagy munkafeltételeit érdemben befolyásolhatják.

A magas kockázatú besorolás több releváns kötelezettséget von maga után. A szolgáltatóknak kockázatkezelési rendszert kell működtetniük, megfelelő minőségirányítási rendszert kell fenntartaniuk, és biztosítaniuk kell többek között az átláthatóságot, az emberi felügyelet lehetőségét, valamint az adatminőségi követelmények teljesülését. Az alkalmazókra, vagyis a munkahelyi deployerekre is vonatkoznak kötelezettségek: az AI Act 26. cikkének (7) bekezdése alapján a munkahelyen használt magas kockázatú MI-rendszer üzembe helyezése vagy alkalmazása előtt tájékoztatni kell a munkavállalók képviselőit és az érintett munkavállalókat arról, hogy ilyen rendszer alkalmazásának lesznek kitéve. Ezek a kötelezettségek nem szüntetik meg önmagukban a technostresszt vagy a túlterheltséget, de olyan átláthatósági és szervezeti garanciákat teremtenek, amelyek segíthetik a túlzott monitorozásból, bizonytalanságból és kontrollvesztésből fakadó pszichoszociális kockázatok mérséklését.

Az izoláció mérséklése, emberi felügyelet és szervezeti visszacsatolás

Az izoláció a digitális gazdaság, a platformmunka, a távmunka és az algoritmikusan támogatott munkaszervezés egyik fontos pszichoszociális kockázata lehet. A digitális platformokon, alkalmazásokon vagy automatizált rendszereken keresztül történő feladatkiosztás csökkentheti a spontán munkahelyi interakciókat, az informális tanulási lehetőségeket, valamint a közvetlen vezetői és kollegiális támogatást. Ez különösen akkor válhat kockázattá, ha a munkavállaló a munkaszervezéssel elsősorban digitális értesítéseken, algoritmikus értékeléseken vagy alkalmazásokon keresztül találkozik, miközben kevés lehetősége van kérdezni, visszajelzést adni vagy a döntések emberi felülvizsgálatát kérni [15], [16].

Az AI Act nem ír elő közvetlenül szociális interakciókat vagy munkahelyi közösségépítő mechanizmusokat, ezért az izoláció mérséklése csak közvetett módon kapcsolható a rendelethez. Releváns azonban, hogy a magas kockázatú MI-rendszerek esetében a rendelet több olyan követelményt is megfogalmaz, amely a munkavállalók tájékoztatását, az emberi felügyeletet és a rendszer használatának értelmezhetőségét erősítheti. Ezek a követelmények nem szüntetik meg automatikusan a társas elszigetelődés kockázatát, de hozzájárulhatnak ahhoz, hogy az algoritmikus munkaszervezés ne teljesen zárt, emberi visszacsatolástól elszakított folyamatként működjön. A 27. cikk alapjogi hatásvizsgálatra vonatkozó rendelkezése e szempontból óvatosan használható hivatkozásként, mert a rendelkezés nem minden magas kockázatú MI-rendszer minden alkalmazójára vonatkozik, hanem meghatározott alkalmazói körben és meghatározott rendszertípusok esetén ír elő alapvetőjogi hatásvizsgálati kötelezettséget [3]. Mégis releváns a munkahelyi pszichoszociális kockázatok elemzésében, mert azt a szabályozási szemléletet fejezi ki, hogy a magas kockázatú MI-rendszerek bevezetésekor nemcsak technikai, hanem alapvetőjogi és társadalmi hatásokat is vizsgálni kell.

Az izoláció szempontjából erősebb kapcsolódási pontot jelent a 14. cikk szerinti emberi felügyelet és a 26. cikk (7) bekezdésében szereplő munkavállalói tájékoztatási kötelezettség. A 14. cikk célja, hogy a magas kockázatú MI-rendszerek működése során természetes személyek megfelelő felügyeletet gyakorolhassanak, míg a 26. cikk (7) bekezdése előírja, hogy a munkavállalókat és képviselőiket tájékoztatni kell, ha a munkahelyen magas kockázatú MI-rendszer alkalmazásának lesznek kitéve. Ezek a rendelkezések nem kényszerítik ki az emberi kapcsolódást a szó szoros értelmében, de erősíthetik az emberi visszacsatolás, a szervezeti kommunikáció és a munkavállalói részvétel feltételeit.

Ebből következően az AI Act izolációval kapcsolatos munkavédelmi jelentősége nem abban áll, hogy önmagában megszünteti a digitális munkavégzés társas kockázatait, hanem abban, hogy az algoritmikus döntéshozatal köré olyan tájékoztatási és felügyeleti keretet rendel, amely támogathatja a munkavállalók bevonását és a döntési folyamatok emberi értelmezhetőségét. A pszichoszociális kockázatkezelés szempontjából ez különösen akkor lehet releváns, ha a munkáltató a jogszabályi megfelelést összekapcsolja vezetői kommunikációval, panasz- és visszacsatolási csatornákkal, valamint a munkavállalók bevonásával a technológiai rendszerek bevezetésekor.

Információs deficit és átláthatóság

Az információs deficit az algoritmikus rendszerek átláthatatlanságából és az információs aszimmetriából fakadó bizonytalanságot jelöli. Munkahelyi környezetben ez akkor

válhat pszichoszociális kockázattá, ha a munkavállaló nem érti, hogy egy MI-rendszer milyen adatok, szempontok vagy értékelési logika alapján befolyásolja a teljesítményértékelését, feladatbeosztását, előmeneteli lehetőségeit vagy munkafeltételeit. Az algoritmikus menedzsment szakirodalma szerint az algoritmikus kontroll egyik sajátossága éppen az, hogy a munkavállalók gyakran korlátozottan látják át azokat a szabályokat és értékelési mechanizmusokat, amelyek munkájukat alakítják [17]. A „fekete doboz" jelleg nem minden MI-rendszer esetében azonos mértékű, és nem minden algoritmikus döntéstámogató eszköz teljesen értelmezhetetlen. Ugyanakkor a gépi tanulási és különösen a mélytanulási megoldások esetében előfordulhat, hogy a rendszer működésének részletes ok-okozati logikája a nem szakértő felhasználók, így a munkavállalók számára nehezen érthető. Ez a nehezen értelmezhető működés nagyrészt abból fakad, hogy a mesterséges intelligencia nem egy hagyományos szoftver, hanem egy többlépcsős, komplex rendszer, amelynek adatgyűjtési, feldolgozási és modellalkotási fázisai sajátos információbiztonsági és átláthatósági kihívásokat hordoznak magukban [18]. Ez nem szükségszerűen vezet pszichés ártalomhoz, de növelheti a bizonytalanságot, gyengítheti a szervezeti igazságosság észlelését, és csökkentheti a munkavállalói bizalmat.

Az AI Act e problémakörhöz elsősorban az átláthatóságra, a használati információkra és az egyedi döntések magyarázatára vonatkozó szabályokon keresztül kapcsolódik. A 13. cikk előírja, hogy a magas kockázatú MI-rendszereket úgy kell megtervezni és fejleszteni, hogy működésük kellően átlátható legyen az alkalmazók számára, és a szolgáltatóknak megfelelő használati utasítást kell biztosítaniuk. Ez a tájékoztatás többek között a rendszer rendeltetésére, képességeire, korlátaira, pontosságára, teljesítményére, az emberi felügyelet módjára és az előrelátható kockázatokra vonatkozó információkat tartalmazza. A 13. cikk tehát elsődlegesen a szolgáltató és az alkalmazó közötti átláthatóságot erősíti. Munkahelyi szempontból ennek közvetett jelentősége van, ha a munkáltató nem kap megfelelő információt a használt rendszer rendeltetéséről, korlátairól és kockázatairól, akkor a munkavállalók számára sem tud érdemi és pontos tájékoztatást adni. A 13. cikk ezért nem közvetlen munkavállalói magyarázati jog, hanem olyan előfeltétel, amely támogathatja a munkáltatói tájékoztatást, a munkavédelmi kockázatértékelést és az emberi felügyelet megszervezését.

A munkavállalók szempontjából közvetlenebb jelentőségű a 86. cikk, amely az egyedi döntéshozatal magyarázatához való jogot szabályozza. A rendelkezés alapján az a személy, akire nézve a magas kockázatú MI-rendszer kimenetén alapuló döntés joghatással jár, vagy egészségére, biztonságára vagy alapvető jogaira hasonlóan jelentős hatással van, kérésére világos és érdemi magyarázatot kaphat az MI-rendszernek a döntéshozatali eljárásban betöltött szerepéről és a döntés fő elemeiről. Ez a szabály különösen releváns lehet például toborzási, kiválasztási, teljesítményértékelési vagy munkaviszonyt érintő döntések esetén. A 86. cikk azonban nem feltétlenül követel teljes algoritmikus modellmagyarázatot, paramétersúlyok feltárását vagy lépésről lépésre történő technikai rekonstrukciót. Inkább olyan világos és érdemi magyarázati jogot biztosít, amely segíthet megérteni, hogy a magas kockázatú MI-rendszer kimenete milyen szerepet játszott az adott döntésben.

Összességében az AI Act információs deficittel kapcsolatos jelentősége abban áll, hogy az átláthatóságot nem pusztán etikai elvként, hanem jogi és szervezeti követelményként kezeli. A 13. és 86. cikk olyan eszközöket adhat a munkáltatók, munkavállalók és képviselőik kezébe, amelyek támogathatják az algoritmikus döntések érthetőbbé tételét. [19] Ez közvetetten hozzájárulhat a bizonytalanság, az igazságtalanságérzet és a kontrollvesztés

mérsékléséhez, feltéve, hogy a szervezetek a jogi megfelelést érdemi munkavállalói tájékoztatással és visszacsatolási mechanizmusokkal kapcsolják össze.

Kontrollvesztés és emberi felügyelet

A kontrollhiány a digitális és algoritmikusan támogatott munkaszervezés egyik központi pszichoszociális kockázati dimenziója. A munkapszichológiai szakirodalomban régóta ismert összefüggés, hogy a magas munkahelyi követelmények különösen akkor járhatnak fokozott megterheléssel, ha a munkavállaló alacsony döntési mozgástérrel vagy korlátozott kontrollal rendelkezik saját munkája felett. [20] Ez a logika a digitális munkakörnyezetben is releváns: az algoritmikus rendszerek nem csupán információt szolgáltatnak, hanem a feladatkiosztás, a teljesítményértékelés és a munkaritmus alakításán keresztül befolyásolhatják a munkavállalói autonómiát. Az algoritmikus menedzsmenttel kapcsolatos szakirodalom arra mutat rá, hogy az algoritmusok nemcsak koordinációs, hanem kontrollfunkciókat is betölthetnek. Irányíthatják a munkafolyamatokat, rögzíthetik és értékelhetik a teljesítményt, valamint bizonyos esetekben jutalmazási vagy szankcionáló logikákkal is összekapcsolódhatnak. Ha ezek a folyamatok nem átláthatók, és nincs érdemi emberi felülvizsgálati vagy beavatkozási lehetőség, a munkavállaló csökkent kontrollt és kiszolgáltatottságot élhet meg.

Az AI Act erre a problémakörre elsősorban a 14. cikkben megfogalmazott emberi felügyeleti követelményen keresztül kapcsolódik. A rendelkezés szerint a magas kockázatú MI-rendszereket úgy kell megtervezni és fejleszteni, hogy természetes személyek megfelelő felügyeletet gyakorolhassanak felettük a használat során. A felügyeleti intézkedések célja, hogy megelőzzék vagy minimálisra csökkentsék a magas kockázatú MI-rendszerek használatából eredő egészségi, biztonsági és alapjogi kockázatokat, különösen akkor, ha ezek a kockázatok a rendszer rendeltetésszerű vagy észszerűen előrelátható használata során merülhetnek fel.

A 14. cikk nem minden esetben jelent klasszikus human-in-the-loop modellt, és nem teszi minden MI-rendszert puszta javaslattevő eszközzé. Inkább azt írja elő, hogy a magas kockázatú rendszerek esetében a felügyeletet ellátó személyeknek megfelelő eszközökkel, jogosultságokkal és ismeretekkel kell rendelkezniük ahhoz, hogy értelmezni tudják a rendszer működését, figyelemmel kísérjék annak kimeneteit, felismerjék az esetleges hibákat vagy rendellenességeket, és szükség esetén beavatkozzanak. A rendelkezés említi azt is, hogy a felügyeletnek lehetővé kell tennie a rendszer használatának megszakítását vagy leállítását is, ha ez szükséges és arányos.

Az emberi felügyelet pszichoszociális jelentősége abban áll, hogy mérsékelheti az automatizált rendszerekkel szembeni kiszolgáltatottság érzését. Ha a munkavállaló tudja, hogy az algoritmikus kimeneteket felelős, megfelelően képzett emberi döntéshozó értelmezi, ellenőrzi és adott esetben felülvizsgálhatja, az támogathatja a kontrollérzetet és a szervezeti igazságosság észlelését. Ez azonban nem automatikus következmény, a 14. cikk csak akkor járulhat hozzá érdemben a pszichoszociális kockázatok mérsékléséhez, ha a szervezet a felügyeleti szerepeket világosan kijelöli, a döntési felelősséget nem hárítja teljesen az MI-rendszerre, és tényleges panasz- vagy felülvizsgálati lehetőségeket biztosít. A kontrollhiány tehát nem kizárólag jogi kérdés, hanem vezetési és munkaszervezési feladat is.

A PSZICHOSZOCIÁLIS KOCKÁZATOK ÉS AZ AI ACT SZABÁLYOZÁSI ESZKÖZTÁRA

Az alábbi táblázat a tanulmány pszichoszociális elemzési keretét foglalja össze. A táblázat nem azt állítja, hogy az AI Act automatikusan megszünteti az egyes pszichoszociális kockázatokat, hanem azt mutatja be, hogy a rendelet mely rendelkezései kapcsolhatók elsősorban és közvetetten az adott kockázatok mérsékléséhez. (1. táblázat)

Pszichoszociális kockázati dimenzió	Kóroki tényező a digitális munkahelyen	Releváns AI Act rendelkezés	Lehetséges munkavédelmi jelentőség
Túlterheltség	Invazív monitorozás, érzelemfelismerés, teljesítmény- és figyelemkövetés miatti fokozott pszichés terhelés.	5. cikk	Korlátozza az érzelemfelismerő rendszerek munkahelyi alkalmazását, és mérsékelheti az invazív monitorozásból fakadó terhelést.
Izoláció	Digitális platformokon vagy alkalmazásokon keresztül történő munkaszervezés, csökkent emberi visszacsatolás és gyengülő társas támogatás.	14. cikk; 26. cikk; 27. cikk	Támogatja az emberi felügyeletet, a munkavállalói tájékoztatást és a technológiai bevezetés alapjogi szempontú mérlegelését.
Információs deficit	Átláthatatlan algoritmikus döntések, ismeretlen értékelési szempontok, információs aszimmetria.	13. cikk; 86. cikk	Csökkenti az információs aszimmetriát az alkalmazóknak szóló tájékoztatás és az egyedi döntés magyarázatához való jog révén.
Kontrollhiány	Csökkent autonómia, korlátozott beavatkozási lehetőség, algoritmikus kimenetek kritikátlan elfogadása.	14. cikk	Növeli az emberi felülvizsgálat, beavatkozás és leállítás lehetőségét a magas kockázatú rendszerek esetében.

1. Táblázat: A digitális pszichoszociális kockázatok és az AI Act kapcsolódó szabályozási eszközei. Forrás: saját szerkesztés.

KÖVETKEZTETÉS

A mesterséges intelligenciáról szóló (EU) 2024/1689 rendelet olyan horizontális uniós szabályozási keretet hoz létre, amely nem munkavédelmi jogszabályként, hanem

belső piaci, biztonsági és alapjogvédelmi logikára épülő rendeletként szabályozza a mesterségesintelligencia-rendszerek fejlesztését, forgalomba hozatalát és alkalmazását [3]. A tanulmány elemzése ugyanakkor arra mutat rá, hogy a rendelet egyes rendelkezései, különösen a tiltott MI-gyakorlatokra, a magas kockázatú rendszerekre, az átláthatóságra, az emberi felügyeletre, az adatminőségre és az egyedi döntések magyarázatára vonatkozó szabályok, közvetett módon kapcsolódhatnak a munkahelyi pszichoszociális kockázatok megelőzéséhez és kezeléséhez.

A digitális munkakörnyezetben megjelenő pszichoszociális kockázatok nem kizárólag a technológia jelenlétéből fakadnak, hanem abból, ahogyan az MI-rendszerek a munkaszervezésbe, a teljesítményértékelésbe, a feladatkiosztásba, a megfigyelésbe és a munkavállalói kontrollviszonyokba beépülnek. A tanulmányban alkalmazott pszichoszociális, négydimenziós elemzési keret, a túlterheltség, az izoláció, az információs deficit és a kontrollhiány azt mutatja, hogy az AI Act egyes mechanizmusai nem önmagukban szüntetik meg ezeket a kockázatokat, hanem olyan szabályozási feltételeket teremthetnek, amelyek támogatják azok azonosítását, mérséklését és szervezeti kezelését.

A hagyományos munkavédelmi szabályozás továbbra is meghatározó marad. A 89/391/EGK keretirányelv és a magyar Munkavédelmi törvény alapján a munkáltató felelőssége a munkakörnyezetből, a munkaszervezésből és a munkavégzés módjából eredő kockázatok értékelése és kezelése. A magyar szabályozásban a pszichoszociális kockázat fogalma is megjelenik, ami különösen indokolttá teszi, hogy a digitális és algoritmikus munkaszervezés hatásai ne pusztán adatvédelmi vagy technológiai kérdésként, hanem munkavédelmi szempontból is értelmezésre kerüljenek. Ugyanakkor e követelmények csak akkor tölthetnek be tényleges munkavédelmi jelentőséget, ha a szervezetek azokat összekapcsolják a munkavállalói tájékoztatással, a részvétellel, a vezetői felelősséggel és a rendszeres pszichoszociális kockázatértékeléssel.

Gyakorlati szempontból ez azt jelenti, hogy az MI-rendszerek munkahelyi bevezetésekor nem elegendő kizárólag jogi vagy informatikai megfelelőségi szempontokat vizsgálni. A munkáltatóknak célszerű előzetesen értékelniük, hogy az adott rendszer milyen hatással lehet a munkatempóra, a regenerációs lehetőségekre, a társas kapcsolatokra, az algoritmikus döntések érthetőségére és a munkavállalói autonómiára. Különösen fontos az emberi felügyeleti pontok világos kijelölése, a döntések magyarázhatósága, a munkavállalói panasz- és visszacsatolási csatornák biztosítása, valamint annak vizsgálata, hogy a rendszer alkalmazása nem növeli-e aránytalanul a teljesítménynyomást vagy az információs aszimmetriát.

A tanulmány korlátja, hogy jogszabályi és koncepcionális elemzésre épül, ezért nem vállalkozik az AI Act tényleges munkahelyi pszichoszociális hatásainak empirikus mérésére. További kutatások szükségesek annak vizsgálatára, hogy az AI Act által előírt átláthatósági, emberi felügyeleti és adatminőségi követelmények a gyakorlatban milyen módon befolyásolják a munkavállalók terhelését, kontrollérzetét, szervezeti igazságosság-észlelését és pszichés jóllétét.

Összességében az AI Act nem tekinthető a pszichoszociális kockázatok önálló munkavédelmi szabályozásának, de fontos kapcsolódási pontot teremt a technológiaszabályozás, az alapjogvédelem és a munkavédelem között. Jelentősége abban áll, hogy a munkahelyi MI-rendszerek szabályozása révén a pszichoszociális kockázatok egy része már a technológia tervezési, forgalomba hozatali és alkalmazási szakaszában láthatóvá és kezelhetővé

válhat. A biztonságtudomány számára ez új kutatási és gyakorlati feladatot jelent, a mesterséges intelligencia munkahelyi alkalmazását nemcsak technikai innovációként, hanem az egészséget, biztonságot és emberi méltóságot érintő szociotechnikai beavatkozásként kell értelmezni.

FELHASZNÁLT FORRÁSOK

Irodalom

[1] E. Gábor, "A pszichoszociális kockázatok európai uniós és magyar szabályozási keretei," *Lege Artis Medicinae*, megjelenés alatt, 2026.

[2] E. Gábor és G. Szabó, "Leading in the AI-driven workplace: Key challenges in psychosocial risk management," in *AI and business environment: Transformations, challenges and ethics in the digital age*, Tirana Business University College, 2026, pp. 47–67. [Online]. Elérhető: https://tbu.edu.al/wp-content/uploads/2026/02/TBU_Proceedings-2026-Finale.pdf

[4] M. Bowdler, H. Lahti, M. Jelenko, G. Buresti, és T. Valtonen, "Algorithmic management and psychosocial risks at work: An emerging occupational safety and health challenge," *Scand. J. Work Environ. Health*, vol. 52, no. 1, pp. 1-5, Jan. 2026, https://doi.org/10.5271/sjweh.4270

[5] European Commission, Directorate-General for Employment, Social Affairs and Inclusion, *Study exploring the context, challenges, opportunities, and trends in algorithmic management in the workplace – Final report*, Publications Office of the European Union, 2025. [Online]. Elérhető: https://data.europa.eu/doi/10.2767/5629841

[8] Európai Bizottság, "The European Pillar of Social Rights in 20 principles." [Online]. Elérhető: https://ec.europa.eu/social/main.jsp?catId=1606&langId=hu

[10] Cs. Kollár, "A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában," in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Szerk. Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2019, pp. 47–61. Elérhető: https://drkollar.hu/wp-content/uploads/2020/01/kiadvany-2019.pdf

[11] S. Wright, "Artificial intelligence and work: A review of the European policy landscape," *Journal of Industrial Relations*, vol. 67, no. 5, pp. 794–805, 2025. Elérhető: https://doi.org/10.1177/00221856251394780

[12] European Agency for Safety and Health at Work, *OSH Pulse 2025: Occupational safety and health in the era of climate and digital change*, 2025. [Online]. Elérhető: https://osha.europa.eu/sites/default/files/documents/OSH-pulse-2025-climate-digital-change_EN.pdf

[13] G. R. Oosterwijk, M. Hasdenteufel, és J. Nogarede, Szerk., *Time to build a European digital ecosystem: Recommendations for the EU's digital policy*. Foundation for European Progressive Studies; Friedrich-Ebert-Stiftung, 2024. [Online]. Elérhető: https://feps-europe.eu/wp-content/uploads/2024/12/Time-to-build-a-European-digital-ecosystem-1.pdf

[14] European Agency for Safety and Health at Work, *Digital technologies at work and psychosocial risks – Evidence and implications for occupational safety and health*, Publications Office of the European Union, 2024. [Online]. Elérhető: https://data.europa.eu/doi/10.2802/0488296

[15] M. H. Jarrahi et al., "Algorithmic management in a work context," *Big Data & Society*, vol. 8, no. 2, 2021, doi: 10.1177/20539517211020332.
[16] K. C. Kellogg, M. A. Valentine, és A. Christin, "Algorithms at Work: The New Contested Terrain of Control," *Academy of Management Annals*, vol. 14, pp. 366-410, 2020, doi: 10.5465/annals.2018.0174.
[17] M. Möhlmann, L. Zalmanson, O. Henfridsson, és R. W. Gregory, "Algorithmic Management of Work on Online Labor Platforms: When Matching Meets Control," *MIS Quarterly*, vol. 45, no. 4, pp. 1999–2022, Dec. 2021, doi: 10.25300/MISQ/2021/15333.
[18] Cs. Kollár, "A mesterséges intelligencia, mint komplex rendszer információbiztonsági kihívásai," in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Szerk. Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2019, pp. 62–70. Elérhető: https://drkollar.hu/wp-content/uploads/2020/01/kiadvany-2019.pdf
[19] Bird & Bird, *European Union Artificial Intelligence Act: A guide*, 2026. [Online]. Elérhető: https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf
[20] R. A. Karasek Jr., "Job Demands, Job Decision Latitude, and Mental Strain: Implications for Job Redesign," *Administrative Science Quarterly*, vol. 24, pp. 285-308, 1979, doi: 10.2307/2392498.

Jogszabályok

[3] *Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról... (a mesterséges intelligenciáról szóló rendelet)*, HL L 2024/1689, 2024.7.12. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32024R1689
[6] *Az Európai Unió Alapjogi Chartája*, HL C 326, 2012, pp. 391–407. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:12012P/TXT
[7] *Intézményközi kihirdetés a szociális jogok európai pilléréről (2017/C 428/09)*, HL C 428, 2017, pp. 10–15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52017DC0250
[9] *Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata*, 2012. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:12012E/TXT

DOI: https://doi.org/10.12700/btsz.2026.8.2.127

ARTIFICIAL INTELLIGENCE AGENTS IN OFFENSIVE AND DEFENSIVE CYBER SECURITY

MESTERSÉGES INTELLIGENCIA ÁGENSEK AZ OFFENZÍV ÉS DEFENZÍV KIBERBIZTONSÁGBAN

KELEMEN László[1] – OLÁH Róbert[2]

Abstract

This paper explores the use of AI-based autonomous agents in offensive and defensive cybersecurity environments. Through laboratory experiments, it evaluates the vulnerability detection and network monitoring capabilities of large language model–based agents. The study analyzes agent behavior in a Cisco Packet Tracer simulated network using ASI, DC, and FT metrics, and tests a DeepSeek R1 and OpenClaw Clawdbot–based agent in a simulated office infrastructure. The research pro-vides practical insights into AI-driven threats and defense strategies for secu-rity professionals, pentesters, SOC/CSIRT teams, and researchers, who are interested in the "Practical understanding of AI-based threats and defense options in a pre-designed lab environment where the offensive and defensive capabilities of AI agents were evaluated.

Keywords

cybersecurity, threats, network traffic, pentesters, autonomous agents, lan-guage models

Absztrakt

A cikk az AI-alapú autonóm ügynökök (agentek) defenzív és offenzív kiberbiztonságban betöltött szerepét mutatja be és vizsgálja. A tanulmány célja annak feltárása, hogy a jelenlegi nagy nyelvi modellekre épülő „agentek" milyen tényleges sérülékenység-felderítési és hálózati forgalom-elemzési képességekkel rendelkeznek, saját kialakított labor környezetekben mért, reprodukálható kísérletek alapján. A vizsgálat egyik ága egy Cisco Packet Tracer alapú szimulált hálózaton elemzi az AI ágensek észlelési és döntési viselkedését (ASI, DC, FT mérőszámok), míg a másik ága egy szimulált irodai infrastruktúrát modellező laborban értékeli egy DeepSeek R1 modellre épülő, OpenClaw Clawdbot alapú autonóm „agent" felderítési és sérülékenység-azonosítási teljesítményét. A mű elsődleges célközönsége: biztonsági szakemberek, penteszterek, SOC/CSIRT csapatok, valamint kutatók, akik az „Az AI-alapú fenyegetések és védekezési lehetőségek gyakorlati megismerése egy előre kialakított laborkörnyezetben, ahol AI-agentek támadó és védelmi offenzív képességeit értékelését végzik.

Kulcsszavak

kiberbiztonság, fenyegetés, hálózati forgalom, penteszterek, autonóm ügynökök, nyelvi modellek.

[1] kelemenl@cyberexpert.hu | ORCID: 0009-0007-7566-8063 | penetrációs teszter, penetration tester | Sérülékenység kutató, etikus hacker, OFSZ Zrt

[2] olah.robert0721@gmail.com | ORCID: 0009-0007-9134-9521 | IT teacher, Center of Erd Education | Informatika oktató, Érdi Tankerületi Központ

BEVEZETÉS

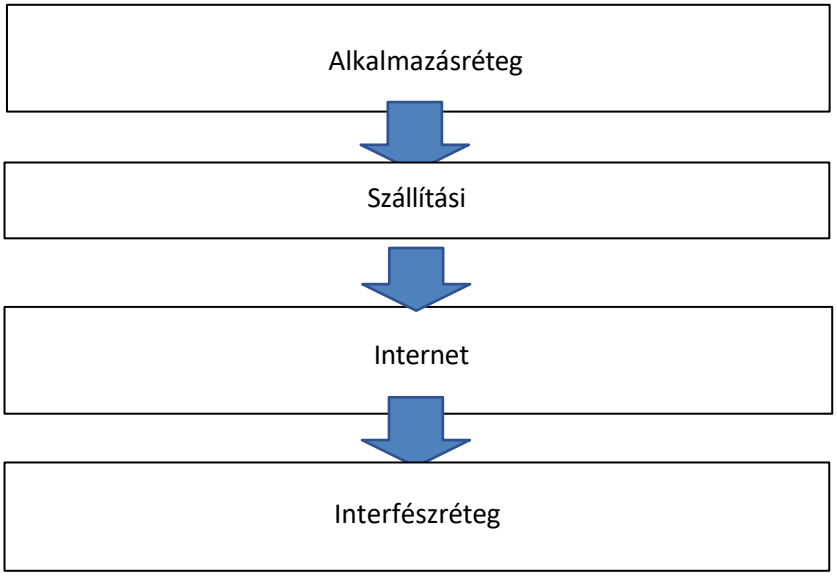
A mesterséges intelligencia és a kiberbiztonság konvergenciája az elmúlt évek egyik legdinamikusabban fejlődő kutatási területe. Az LLM-alapú autonóm ügynökök megjelenése új típusú fenyegetéseket és egyben új védelmi lehetőséget is jelentenek. Jelen tanulmány célja kettős: egyfelől elméleti és szimulációs megközelítésben mutatja be az AI ágensek és a hálózati sérülékenységek viszonyát, másfelől egy gyakorlati, izolált laboratóriumi környezetben végzett kísérletsorozat eredményeit ismerteti, ahol egy LLM-alapú „agent" szimulált irodai hálózati infrastruktúrán végzett felderítési és sérülékenység detektálási feladatokat. Az offenzív, sérülékenység felderítési vizsgálat célja az is, hogy bemutassa egy esetleges rosszindulatú támadó milyen képességű rendszert tud összerakni nyílt-forráskódú, illetve könnyen hozzáférhető rendszerekből.

Természetes nyelvi feldolgozás

A természetes nyelvi feldolgozás egy komoly kutatási terület, mert ezen a területen is alkalmazható a gépi tanulás, a gépi intelligencia a nyelv megértése, az emberi nyelvet amely lehet írott vagy szóbeli formában (adott szöveg értelmezés és felismerés , beszédfelismerés, fordítás adott nyelvről másik idegen nyelvre) A modell betanítjuk arra a funkcióra amire a feladat specifikációja szól. Nyilván van lehetőség további utakat nyitni, a modell további tanulás céljából. Az NLP segítségével, a szöveget tudjuk értelmezni, hangalapú információt felismerni, idegen nyelvű fordítás. Az NLP működésében a matematikai műveletek állnak, amelynek segítségével a gép számára értelmezhető az információ. Tekintettel mivel a kutatás a agensek témakörére épül, az ügynök az lehet maga a nyelvi modell, amire tanítunk, szabályokat állíthatunk fel a modellben. Az ügynököket egy neurális hálózatban képzeljük el, ezek lesznek a csomópontok az élek pedig a kommunikációs csatornák. Input ügynökként az információ feldolgozása történik meg, amely átmegy egy tisztító műveleten, majd ezután történik meg az információ elemzése, végül megtörténik a döntés és a válasz amely az eredmény kimenete lesz. Egy modell struktúrában több okos modell dolgozhat együtt, elemző ügynök, döntési ügynök, végrehajtó ügynök. koordinátor ügynök. Az elemző ügynök értelmezheti a rendszerben a logokat, és eseményeket, és elvégezheti az anomáliák felismerését is. A döntési ügynök, priorizálja a fenyegetéseket és ennek tudatában születik meg a döntés hogyan viselkednek az ágens. **[1][6]**

Sérülékenységet kategorizált súlyosság szerint

Amikor több számítógépet összekapcsolunk egy hálózatban, az információ nem közvetlenül, egy lépésben jut el egyik gépből a másikba, hanem több feldolgozási szakaszon keresztül halad. A továbbított adatok először jelekké alakulnak, amelyek lehetnek például elektromos impulzusok, rádióhullámok vagy fényjelek. Ezeket a jeleket a fogadó rendszer értelmezi, majd fokozatosan visszaalakítja olyan adatokká, amelyeket már szoftverek is fel tudnak dolgozni. Így a nyers fizikai jelből végül egy strukturált információ lesz, amit a felhasználói alkalmazások meg tudnak jeleníteni vagy használni. A hálózatban többféle protokoll működik kiemelt a TCP -IP protokoll. A TCP-ip protokoll. A protokollok segítségével jut el a csomag a hálózat egyik szegmenséből a másikba. [11]



1.ábra TCP IP réteg (saját szerkesztés)

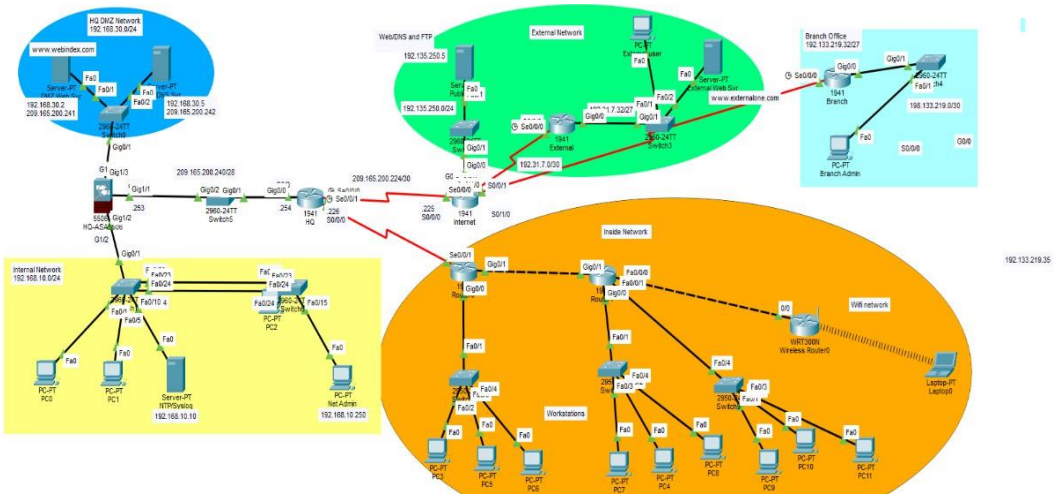
LLM konkrét shell parancsot generál

A nagy nyelvi modellben lehetőségünk van shell parancsot is generálni, a generálás a nyelvi modell által amit betanítottak az alapján generál scriptet, a másik nézőszempont pedig azt lehetne ami az ágens érzékelő érzékel, annak függvényében generálódik script amit az MI le futtathat a hálózaton. pl a szabad portok lezárása , behatolási pont védelme, és tűzfalszabályok módosítása a hálózat védelmének érdekében. Az igazat megvalva az MI-nek gyorsan kell döntenie, hogy mielőbb biztosítsa a hálózat védelmét a behatolás ellen, vagy megakadályozza a további károkat. Az MI modellnek hogy az ágensekkel jól tudjon együtt működni, szükséges behatolási mintázatokra, ami alapján hozza a döntést az MI a hálózatban.

A támadási mintázatok tartalmazzák a behatolás tényét, az MI modell pedig ezzel a tudáshalmazzal rendelkezik, azonban találkozhat az MI olyan hálózati behatolással ami nem ismert számára, sajnos ebben az esetben mondhatjuk a hipotézisként hogy nem rendelkezik a felismerés tényével, adott támadási szituációra, de úgy gondolom hogy egy fel nem ismert támadás esetén az MI dönthet , arra tekintve hogy az adott hálózati támadás generálhat egy olyan mintarészt amiből felismerhető részeket és annak ismeretében hozhat döntést.

A hálózati sérülékenységek

A mai modern információs társadalomban az informatikán belül a számítógépes hálózatok fontos szerepet töltenek be, a vállalati környezetben is. Az internet és a vállalati informatikai infrastruktúra informatikai hálózatra is épül. A rendszer működésének szempontjából lehetnek benne gyengeséges, és hálózati sérülékenységek az erőségek mellett. a Hálózati hiba olyan hiba amely a hálózati rendszerben illetéktelen hozzáférést, adatlopást, vagy olyan tevékenység amely kárt okoz a hálózatban. Az alábbi képen egy elképzelt hálózatot látunk ahol az ágensek működhetnek. [4][6]



2.ábra Hálózati modell saját szerkesztés [4]

Eszköz	Interface	IP cím	Subnet Mask	Gateway	DNS
Internet	S0/0/0	209.165.200.225	255.255.255.252	n/a	n/a
Internet	S0/0/1	192.31.7.1	255.255.255.252	n/a	n/a
Internet	S0/1/0	198.133.219.1	255.255.255.252	n/a	n/a
Internet	G0/0	192.135.250.1	255.255.255.0	n/a	n/a
HQ	S0/0/0	209.165.200.226	255.255.255.252	n/a	n/a
HQ	G0/0	209.165.200.254	255.255.255.240	n/a	n/a
HQ-ASA5506	G1/1	209.165.200.253	255.255.255.240	n/a	n/a
HQ-ASA5506	G1/2	192.168.10.1	255.255.255.0	n/a	n/a
HQ-ASA5506	G1/3	192.168.20.1	255.255.255.0	n/a	n/a
Branch	S0/0/0	198.133.219.2	255.255.255.252	n/a	n/a
Branch	G0/0	198.133.219.62	255.255.255.224	n/a	n/a
External Web Server	NIC	192.31.7.35	255.255.255.224	192.31.7.62	n/a

Eszköz	Interface	IP cím	Subnet Mask	Gateway	DNS
External User	NIC	192.31.7.33	255.255.255.224	192.31.7.62	192.135.250.5
AAA/NTP/Syslog Server	NIC	192.168.10.10	255.255.255.0	192.168.10.1	n/a
DMZ DNS Server	NIC	192.168.20.5	255.255.255.0	192.168.20.1	n/a
DMZ Web Server	NIC	192.168.20.2	255.255.255.0	192.168.20.1	192.168.20.5
PC0, PC1, PC2	NIC	DHCP	255.255.255.0	192.168.10.1	192.168.10.10
Branch Admin	NIC	198.133.219.35	255.255.255.224	198.133.219.62	192.135.250.5
NetAdmin PC	NIC	192.168.10.250	255.255.255.0	192.168.10.1	192.168.10.10

1.táblázat ip cím tervezet a szimulációhoz

A sérülékenységek a hálózatban az alábbiak alapján soroltuk be.

- Hardveres
- Szoftveres
- Konfigurációs hibák

A hardveres sérülékenységek szintén lehetnek a szoftveres mellett, az alábbiak szerint

- Router, swich, szerver hiba
  - port hiba/Interfész hiba
  - IC áramköri hiba
- Táp hiba, Memória hiba

Szoftveres esetén (lehetséges esetek)

- Cisco router esetén IOS hiba,
- parancsértelmező shell
- rossz vagy nem megfelelő konfiguráció
- sikertelen firmware frissítés, esetén rollback ami az legutóbbi stabil firmware verzióra tér vissza. [4] [6]

Sérülékenységek felismerése

A hálózatok működése során lehetnek sérülékenységek, ilyen az információ továbbítása során mint adatcsomag, a protokollok segítségével az adott adatcsomag, ha sérült rész érkezett A alhálózatból B be akkor a TCP /IP protokoll segítséget adhat az adatcsomag kijavításában, mert a protokoll kéri a adó állomástól hogy újra küldje el a vevő állomás felé. Ez a hálózatnak csomag biztonságot ad a hibamentes csomagküldés szempontjából, minden egyes bit információ ellenőrizve van, ha nem egyezik az ellenőrző összeg akkor a hibás csomag újraküldését kéri a protokoll. [6]

Hálózati támadások szimulációs modell alapján

A packet tracerben tervezett modellben vizsgálati eseteket végeztünk, amelyben a hálózat védelmi lehetőségeit tártuk fel. Az érzékelő ágensek itt a routerek, szerverek, gépek, a cselekvő funkció pedig a konfigurációban beállított funkciók pl : tűzfalszabályok, (iptables). A behatolás ellen pedig egy tűzfalat konfiguráltunk fel, ami egy ASA tűzfal. a szimulátoron kívül egy ASA tűzfalra hardverként kell tekinteni amit beépítve a hálózatban a webes felületen érhető és konfigurálható. A hálózati támadások szimulált környezetben történtek amely alapján kaptuk az eredményeket. DDOS támadás, egy túlterheléses támadás ami azt jelenti az esetünkben hogy a hálózati erőforrásokat pl ruoter és hálózati szerverek túlterhelése a cél. Óriási adatforgalmat küldenek a hálózatra amelynek segítségével a routerek működését bénítják meg, így a rendszer felhasználói ne érjék el a hálózati erőforrásokat. [11][12]

Védekezési módszerek

Egy hálózati támadás során többféle védekezési módszer alkalmazható. (Viselkedés alapú elemzés, AI alapú forgalomfigyelés, Webes Application Firewall stb.) A hálózati szimulációs modellünkben az ASA tűzfal szerver található, amely alkalmas a hálózati védelemre, ezen kívül ASA nélkül alkalmazhatók a routereken az ACL szabályok amelyek a hálózat csomag forgalmi szabályát és védelmét szolgálhatja.

Az ASA tűzfal konfigurálása az alábbiak alapján történt

- Konfigurálja az INSIDE és OUTSIDE interfészt

Jelenleg csak a G1/1 (KÜLSŐ) és G1/2 (BELSŐ) interfészt kell konfigurálnia. A G1/3 (DMZ) interfész a tevékenység 5. részében lesz konfigurálva.

- Hozza létre a G1/1 interfészt a külső hálózathoz (209.165.200.224/29), állítsa a biztonsági szintet a legalacsonyabb 0-ra, és engedélyezze az interfészt.

NETSEC-ASA(config-if)# interface

g1/1 NETSEC-ASA(config-if)#

nameif OUTSIDE

NETSEC-ASA(config-if)# ip address 209.165.200.226 255.255.255.248

NETSEC-ASA(config-if)# secu-

rity-level 0 NETSEC-ASA(config-

if)# no shutdown

b. Konfigurálja a G1/2 interfészt a belső hálózathoz (192.168.1.0/24), állítsa a biztonsági szintet a legmagasabb 100-as értékre, és engedélyezze az interfészt

NETSEC-ASA(config)# interface

g1/2 NETSEC-ASA(config-if)#

nameif INSIDE

NETSEC-ASA(config-if)# ip address 192.168.1.1 255.255.255.0

NETSEC-ASA(config-if)# security-

level 100 NETSEC-ASA(config-if)#

no shutdown

OSPF a forgalomirányítást

A routerek forgalomirányítása kiemelendő tématerület és funkció is, hiszen ez alapján döl el a a hálózati forgalmi csomag működése.

Részlet a forgalomirányítás konfigurációból.

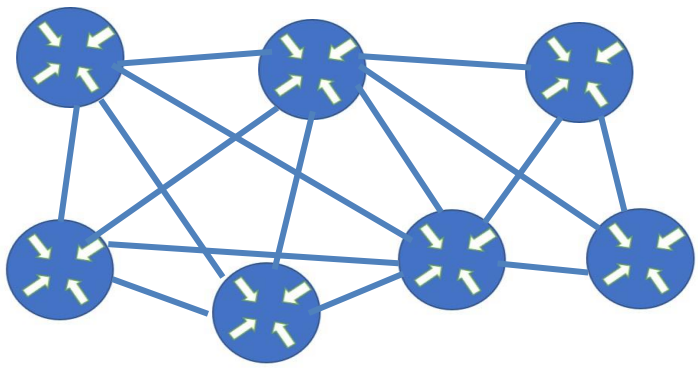
NETSEC-ASA(config-if)#router ospf 2

NETSEC-ASA(config-if)#network 209.165.200.0

NETSEC-ASA(config-if)#network 192.31.7.1

A fenti konfiguráció részlet alapján konfiguráljuk be a forgalomirányítást.

Az OSPF (Open Shortest Path First) egy link-state alapon működő forgalomirányítás protokoll, amely a Dijkstra algoritmus segítségével számítsa ki az legrövidebb útvonalat a hálózatban. A OSSPF működése egy olyan algoritmuson alapul ami a legrövidebb utat számolja ki és határozza meg a hálózat környezetében. Ez az alábbi kép alapján tudjuk elképzelni.



3.ábra Hálózati gráf (OSPF útvonalak) saját szerkesztés

A nyelvi modellek hozzáillesztése a hálózathoz

A hálózat működéséhez az AI hozzáilleszthető. AI agentek képesek lehetnek önállóan felderítési, sebezhetőség-azonosítási és kihasználási feladatokat elvégezni kontrollált labor környezetben. Az AI modell amelyben által az ágensek működnek a hálózat valós adatait figyelik, és ehhez mérten módosításra kerülhetnek a kapcsolati költségek, így a fenti ábra mintaként szolgál, hogy az útvonal költségek a Dijkstra algoritmus segítségével meghatározhatóak legyenek. AI modellek a neurális hálózatban működnek, az útvonalakat proaktívan optimalizálva vannak. Itt az AI felismeri a hálózati hibákat, és a szokatlan forgalmi mintákat. Automatikus újraroting történhet.

AI felismerheti

- hálózati hibákat
- DDoS támadásokat
- szokatlan forgalmi mintákat

Az AI döntések, meghatározzák a hálózat forgalmi működését. AI AI nem váltható ki az OSP re mint protokollra, mert a mesterséges intelligencia alkalmazása kiegészítő csomagként kell elképzelni amely segítheti a hálózat optimálisabb működését, azonban a betanított modell függvényében végezhet optimális forgalomirányítást az OSP protokollal együtt. Egy kontrollált laborban az AI ügynökök a felderítés során mint egy térkép rajzolódik ki az egyes hálózati szegmensek, és összekapcsolják a megfigyeléseket a modellben betanított hálózati mintákkal. A hálózat felderítése során nemcsak a hálózatot ismerheti fel, hanem a konfigurációs hibákat, pl helytelen ACL tűzfalszabályok. A hálózati felderítés nagyrészt automatizálható, és priorizálhatóak a támadási felületek ha bekövetkezik támadás a hálózatban. Az AI felismerheti a hibákat, elemezheti az outputokat, de nem mindent ismerhet fel, hiszen a modellt tanitani kell amihez sok minta kell, támadási lánc ami alapján dönt az AI az ágensekre kivetítve. A recon és scan automatizálás miatt a tömeges támadások könnyebbé válhatnak, ebben az esetben az elsődleges cél az **attack surface minimalizálás** azaz a feleslegesen nyitva hagyott portok automatikus lezárásra kerülnek (tiltás), és ami nem kell a hálózati szolgáltatásokhoz azt célszerű kikapcsolni. Fontos a hálózatban a megfelelő jogosultsági szint, és annak alkalmazása, ha egy fiók kompromitálódna kevesebb a kár. Célszerű autentikációs módot alkalmazni így jelentősen csökkentjük a jogosulatlan hozzáférés mellett az admin felületek elrejtése a publikus hálózaton. A tapasztalat azt mutatja, hogy az AI korában a támadók gyorsan feltérképezik a hálózatot és keresik az automatikus sebezhetőséget. Az alábbi mérőszámokat alkalmaztam a hálózatban, Az ASI modellezési metrika, amit alkalmaztam a modellünkre. [8][7][12]

$$ASI=P+S+E$$

- P (nyitott portok száma)
- S=aktív hálózati szolgáltatások száma
- E=külső interfészek száma

$$ASI=3+3+2=7$$

Az ASI nál nincs szabványos maximum, mert a hálózatok mérete eltérő lehet, de a hálózat rendszeradminisztrátora azonban meghatározhatunk a saját tervezett és konfigurált hálózatban egy relatív maximum értéket, de legjobb ha egy normalizált értéket határozunk meg az alábbiak alapján

$$\text{ASI norm} = \text{ASI}/\text{ASI max}$$

ASI norm	Jelentése
0.0-0.2	nagyon biztonságos
0.2-0.5	közepes
0.5-0.8	gyenge
0.8-1.0	kritikus szint

2.táblázat Normalizált értékek (saját szerkesztés)

Észlelési képesség (DC)

DC = detektált események / összes szimulált esemény

Értéksáv	Jelentése	Okok
0 – 0.5 (0–50%)	a támadások nagy része **észrevétlen marad**	· nincs ACL / monitoring · túl nyitott hálózat
0.5 – 0.8 (50–80%)	· a támadások egy része észrevétlen marad · részleges védelem	· hiányos logging · kevés monitoring pont
0.8 – 1.0 (80–100%)	· a hálózatod **szinte minden támadást észrevesz** · jól működik a monitoring / logging / ACL / IDS logika	· jól konfigurált ACL-ek · van logolás · van (vagy szimulált) IDS logika

3.táblázat Észlelési képesség

Tűzfal vizsgálat:

Mennyire szigorú a tűzfal.

FT=Deny rules / Total rules

- 0 nincs védelem
- 1 mindent tilt

DC = detektált események / összes szimulált esemény

- ideális: 0.4 – 0.8 érték

OFFENZÍV VIZSGÁLAT

Technikai megvalósítás és kísérleti környezet

A kutatás célja egy autonóm, nagy nyelvi modell (LLM) alapú kiberbiztonsági ügynök („agent") gyakorlati képességeinek vizsgálata volt, különös tekintettel a hálózati felderítés és sérülékenységvizsgálat, a sérülékenységek feltárásának területére. Alapvetően azon lehetőség feltárása is a vizsgálat célja volt, hogy nyílt forráskódú és könnyen hozzáférhető elemekből például egy rosszindulatú támadó milyen képességű rendszert képes összeállítani és ezzel mire lehet képes. A sérülékenységek kihasználása jelen vizsgálatnak nem volt célja. A rendszer egy irodai hálózatot szimulálva egy izolált laboratóriumi környezetben került kialakításra, ahol az „agent" képes volt távoli kapcsolaton keresztül műveleteket végrehajtani egy dedikált támadó környezeten keresztül. A jelen fejezet részletesen bemutatja a rendszer architektúráját, működési modelljét, a használt eszközöket, valamint a kísérleti konfigurációt.

Rendszer architektúra

A kialakított rendszer egy többrétegű, virtualizált architektúrán alapul, amelynek célja az autonóm döntéshozatal és a tényleges végrehajtás szétválasztása volt. A virtualizációs réteget egy Proxmox VE 9.1.1 alapú hypervisor biztosította, amelyen a virtuális gépek KVM (Kernel-based Virtual Machine) technológiával futottak. Az „agent" környezetnek egy Openclaw alapú Clawdbot konfiguráció került telepítésre, amely képes természetes nyelvi input feldolgozására, feladatok strukturált bontására, valamint külső rendszerek vezérlésére. Az LLM-komponensnek egy API-n keresztül elérhető modellt használt. Ez a modell a Deepseek Reasoner (R1) nagynyelvi modell volt.A felhasználó és az „agent" közötti kommunikáció a Telegram Bot API-n keresztül. A rendszer három logikai rétegre bontható: (1) felhasználói réteg (Telegram interfész), (2) döntési réteg („agent" VM, LLM, task planner, parancs-generátor), és (3) végrehajtási réteg (Kali Linux VM). Az „agent" és a Kali VM közötti kommunikáció SSH protokollon keresztül valósult meg, kulcs alapú autentikációval, egy ehhez generált kulcs párral.

Hálózati topológia és izoláció

A kísérleti környezet egy logikailag elkülönített, labor jellegű hálózatban került kialakításra. A topológia három fő szegmensből állt. Az „agent" VM kizárólag a Kali Linux rendszerrel kommunikált SSH kapcsolaton keresztül, a Kali VM ezzel párhuzamosan rendelkezett közvetlen, de szegmentált hálózati hozzáféréssel a 192.168.100.0/24 teszthálózaton lévő célrendszerekhez. A fizikai hálózatban több fizikai hálózati eszköz volt található, munkaállomásokkal és egyéb eszközökkel egyaránt.

Az „agent" működési modellje

Az „agent" működése egy többlépcsős, visszacsatolásos döntési és végrehajtási folyamaton alapul.

A folyamat a következő, jól elkülönített logikai fázisokból áll:

Az első fázis a természetes nyelvi feldolgozás és célkitűzés-generálás: a felhasználói üzenet tokenizálódik, majd az LLM egy belső reprezentációt épít fel a feladatról, amelyet strukturált célokba fordít (pl. „azonosítsd az aktív hostokat a 192.168.100.0/24 hálózaton").

A második fázis a tervező modul (task planner) működése, amely a célt atomi részfeladatokra bontja, prioritásokat rendel hozzájuk, és egy végrehajtási sorrendet javasol. A

Clawdbot/OpenClaw architektúrában ez a réteg szervesen integrálódik a „skills" alrendszerrel, ahol a tervező a rész feladatokhoz nem közvetlenül parancsokat rendel, hanem először a „workspace"-ben és a ClawHub regiszterben elérhető SKILL.md fájlok között keres megfelelő képességet (pl. nmap-recon, service-enum, vuln-lookup).

A harmadik fázis a parancs-szintézis: a tervező által előállított rész feladathoz az LLM konkrét „shell" parancsot generál, amelybe akár a korábbi futások eredményeiből kinyert paraméterek (pl. azonosított IP-tartomány, nyitott portok) kerülnek beillesztésre.

A negyedik fázis a végrehajtás és visszacsatolás: a generált parancs SSH-n keresztül futtatásra kerül a Kali VM-en, a standard output (stdout) és standard error (stderr) csatornák tartalma visszakerül az „agent" kontextusába. Az „agent" ezt elemzi, és a következő döntési ciklus alapjául használja.

Ez az architektúra egy ReAct (Reason + Act) típusú „agent"-keretrendszert valósít meg, amelyben a megfigyelés–gondolkodás–cselekvés ciklus explicit módon megjelenik.

SSH-alapú vezérlés és végrehajtás

A rendszer egyik kulcseleme az SSH-alapú vezérlési mechanizmus. A kulcs alapú autentikáció valósult meg, az „agent" VM tartalmazza a privát kulcsot, a Kali VM authorized_keys fájlja a nyilvános kulcsot.

A Kali Linux rendszeren az „agent" által használt felhasználói fiók (pentest_"agent") egy dedikált, korlátozott shell-környezetben (rbash) futott. Bizonyos, magasabb privilégiumot igénylő műveletek végrehajtásához korlátozott „sudo" jogosultságok álltak rendelkezésre, amelyek egy whitelist alapú sudoers konfigurációval kerültek engedélyezésre.

Használt eszközök és vizsgálati módszerek

A vizsgálatok során az „agent" dinamikusan és szabadon választott a feladat végrehajtása érdekében a Kali Linux teljes eszköztárból. Előre nem került neki meghatározásra egyetlen eszköz sem, teljesen autonóm módon döntött mit és hogyan használ.

Az önálló döntései során az alábbi eszközöket használta:

Felderítési fázis: nmap (TCP SYN scan, -sS, -sV, -O), netdiscover (ARP-alapú host discovery), masscan (nagy sebességű port scanning). Az nmap futtatásakor az „agent" az -oX kapcsolóval XML formátumú kimenetet igényelt, amelyet utólag egy Python-alapú parser dolgozott fel strukturált adattá (nyitott portok, szolgáltatás verziók, OS fingerprint).

Webes alkalmazások vizsgálata: nikto (HTTP fejlécek és ismert sebezhetőségek), gobuster (directory és file enumeration szótár alapú módszerrel), whatweb (technológia-fingerprinting). A gobuster alapértelmezetten a SecLists common.txt szótárát használta.

Sérülékenység-azonosítás: searchsploit (offline Exploit-DB keresés), sqlmap (SQL injection automatikus detektálása és tesztelése), Metasploit Framework (moduláris exploit keretrendszer). DNS-felderítéshez dnsenum és dnsrecon kerültek alkalmazásra.

Fontos megjegyezni, hogy az eszközök paraméterezése sem volt előre kötött: az „agent" kontextusfüggően állította be az -T (időzítési profil), --min-rate, és -p (portlista) kapcsolókat, a tapasztalati alapján szabadon. Ez a rugalmasság közelebb áll az emberi sérülékenység kutatók/pentesterek módszertanához, azonban növeli a kiszámíthatatlanságot és nehezíti a reprodukálhatóságot.

OWASP-alapú metodológiai leképezés és a „skill”

Az „agent” működése implicit módon illeszkedik az OWASP Web Security Testing Guide (WSTG) és az OWASP Testing Guide általános fázisaihoz. A vizsgálathoz alkalmazott OpenClaw Clawdbot „agent” úgynevezett „skill”-ekkel rendelkezhet. Ezeket képességeket vagy előre meghatározott témákban lehet hozzá integrálni vagy akár utasításra saját képességekkel lehet felruházni. (például: „Bővítsd ki a képességeidet az OWASP módszertan szerinti eszköztárral!”) A teszt rendszer tekintetében az OWASP módszertan teljes tárháza került elsődlegesen „skill” -ként integrálva az „agent”-be.

A rendszerben „.md” fájlokban találhatóak a képességekhez köthető „tudás” alapok. A vizsgált rendszer sérülékenység vizsgálat teszter képesség fájljai:

├── methodology.md (3 945 B) – A vizsgálatot végző saját sérülékenységvizsgálati tapasztalatai

├── owasp-methodology.md (15 030 B) – OWASP módszertan (14 fejezet)

├── report-template.md (626 B) – Jelentés sablon

└── tools.md (5 069 B) – Eszközök és parancsok referencia

Logging és auditálhatóság

A kísérleti rendszer naplózási alrendszere két jól elkülönített szinten működik, amelyek együttesen biztosítják a teljes működés visszakövethetőségét és a kísérletek utólagos reprodukálhatóságát.

- Első szint — Parancs- és eredménynaplók

A végrehajtott parancsok nyers kimenete fájlrendszer-szinten kerül megőrzésre. A vizsgálati eredményeket dátumozott szöveges fájlok tárolják scan_YYYY-MM-DD.txt névkonvencióval; ezek például az nmap, curl és nikto futtatások kimenetét tartalmazzák egységes sorrendben, az egyes eszközök kimenetei blokkfejlécekkel elválasztva. A könyvtárba minden futtatott parancs kimenete automatikusan mentésre kerül, ami lehetővé teszi az eszközök közötti átmenetek és a vizsgálat teljes menetének offline rekonstrukcióját.

Az összegző értékelés PDF formátumban, pentest_report_YYYY-MM-DD.pdf névvel kerül előállításra. A riport generálása a generate_report.py szkripttel történik, (melyet az „agent” készített. A szkript beolvassa az adott nap vizsgálat fájljait és kinyeri a strukturált adatokat (nyitott portok, azonosított szolgáltatások, potenciális sérülékenységek), majd egy előre definiált sablonra vetítve egységes, olvasható riportot állít elő.

- Második szint — Memórianaplók (workspace/memory/YYYY-MM-DD.md)

Az „agent” hosszú távú kontextus-megőrzése egy külön memória-könyvtárban, napi „Markdown” fájlokban valósul meg. A methodology.md konfigurációs fájl explicit előírja ezt a viselkedést: a „napi napló memóriába" direktíva határozza meg, hogy az „agent” minden munkanap végén összefoglaló bejegyzést készít az aktuális dátumhoz tartozó memória fájlba (workspace/memory/YYYY-MM-DD.md).

A memória fájl struktúrája kötetlen, de jellemzően tartalmazza a nap során elvégzett feladatok listáját, az azonosított sérülékenységeket és azok kontextusát, az „agent” döntési folyamatának kulcs lépéseit (például az eszközváltás indokát), valamint a nyitott kérdéseket

és a következő munkamenetbe átvitt feladatokat. Ezen kívül rögzítésre kerülnek a rendellenes események is, például a félresikerült parancsok, váratlan válaszkódok, vagy az „agent" által explicit bizonytalansági jelzéssel ellátott döntések.

Kísérleti konfiguráció

A kutatás teszthálózata egy olyan izolált laborhálózat, amely egy szimulált irodai infrastruktúra mintájára készült, amely egy Proxmox VE alapú szerver platformot és a hozzá tartozó belső hálózatot foglalja magába. A teszthálózat nem tartalmazott „CTF" szervereket, hanem egy szándékosan egy valós példa hálózat szimulációját tűzte ki célul.

A vizsgált alhálózaton összesen 7 aktív host került azonosításra. Az egyes eszközök szerepe és kockázati besorolása nmap OS fingerprinting és service detection kimenetei, alapján került meghatározásra.

A hálózat főbb komponensei a következők voltak: egy „fogyasztói" kategóriás router mint hálózati átjáró, amelyen aktív UPnP-szolgáltatás és nyitott HTTP admin felület futott, két Proxmox-csomópont, amelyek közül az egyiken a hypervisor REST API-ja belső hálózatról korlátozás nélkül elérhető volt; egy Windows 10/11 munkaállomás egy azonosítatlan nyitott porttal, valamint két azonosítatlan, feltehetőleg mobil- vagy IoT-kategóriájú eszköz. A tesztelő Kali Linux VM maga is a Proxmox infrastruktúrán belül futott, ami azt jelenti, hogy a tesztelő és a vizsgált rendszerek azonos fizikai hardveren osztoztak.

Az alkalmazott eszközök — pl. nmap, curl, openssl — kizárólag a felderítési fázisban kerültek felhasználásra, aktív exploitálási kísérlet nem történt.

ÖSSZEFOGLALÓ ÉS ÉRTÉKELÉS

A kísérlet eredményei

A kutatás egy autonóm, LLM-alapú kiberbiztonsági agent egy iroda hálózati környezetben való alkalmazhatóságát demonstrálta. A nyílt forráskódú és a könnyen hozzáférhető elemek használata azt is demonstrálta, hogy egy feltételezett rosszindulatú támadó milyen képességű rendszert képes elkészíteni és azt milyen módon tudja használni. A vizsgálat jelen esetben kimondottan nem hagyományos sérülékeny „CTF" (Capture the Flag) rendszereken végezte a sérülékenység vizsgálatokat, mivel az volt a cél, hogy minél valósághűbb környezetben végezze a vizsgálatokat az ügynök. Egy szervezet ellen irányuló szimulált támadás, vagy fenyegetettség elemzés alapjait mutattatja be elsődlegesen ez a vizsgálat. A vizsgálat feltételezte azt hogy a „támadó" már a hálózathoz kapcsolódik akár egy nyitott vagy rosszul konfigurált wi-fi hálózaton keresztül. Az „agent" képes volt önállóan elvégezni a hálózati felderítés teljes első fázisát: azonosított 7 aktív hostot, feltérképezte a futó szolgáltatásokat, és 5 sérülékenységet kategorizált súlyosság szerint. A legkritikusabb megállapítások (aktív UPnP-szolgáltatás a TP-Link routeren (F-01), a nyitott HTTP admin panel (F-02), és a Proxmox REST API belső hálózatról való korlátlan elérhetősége (F-03)), mind olyan problémák, amelyek valódi irodai hálózatokon is rendszeresen előfordulnak. A vizsgálat során megállapítható volt, hogy az „agent" képes volt a sérülékenység felderítések során önálló döntéseket hozni. A vizsgálat során amennyiben egy-egy szoftver eszköz nem volt megfelelő valamiért, az eszközhasználat során is meghozta az önálló döntéseket, azaz eszközt váltott, illetve utána nézett az adott eszköz javasolt beállításainak is a távoli LLM segítségével.

Az autonóm sérülékenység vizsgálat és „pentesting" rendszerek kockázatai

Az LLM-alapú, autonóm ügynökök kiberbiztonsági alkalmazása a kutatási szakirodalomban egyre nagyobb figyelmet kap. Fang és munkatársai (2024) kísérletei azt mutatják, hogy GPT-4 alapú ágensek képesek egy- és néhány-lépéses CVE-sérülékenységek önálló azonosítására és kihasználására, ha azok leírása elérhető a modell számára, azaz az automatizált exploitálás küszöbe lényegesen alacsonyabb lett, mint korábban feltételezték.[7] Ez a tendencia közvetlenül releváns a jelen kutatásra. Az „agent" jelenlegi feladatai a sérülékenység felderítési fázisára korlátozódtak a vizsgálat során, azonban a művelet kiterjesztése exploit-generálással, akár egy Metasploit modul kiválasztásán keresztül, minimális plusz ráfordítást igényelne.

Raman és munkatársai (2024) megmutatják, hogy az LLM-alapú agensek azonos bemenetre különböző futtatások során eltérő parancssorokat generálhatnak, ami reprodukálhatatlan, esetenként destruktív mellékhatásokhoz vezethet egy éles rendszeren. Ez különösen kritikus, ha a rendszer „sudo" jogosultságokkal rendelkezik, mivel egy hibásan generált parancs szolgáltatás kiesést vagy adatvesztést okozhat.[8]

Hálózati forgalom elemzés tapasztalatai

A kiberbiztonság fontos szempont a mai világban. A hálózatot a modern technológiai eszközökkel védenünk kell, biztosítva a hálózat működését is. A nagy adatmennyiségeket BIG Data alapon dolgozzuk fel. A hálózati modell létrehozásához a Packet tracert alkalmaztuk amelyben az ügynökök viselkedését mutattuk be, kiemelve a hálózati sérülékenységet, és a védelmi lehetőségeket. A természetes nyelvi feldolgozást vettük alapul NLP amely az emberi megértést szolgálja, Az NLP feladata az volt hogy felismerje az írott szöveget, vagy hang alapon beszédfelismerés, fordítás során. A modell betanítása a feladatnak célirányosan kell. Az NLP működésének alapja matematikai műveletek, amelyek révén a gép képes értelmezni az információt. A nyelvi modellben szabályokat állítunk fel amelyre tekintve születik meg a döntés az MI által. Az agensek a neurális háló fontos résztvevői, amelyek alapján létrejön a döntés és az eredmény. A döntési ügynök határozza meg a kimenetet. Több ügynök dolgozhat a rendszerben amely alapján létrejön a kimenet és annak értéke. Az MI modell rendelkezik adott tudás halmazzal, ami előre be van tanítva. A hálózati sérülékenység esetében a gyengeségeket is előtérbe helyeztük.

A Hálózati támadások szimulációs modell alapján tárgyaltuk, beépítve a tűzfal szabályokat és a támadások elleni védekezés mértékét. AI agentek képesek lehetnek önállóan felderítési, sebezhetőség-azonosításban. A modellt tanítani kell a támadások felismeréséhez, és a védelmi veszély elhárításhoz. mérőszámokat alkalmaztam a hálózatban amelyre tekintve betekintést kaphatunk hálózatok védelmi hatékonyságára.[10]

Etikai vonatkozások

Az autonóm kiberbiztonsági ügynökök etikai megítélése a kutatási közösségben megosztott. Az ACM Code of Ethics (2018) értelmében a biztonsági kutatás csak explicit, informált hozzájárulással végezhető olyan rendszereken, amelyeket a kutató nem egyedül üzemeltet. [9]

A „dual-use" probléma, hogy az azonos eszköz és tudás egyszerre szolgál védelmi és támadói célokat, az autonóm ügynökök esetén különösen éles. Floridi és Cowls (2019) AI-etikai

keretrendszere alapján az ilyen rendszerek fejlesztői számára különös felelősség hárul az elővigyázatosság elvének betartására. Egy autonóm rendszer képes önállóan mérlegelni és végrehajtani hálózati műveleteket, akkor az emberi felügyelet csökkentése csak akkor igazolható etikailag, ha a rendszer lehetséges hatásköre előzetesen, explicit módon korlátozott és auditált.[10]

Összességében a kutatás azt mutatja, hogy az LLM-alapú sérülékenység kutató ügynökök valós, nem mesterségesen sérülékennyé tett hálózatokon is értékes felderítési eredményeket produkálnak, ugyanakkor az autonómia növelése, különösen az exploit-végrehajtás és a privilege escalation irányában, olyan kockázati küszöböt emel, amely technikai és etikai kontroll nélkül nem léphető át felelősen. Megerősíti ezt az, hogy az Antropic cég Mythos nevű legújabb LLM modelljének (2026) hasonló felhasználási tesztjei miatt korlátozott körben engedélyezte a tesztelést nagyobb cégeknek, tekintettel arra, hogy releváns rendszerekben több éve ott lévő addig ismeretlen sérülékenységeket is feltárt az autonóm ügynök, mely mögött az említett nagy nyelvi modell állt.

Alapvetően az offenzív vizsgálat is megerősíti azt, hogy egy rosszindulatú támadó összse tud építeni egy mesterséges intelligencia alapú sérülékenység felderítő és támadó eszközt, amelyet irányítani tud egyszerű szöveges parancsokkal a felderítés és támadásának végrehajtása érdekében. Ez a támadások egyre gyorsabb és kifinomultabb kivitelezéséhez vezet, melyet a mesterséges intelligencia irányít és hajt végre. A megállapított tények alapján kiemelten fontosak, hogy a védekező mechanizmusokat is ennek megfelelően készítsük fel a védekező munkára

FELHASZNÁLT IRODALOM

[1] Bottyán János, A nagy nyelvi modellek működése és képzése, valamint alkalmazásuk stratégiai elemzése BottyánSándor, https://real.mtak.hu/218677/1/06_bottyan_77-95_WEB-NSZ_2025_1.pdf

[2] https://www.tutorial.hu/ai/local-llm-otthoni-gepen-futtathato-nagy-nyelvi-modellek/

[3] Junjie Wang, Yuchao Huang, Chunyang Chen, Zhe Liu, Song Wang, Qing Wang. Software Testing with Large Language Models: Survey, Landscape, and Vision, 2024

[4] Horváth Imre, Számítógép hálózatok kiépítése Kommunikációs protokollol https://www.nive.hu/Downloads/Szakkepzesi_dokumentumok/Bemeneti_kompetenciak_meresi_ertekelesi_eszkozrendszerenek_kialakitasa/7_1173_031_101030.pdf

[5] http://elmfiz.elte.hu/fizinf/OpRendszerek/halozat.pdf

[6] Andrew S. Tanenbaum: Számítógép-hálózatok, Panem, 2004

[7] Xinyao Fang · Yifan Wu · Pengcheng He · et al., Large Language Models for Automated Vulnerability Discovery and Exploitation, USA: arXiv, 2024.

[8] Shashank Raman · Nicholas Carlini · Florian Tramèr · et al., Evaluating the Reliability of Large Language Models in Code Generation, USA: arXiv / Google DeepMind, 2024.

[9] Association for Computing Machinery, ACM Code of Ethics and Professional Conduct, New York: ACM Press, 2018.

[10] Luciano Floridi · Josh Cowls, A Unified Framework of Five Principles for AI in Society, Harvard Data Science Review, USA: Harvard University, 2019.

[11] Barna Bianka Rita, Kollár Csaba, Oroszi Eszter Diána A social engineering helye az információbiztonsági auditban BIZTONSÁGTUDOMÁNYI SZEMLE 5 : 1 pp. 25-41. , 17 p. (2023)

[12] Kollár Csaba, Jagodics Ibolya, 21. századi social engineering támadások, védekezés és szervezeti hatások Európában, DOI: 10.38146/BSZ.2023.1.6 pp 113-126 (2023)

DOI: https://doi.org/10.12700/btsz.2026.8.2.143

TRAINING OBJECTIVES AND QUALIFICATION LEVELS FOR OCCUPATIONAL SAFETY REPRESENTATIVES – A CASE STUDY

A MUNKAVÉDELMI KÉPVISELŐK KÉPZÉSI CÉLJAI ÉS KÉPZETTSÉGI SZINTJE – ESETTANULMÁNY

LEISZTNER Péter[1]

Abstract

Employee participation is essential to the effective functioning of occupational safety and health, with occupational safety representatives providing its institutionalized form. This study explores the knowledge and training levels Hungarian occupational safety and health professionals consider acceptable for these representatives, with particular emphasis on establishing a shared professional language. Using an intrinsic case study approach, the research involved ten highly qualified and experienced occupational safety professionals. Data were collected through semi-structured interviews and analyzed using qualitative content analysis. The findings indicate that intuitively defined expectations often exceed legal minimum requirements, while conscious consideration of competency levels tends to moderate them. These results highlight the importance of aligning training frameworks with both regulatory requirements and professional expectations, thereby supporting the further development of occupational safety education.

Keywords

workers' representative, occupational safety and health, training and educational objectives, Bloom's taxonomy, competency development

Absztrakt

A munkahelyi biztonság és egészségvédelem hatékony működésében meghatározó szerepet játszik a munkavállalók részvétele, amelynek intézményesített formáját a munkavédelmi képviselők jelentik. Jelen tanulmány azt vizsgálja, hogy a magyar munkavédelmi szakemberek milyen tudás- és képzési szintet tartanak elfogadhatónak a munkavédelmi képviselők esetében, különös tekintettel a közös szakmai nyelv kialakítására. A kutatás intrinsic esettanulmány módszertannal, tíz felsőfokú végzettséggel és jelentős szakmai tapasztalattal rendelkező munkavédelmi szakember bevonásával készült. Az adatgyűjtés félig strukturált interjúk segítségével történt, amelyeket kvalitatív tartalomelemzésnek vetettek alá. Az elemzés a kognitív és képzési szintek mentén értelmezte az elvárásokat. Az eredmények szerint az intuitívan megfogalmazott elvárások gyakran meghaladják a jogszabályi minimumokat, ugyanakkor a szintek tudatos értelmezése mérsékli azokat. A tanulmány következtetései a munkavédelmi képzési rendszer továbbfejlesztését támogathatják.

Kulcsszavak

munkavédelmi képviselő, munkahelyi biztonság és egészségvédelem, képzés és oktatási célok, Bloom-féle taxonómia, kompetenciafejlesztés

[1] leisztner.peter@uni-obuda.hu | 0000-0001-5302-5832 | PhD Student, Óbudai University Doctoral School for Safety and Security Sciences | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

The report of the British Committee on Safety and Health at Work, chaired by Lord Alfred Robens in 1972, highlighted that an overly detailed regulatory environment can paradoxically lead to apathy. Such regulation may encourage both employers and employees to regard occupational safety and health solely as a state responsibility, thereby marginalizing their own roles. The Committee's central recommendation was that the general responsibility for regulating occupational safety and health should be reinterpreted and exercised as a shared responsibility between employers and employees. This reasoning was based on the need to establish a more effective, self-regulating system [1].

A fundamental element of the practical implementation of self-regulation is the fulfilment of employers' information and consultation obligations [2], as well as the enforcement of regulations concerning the election, legal compliance, and training of workers' representatives in the field of occupational safety and health [3]. In parallel, the responsibility of the employee side includes nominating and electing representatives and initiating their training. Numerous empirical studies have demonstrated that the active involvement of employees and their representatives in occupational safety and health measurably contributes to a reduction in the number of workplace accidents [4].

Following the identification of the core and distinguishing competencies required for workers' representatives in the field of occupational safety and health [5], it becomes necessary to precisely define the objectives and levels of their training. However, competence does not merely refer to the possession of knowledge or the achievement of learning objectives, but also to the application of that knowledge in a given context at a defined performance level [6]. This case study focuses on examining this level of knowledge and performance.

A recurring theme in the research series is the status of workers' representatives within occupational safety and health systems. During professional consultations with Hungarian occupational safety and health professionals – regardless of their level of qualification – it was repeatedly noted that the role of workers' representatives in the field of occupational safety and health is difficult to integrate into the organizational structure of occupational safety and health systems. This phenomenon justifies an examination of what educational objectives and training levels occupational safety and health professionals consider appropriate for this group of employees. The case study methodology provides an opportunity for a deeper understanding of the phenomenon within a clearly defined research context [7].

The fulfilment of information and consultation obligations – consistent with employer expectations articulated in the Lisbon Treaty [2] – poses a significant challenge, as a fundamental prerequisite for implementation is the development of a common professional language, that is, effective professional communication [8], [9]. In the case of workers' representatives in the field of occupational safety and health, this task is particularly complex, as it requires the simultaneous application of the terminology of occupational safety and that of the specific workplace profession(s). Both occupational safety-related knowledge and employer-related professional knowledge form part of the core competencies [10], and their development can be achieved relatively effectively through appropriate educational methodologies [11].

Various educational taxonomies provide a theoretical framework for defining educational objectives and training levels, as well as for developing effective teaching methods [12]. Among these, Bloom's taxonomy and its revised versions are of particular importance, along with Webb's Depth of Knowledge taxonomy, the SOLO (Structure of Observed Learning Outcomes) taxonomy, and the taxonomies proposed by Fink and Shulman [12]. The purpose of these frameworks is to support the definition, achievement, and evaluation of educational objectives and learning outcomes. A fundamental expectation in the learning process is that participants acquire the basic elements of knowledge on which they can build in their later studies and practical activities [13].

The case study involved ten occupational safety and health professionals employed in Hungary under an employee employment relationship.

Workers' representatives in the field of occupational safety and health

The Treaty of Lisbon – which amends the Treaty on European Union and the Treaty establishing the European Community – addresses the issue of occupational safety and health in Article 153, placing particular emphasis on informing workers and consulting with them [2]. The European Union defines the role of workers' representatives in the field of occupational safety and health in several legal acts, including those related to collective redundancies [14], the transfer of undertakings or parts of undertakings [15], the establishment of Community-scale undertakings [16], and regulations concerning occupational safety and health [17].

These legal instruments consistently refer to these actors as "workers' representatives" in the field of occupational safety and health; however, different terms are used in the academic literature and in national legislation. For example, some publications of Eurofound refer to them as "employee representatives" [18], while in the Hungarian legal system the term "occupational safety and health representative" is commonly used [3].

According to the European Union directive aimed at introducing measures to improve the safety and health of workers, workers' representatives in the field of occupational safety and health are employees who are elected, designated, or appointed in accordance with national legislation or practice in order to represent workers' interests in matters of occupational safety and health [17].

Under Hungarian legislation, an occupational safety and health representative is an employee elected by the workforce who represents employees' rights and interests related to safe and healthy working conditions, in cooperation with the employer [3].

Any employee of the employer may be elected as a workers' representative in the field of occupational safety and health, ranging from workers performing activities that do not require formal qualifications to senior managers. Consequently, the completion of basic or secondary education (grades 1–12) is not a prerequisite for participation in their training.

Case study

The case study is one of the most widely used and accepted qualitative research methods in the social sciences [19]. Case studies can be classified into three main categories [20]:

- Instrumental case study, in which the researcher focuses on a specific issue or concern and selects a bounded case to illustrate it [21]. This approach is particularly

suitable when the investigation targets a single individual, group, or a well-defined phenomenon [22].

- Collective case study, which is based on the joint examination of multiple cases in order to explore a given problem or phenomenon [21]. The aim of this type of research is to identify common patterns, relationships, or similarities across cases [22]. This method is often applied when studying rare or difficult-to-observe phenomena.
- Intrinsic case study, in which the focus is on the case itself, with the aim of achieving an in-depth understanding of it [21]. This approach is especially suitable for the analysis of unique or rare phenomena, while preserving the analytical procedures characteristic of case study research [20].

In the present research, the intrinsic case study method was applied to explore and understand why workers' representatives in the field of occupational safety and health do not become a defining and indispensable actor within the occupational safety and health organization.

Bloom's taxonomy

In 1956, Benjamin Bloom and his colleagues – Max Englehart, Edward Furst, Walter Hill, and David Krathwohl – published their work Taxonomy of Educational Objectives, which presented a theoretical framework for the classification of educational objectives. The taxonomy developed by Bloom distinguishes six main categories: Knowledge, Comprehension, Application, Analysis, Synthesis, and Evaluation. The categories following the Knowledge level were defined as skills and abilities, emphasizing that knowledge is a prerequisite for the practical application of these skills and abilities [23].

According to Bloom's taxonomy, learning is a hierarchically structured process in which the individual levels build upon one another [13]. The interpretation of each category is as follows [24]:

- Knowledge: recall of facts and information;
- Comprehension: interpretation of the meaning of information and concepts;
- Application: use of acquired knowledge to solve problems or perform tasks;
- Analysis: breaking down information into its constituent parts in order to understand its structure;
- Synthesis: combining elements to create new structures or to solve complex problems;
- Evaluation: making judgments based on defined criteria and standards.

During the case study, Bloom's taxonomy was applied despite the fact that it has been subject to considerable criticism in the literature, primarily due to its emphasis on cognitive skills while giving less attention to the affective and psychomotor domains. Nevertheless, the taxonomy's wide acceptance and extensive use justify its application in educational research [13].

METHOD

The study applies the intrinsic case study method in order to gain an in-depth understanding of how workers' representatives in the field of occupational safety and health are positioned within their roles as defined by the Hungarian regulatory environment. The research focused on the system of relationships between occupational safety and health professionals and the representatives.

Relying on the cognitive levels of Bloom's taxonomy, the study sought to identify the training objectives of workers' representatives in the field of occupational safety and health, involving Hungarian professionals holding higher education qualifications in occupational safety and health.

Participant Selection

As the first step of the study, participants were selected. Sampling began with convenience sampling, as initially the professionals who were most easily accessible were chosen [25]. According to the original plan, additional participants were to be recruited using the snowball method, in which new participants would be identified from the acquaintances of the current study subjects [26]. However, this method proved unsuccessful, and the remainder of the sample was recruited by contacting easily accessible professionals.

The following channels were used to collect applications for participation:

- "Occupational Safety And Health Professionals" Facebook group (approx. 2,500 members; 2 applicants, 1 successfully recruited)
- Author's former classmates (approx. 25 individuals; 3 applicants, 2 successfully recruited)

Interviews and data collection

Semi-structured interviews [25] were conducted with ten occupational safety and health professionals, each holding a higher education degree and possessing over 10 years of professional experience. The gender distribution was balanced (5 women, 5 men). By economic sector: 6 participants were from manufacturing, 1 from trade and vehicle repair, 1 from public administration, defense, and compulsory social security, 1 from electricity, gas, steam supply and air conditioning, and 1 from professional, scientific, and technical activities.

All ten professionals were Hungarian citizens working in Hungary: 3 as specialists, 2 as middle managers, and 5 as executives. Their age groups were evenly distributed: 5 participants aged 26–45, and 5 aged 46–65. The represented employers had workforce sizes ranging from 20 to 13,000 employees.

The purpose of the interviews was to explore the professionals' subjective experiences [27]. A questionnaire with six questions was prepared in advance [28], based on the literature and preliminary data collection, with one question aligned with a parallel study [29]. Based on expert feedback, the questionnaire was revised, and a total of seven questions were finalized. The interviews were conducted in person or via online platforms (e.g., BBB, Microsoft Teams) by individual invitation [30], allowing for interactive participation and immediate responses to unanticipated topics [27].

Educational objectives and application of Bloom's taxonomy

The determination of the cognitive levels of Bloom's Taxonomy was conducted in two parts:

- Examination of occupational safety-related knowledge
- Establishing the required level of workplace- and employer-related knowledge

During the interviews, participants completed two interrelated tasks:

- In the first task, verbs corresponding to different cognitive levels were alphabetically arranged in a table, and each expert selected 20 verbs they considered most important for workers' representatives in the field of occupational safety and health
- In the second task, the cognitive levels and their explanations were placed on cards, and the experts had to select the knowledge level most characteristic for workers' representatives in the field of occupational safety and health

EQF-HuQF training levels

To determine the training levels, participants were asked to select the appropriate level using cards, taking into account skills, responsibility, and autonomy [23], [31].

The cards used for defining the training levels included the EQF-HuQF levels as defined by European Union and Hungarian regulations, along with the associated knowledge, skills, responsibility, and autonomy. Based on this information, the experts had to choose the level that, in their opinion, best reflected the knowledge and skills expected of an worker's representative in the field of occupational safety and health, as well as the responsibility and independence required for the role.

Data Processing

The notes taken during the interviews were subjected to qualitative content analysis, also known as thematic analysis [32], with the aim of identifying the training objectives and levels expected by the experts. The results were subsequently compiled in Excel spreadsheets for further analysis.

RESULTS

During the semi-structured interviews conducted with occupational safety and health professionals holding higher-education qualifications, participants were first asked to select 20 verbs that, in their opinion, characterize the required level of occupational safety-related knowledge of workers' representatives in the field of occupational safety and health. They were also asked to select another 20 verbs that they believed characterize the required level of professional and workplace-related knowledge of workers' representatives in the field of occupational safety and health. During the selection process, participants were allowed to choose freely from the complete list of verbs for both categories.

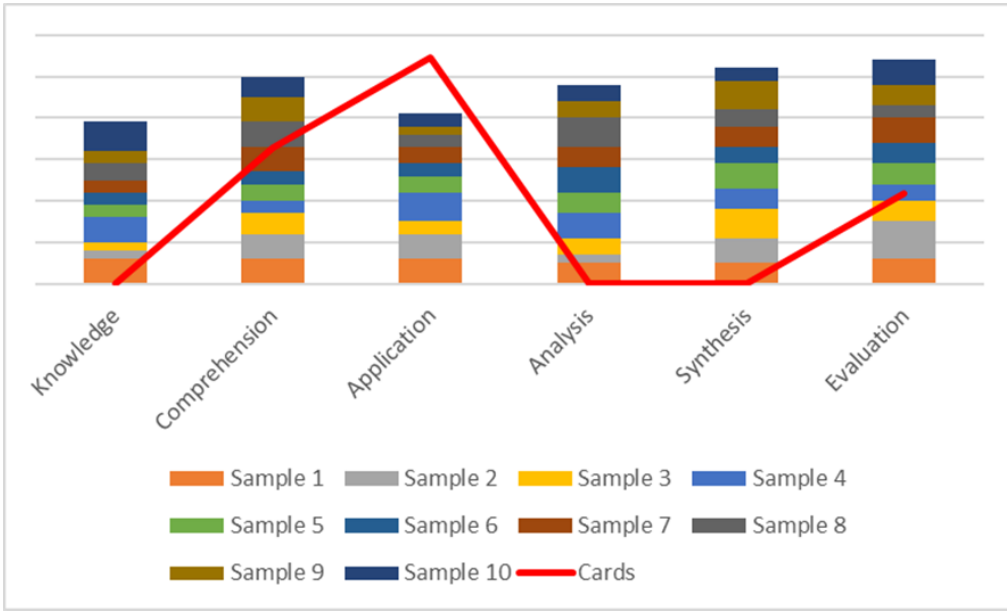


Figure 1. The required level of occupational safety and health knowledge of workers' representatives in the field of occupational safety and health according to Bloom's taxonomy, by respondent, based on the selected verbs and cards

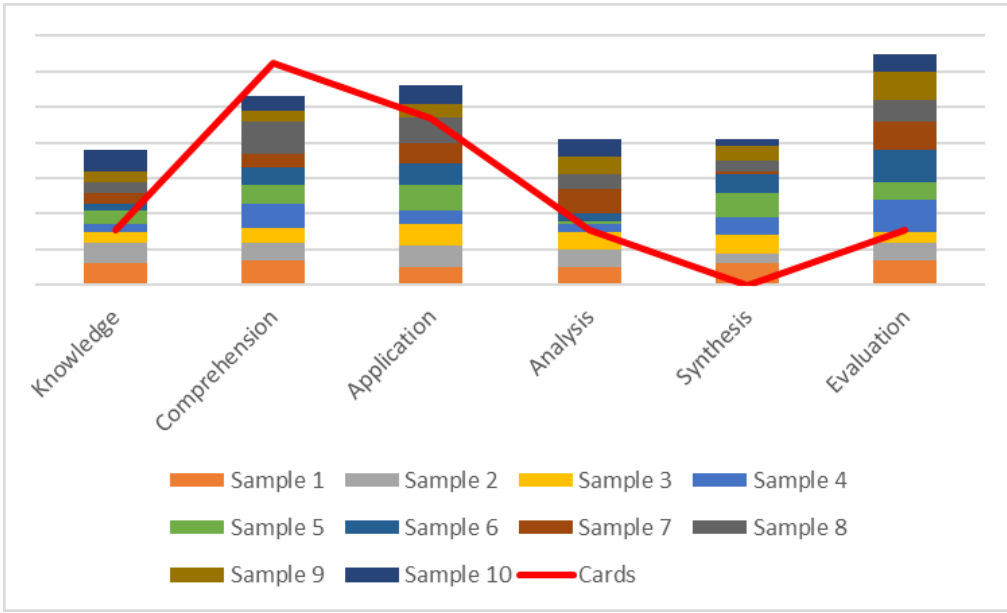


Figure 2. The required level of job-related professional and workplace knowledge of workers' representatives in the field of occupational safety and health according to Bloom's taxonomy, by respondent, based on the selected verbs and cards

When determining the level of both occupational safety-related knowledge and professional and workplace-related knowledge, a significant discrepancy was observed depending on whether the experts were asked to select verbs associated with knowledge levels unfamiliar to them, or to choose cards that included interpretive descriptions of the individual levels. In both cases, it can be established that when selecting verbs, the highest knowledge level was identified as the required level; however, when the interpretations of the levels were taken into account, the experts selected the "application" level for occupational safety-related knowledge and the "understanding" level for professional and workplace-related knowledge. The results of the card-based selection for occupational safety-related knowledge are consistent with statutory requirements, while in the case of professional and workplace-related knowledge they correspond to the minimum level necessary for the use of a common professional language.

During the determination of the EQF–HuQF level, among the experts involved in the study, two selected Level 2 (lower secondary partial qualifications, partial occupations, workshop school programme qualifications), four selected Level 3 (lower secondary partial qualifications, vocational qualifications, vocational qualification add-ons, partial occupations), two selected Level 4 (upper secondary vocational qualifications, vocational qualification add-ons, full vocational occupations), one selected Level 5 (higher-level vocational education, short-cycle higher education), and one selected Level 6 (Bachelor's degree (BA), higher-level vocational education).

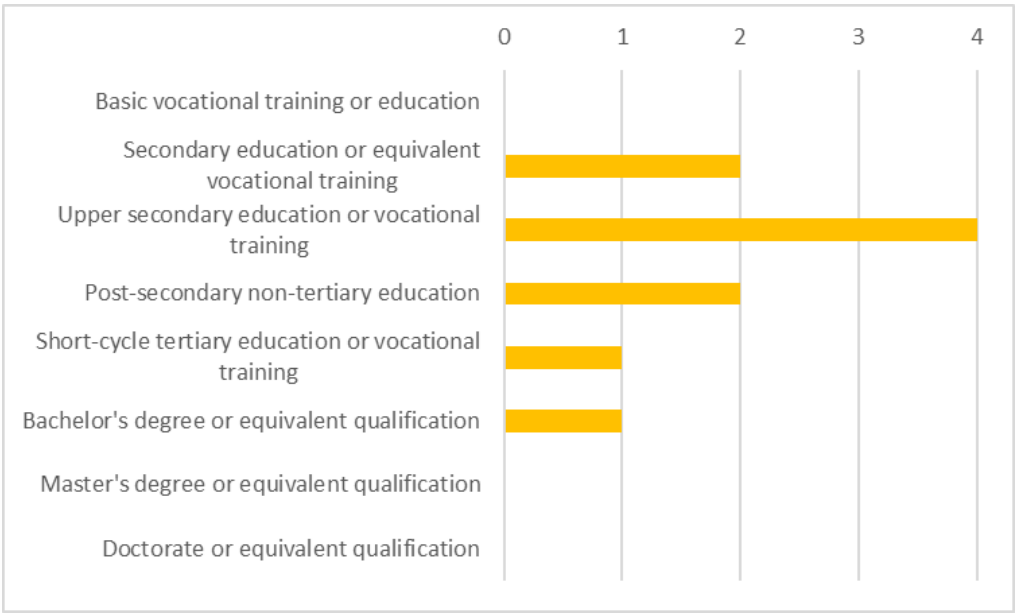


Figure 3. The required qualification level of worker's representatives in the field of occupational safety and health according to the EQF–HuQF levels, based on the selected cards

During the interviews, the implementation of information provision and consultation, as well as the involvement of workers' representatives in occupational safety and health–related communication at the employers represented by the experts, was assessed through a separate, dedicated question.

- Monthly occupational safety and health training sessions
- On a daily basis through middle managers (production managers, supervisors, shift leaders)
- Management walkthroughs twice a week
- Communication via a chat application with key-position employees who have company mobile phones (approximately 60–70% of the workforce)
- Training every Monday, with a review of current issues
- Notice board
- Monthly meetings with worker's representatives in the field of occupational safety and health
- Training sessions held twice a year
- Monthly "all-hands meeting"
- Online channel – Slack Safety
- Anonymous channel – poster with QR code
- Work accident reporting platform
- Shared mailbox / group email addresses
- Representative-based system – professional liaison
- Face-to-face communication
- Daily morning briefing
- Personal communication
- e-mail
- Notice
- In writing
- Not really
- Works Council
- Through worker's representatives in the field of occupational safety and health
- HSE notice board
- Monthly HSE update

Based on the identified communication channels, only two employers were found where occupational safety and health professionals implement information provision and consultation through workers' representatives in the field of occupational safety and health, even if only partially.

DISCUSSION

The definition of educational objectives means clearly specifying what outcomes the education aims to achieve, that is, which knowledge, skills, and attitudes should be conveyed to the participants of the training. These expected outcomes guide the teaching–learning process and can only be considered fulfilled if the participants have actually acquired them [33].

In the training of workers' representatives in the field of occupational safety and health, a key objective is the development of a common language with employees and with the occupational safety and health professional(s). This shared professional language represents a so-called "semi-foreign language" for participants in education [8]. In the case of

participants attending the 16-hour basic training for workers' representatives in the field of occupational safety and health [34], this includes the acquisition of occupational safety-related knowledge, but it may also apply to familiarization with workplace-related professional and workplace-specific knowledge for individuals who are not familiar with all professions, activities, or technologies present at a given employer. It can therefore be stated that professional language is field-specific and specialized; it is distinguished from other professional languages and from general language by its connection to the specific knowledge, methods, tasks, and approaches of each discipline [9].

In line with previous research, the present study also confirmed that professionals would prefer to see occupational safety and health representatives with at least upper secondary education within the occupational safety and health organizations they lead or in which they participate. During the examination of Bloom's taxonomy, all professionals selected verbs from the highest cognitive level, and overall, the largest number of verbs was selected from this level in both knowledge domains examined in the study. At the same time, when the professionals became familiar with the interpretations associated with each level, expectations remained higher than the skill levels defined by European Union and Hungarian legislators, even in this case.

In the determination of the EQF–HuQR level, the aspirations of the research participants became even more apparent, as four respondents expected at least upper secondary education and two expected tertiary education in the training of workers' representatives in the field of occupational safety and health.

The case study demonstrated that, in the opinion of occupational safety and health professionals, workers' representatives do not currently constitute partners for them within occupational safety and health organizations under the existing training system, and they are not relied upon in the development of safe and healthy workplaces.

An interesting result emerged from the examination of occupational safety and health communication channels identified at the employers represented by the participating professionals, as communication through workers' representatives in the field of occupational safety and health was mentioned in only two cases.

An effectively functioning workers' representative in the field of occupational safety and health, who speaks a common language with occupational safety and health professionals, employers, and employees, represents the first step in developing the level of an employer's safety culture [35], in the implementation of the European Union's "zero" vision [35], and in increasing sustainable safety [36].

CONCLUSIONS

According to the components of knowledge as a fundamental competence, occupational safety and health representatives must be trained at an appropriate level in order to acquire the confident use of professional language. The aim of education is for them to master a common language, thereby becoming useful members of the employer's occupational safety and health organization.

The definition of knowledge-related educational objectives falls to two actors within the tripartite system. State responsibilities and training objectives have already been defined at the legislative level; however, employers themselves must develop training objectives and tasks related to workplace-specific, professional, and workplace-related

knowledge. The third participant in the tripartite system—employees and their representatives—can encourage such workplace training and make proposals regarding the definition of educational objectives. Through the National Occupational Safety and Health Committee, employers and employees and their representatives may also communicate their needs and proposals related to occupational safety and health knowledge to the state.

The research highlighted that greater emphasis should also be placed, during the training of occupational safety and health professionals, on issues related to the activities of worker's representatives in the field occupational safety and health.

At the employers represented by the occupational safety and health professionals involved in the study, the relatively low number of elected occupational safety and health representatives compared to the number of employees suggests that both employers and employees need to be more clearly informed about their rights related to the election of occupational safety and health representatives, and especially about the benefits arising from this process.

A defining characteristic of an effective workers' representative in the field of occupational safety and health is the ability to actively participate in occupational safety and health communication, to accurately convey employer-provided information, to take part in employee consultations, and to speak a common professional language even with individuals holding occupational safety and health professional qualifications.

REFERENCES

[1] C. Sirrs, "Accidents and Apathy: The Construction of the 'Robens Philosophy' of Occupational Safety and Health Regulation in Britain, 1961-1974," Feb. 01, 2016, *Oxford University Press*. doi: 10.1093/shm/hkv068.

[2] Az Európai Unió Hivatalos Lapja, "Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata," *Az Európai Unió Hivatalos Lapja*, vol. 55, pp. 0001–0390, 2012, [Online]. Available: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A12012E%2FTXT

[3] *1993. évi XCIII. törvény a munkavédelemről*, no. 10. 2024, pp. 1–55.

[4] D. Walters, M. Quinlan, R. Johnstone, and E. Wadsworth, "Cooperation or resistance? Representing workers' health and safety in a hazardous industry," *Industrial Relations Journal*, vol. 47, no. 4, pp. 379–395, Jul. 2016, doi: 10.1111/irj.12147.

[5] P. Leisztner, F. Faragó, and G. Szabó, "The Identification of the Competency Components Necessary for the Tasks of Workers ' Representatives in the Field of OSH to Support Their Selection and Development , as Well as to Assess Their Effectiveness," *Safety*, vol. 11, no. 3, pp. 1–14, 2025.

[6] M. el asame and M. Wakrim, "Towards a competency model: A review of the literature and the competency standards," *Educ. Inf. Technol. (Dordr).*, vol. 23, pp. 1–12, Jan. 2018, doi: 10.1007/s10639-017-9596-z.

[7] S. Crowe, K. Cresswell, A. Robertson, G. Huby, A. Avery, and A. Sheikh, "The case study approach," *BMC Med. Res. Methodol.*, vol. 11, 2011, doi: 10.1186/1471-2288-11-100.

[8] Z. Sturcz, "Szakmai anyanyelv, szakképzés a közoktatásban, nyelvpedagógiai összefüggések," Eszterhazy Karoly Egyetem, 2020, pp. 379–392. doi: 10.17048/pelikon2018.2020.379.

[9] E. Csányi, "A szaknyelvek jellemzői," in *Szemelvények a BGE kutatásaiból (II. kötet)*, Budapesti Gazdasági Egyetem, 2023, pp. 53–58. doi: 10.29180/978-615-6342-76-8_6.
[10] L. M. Spencer, D. C. McClelland, and S. M. Spencer, *Competency Assessment Methods: History and State of the Art*. Hay/McBer Research, 1998. [Online]. Available: https://books.google.hu/books?id=YgN9tAEACAAJ
[11] S. A. Tucker and K. M. Cofsky, "Competency-based pay on a banding platform: A compensation combination for driving performance and managing change," *ACA Journal*, vol. 3, no. 1, p. 30, 1994, [Online]. Available: https://www.proquest.com/scholarly-journals/competency-based-pay-on-banding-platform/docview/216362458/se-2?accountid=134728
[12] J. Irvine, "Taxonomies in Education: Overview, Comparison, and Future Directions," *Journal of Education and Development*, vol. 5, no. 2, p. 1, May 2021, doi: 10.20849/jed.v5i2.898.
[13] M. A. AlAfnan, "Taxonomy of Educational Objectives: Teaching, Learning, and Assessing in the Information and Artificial Intelligence Era," *Journal of Curriculum and Teaching*, vol. 13, no. 4, pp. 173–191, Aug. 2024, doi: 10.5430/jct.v13n4p173.
[14] "Directive 98/59/EC on the approximation of the laws of the Member States relating to collective redundancies," *International and European Labour Law*, vol. 84, no. July 1998, pp. 981–996, 2018, doi: 10.5771/9783845266190-997.
[15] "Directive 2001/23 on the Approximation of the Laws of the Member States Relating to the Safeguarding of Employees Rights in the Event of Transfers of Undertakings, Businesses or Parts of Undertakings or Businesses," *Official Journal of the European Communities*, vol. 2000, no. October 2000, pp. 639–645, 2018, doi: 10.1017/9781108624374.025.
[16] "Directive 2009/38/EC - Works Council," *Official Journal of the European Union*, no. 9, pp. 28–44, 2009.
[17] "Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work Edoardo Ales," *International and European Labour Law*, vol. 42, no. June 1989, pp. 1210–1242, 2018, doi: 10.5771/9783845266190-1226.
[18] Christine Aumayr-Pintar, "Industrial relations Employee representation at establishment or company level : A mapping report ahead of the 4th European Company Survey," 2019, [Online]. Available: https://www.eurofound.europa.eu/en/publications/eurofound-paper/2020/employee-representation-establishment-or-company-level-mapping
[19] L. Bloomberg and M. Volpe, *Completing Your Qualitative Dissertation: A Roadmap from Beginning to End*. Thousand Oaks, California: SAGE Publications, Inc., 2008. doi: 10.4135/9781452226613.
[20] Hayden Coombs, *Case Study Research Defined [White paper]*. 2022, p. 1. Accessed: Sep. 29, 2025. [Online]. Available: https://doi.org/10.5281/zenodo.7604301.
[21] J. W. Creswell and C. N. Poth, *Qualitative inquiry and research design: Choosing among five approaches.*
[22] R. K. Yin, *Case study research and applications : design and methods*, Sixth edition. Thousand Oaks: SAGE Publications, Incorporated, 2018.

[23] "IACBE Advancing Academic Quality in Business Education Worldwide," Lenexa, 2014.
[24] J. Ajayi, "Blooms taxonomy." [Online]. Available: https://www.researchgate.net/publication/380814622
[25] Hunkár Márta, *A kutatás módszertana*. Debrecen, 2013. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=223 (2022.10.22)
[26] M. Naderifar, H. Goli, and F. Ghaljaie, "Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research," *Strides in Development of Medical Education*, vol. 14, no. 3, Sep. 2017, doi: 10.5812/sdme.67670.
[27] H. Jansen, "3 Systematiek en toepassing van de kwalitatieve survey BT - Kwalitatief onderzoek: Praktische methoden voor de medische praktijk," P. L. B. J. Lucassen and T. C. olde Hartman, Eds., Houten: Bohn Stafleu van Loghum, 2007, pp. 27–41. doi: 10.1007/978-90-313-6373-5_3.
[28] L. M. Spencer and P. S. M. Spencer, *Competence at Work Models for Superior Performance*. Wiley India Pvt. Limited, 2008. [Online]. Available: https://books.google.hu/books?id=2Y8QB-6aIJMC
[29] L. Busetto, W. Wick, and C. Gumbinger, "How to use and assess qualitative research methods," *Neurol. Res. Pract.*, vol. 2, no. 1, p. 14, 2020, doi: 10.1186/s42466-020-00059-z.
[30] P. Leisztner, "A munkavédelmi képviselők szerepe a munkavédelmi feladatok ellátásában," *Biztonságtudományi Szemle*, vol. 5, no. 2, pp. 137–147, 2023.
[31] *A TANÁCS AJÁNLÁSA az egész életen át tartó tanulás európai képesítési keretrendszeréről, valamint az egész életen át tartó tanulás európai képesítési keretrendszerének létrehozásáról szóló 2008. április 23-i európai parlamenti és tanácsi ajánlás hatályon kívül helyezéséről*. 2017.
[32] U. Kuckartz, "Qualitative Text Analysis: A Systematic Approach," 2019, pp. 181–197. doi: 10.1007/978-3-030-15636-7_8.
[33] O. A. Adilov, "Methodological and pedagogical issues in defining educational goals in the management of general secondary schools," 2019.
[34] *A munkavédelmi képviselő alapképzés és továbbképzés képzési követelményei*. 2024, pp. 1–9.
[35] D. Parker, M. Lawrie, and P. Hudson, "A framework for understanding the development of organisational safety culture," *Saf. Sci.*, vol. 44, pp. 551–562, Jul. 2006, doi: 10.1016/j.ssci.2005.10.004.
[36] "EU strategic framework on health and safety at work 2021-2027 Occupational safety and health in a changing world of work," pp. 1–21, 2021, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0323
[37] H. Xu, Q. Mei, S. Liu, J. Zhang, and M. A. S. Khan, "Understand, track and develop enterprise workplace safety, and sustainability in the industrial park," *Heliyon*, vol. 9, p. e16717, May 2023, doi: 10.1016/j.heliyon.2023.e16717.

DOI: https://doi.org/10.12700/btsz.2026.8.2.157

FIRESAFETY IN DATA CENTRES – CURRENT CHALLENGES

ADATKÖZPONTOK TŰZVÉDELMI KÉRDÉSEI – AKTUÁLIS PROBLÉMÁK

SOMOGYI Tamás[1] – NAGY Rudolf[2]

Abstract

The availability of IT services is getting more and more important in the era of digitalisation, especially in case of essential services. Obviously, IT services are provided by servers concentrating in data centres. Moreover, some of the data centres considered part of the critical infrastructure, therefore their security and fire safety is uttermost. Due to their specialities, data centres require special solutions even in the field of fire safety; however, very few studies focused on this topic. The goal of this study is to describe the specialities of data centres' fire safety and explore recent research results to have a better understanding of this important topic.

Keywords

fire, fire safety, data centre

Absztrakt

Digitalizálódó világunkban az elektronikus szolgáltatások rendelkezésre állásának kérdése egyre nagyobb szerepet kap, különösen a társadalom szempontjából alapvetőnek tekinthető szolgáltatások esetében. Minden IT szolgáltatás mögött szükségszerűen megtalálhatóak az IT eszközök, melyek adatközpontokban koncentrálódnak. Az adatközpontok gyakran kritikus infrastruktúra részét képezik, így biztonságuk kérdésköre kiemelt jelentőségű, mely terület része a tűzvédelem is. Az adatközpontok speciális felépítéséből, berendezéséből és használatából fakadóan a tűzvédelem terén egyedi kérdések is felmerülnek, melyek kutatására és tudományos tárgyalására eddig csekély figyelem irányult. Kutatásunk célja feltárni az adatközpontok tűzvédelmi specialitásait, valamint a nemzetközi szakirodalom kutatási irányaiból és eredményeiből leszűrhető következtetések levonása a téma mélyebb megértése érdekében.

Kulcsszavak

tűz, tűzvédelem, adatközpont

[1] somogyit588@gmail.com | ORCID: 0000-0003-1397-697X | PhD student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] nagy.rudolf@uni-obuda.hu | ORCID: 0000-0001-5108-9728 | habil. associate professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary | habil. docens, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az elmúlt három évtizedben látható digitalizáció jelentősen gyorsítja a gazdaság szerkezetének átalakulását, továbbá országonként és fejlettségi szintenként eltérő módon ugyan, de pozitív hatással bír a termelékenységre [1]. Ez a digitalizáció és IT szolgáltatások vezette fejlődés az utóbbi években gyorsulni látszik az egész világon, így Közép-Európában is [2]. Az ipari tevékenység digitalizációjával [3] és a rutinfeladatok tekintetében a robotizációval [4] párhuzamosan átalakulnak a társadalmi szokások és elvárások, gondoljunk csak az internetes vásárlásra [5], és az elektronikus bankolásra [6]. A közigazgatási szervek mind jobban terjedő elektronikus szolgáltatásokat nyújtanak az állampolgároknak [7], az oktatásban teret nyer a digitális oktatás [8]. Mindezek mellett tény, hogy napjainkban egyre szélesebb körűvé válik a mesterséges intelligencia (MI) megjelenése és alkalmazása, ebből fakadóan kutatások sora foglalkozik az MI felhasználási lehetőségeivel [9], [10], [11] valamint a digitalizáció előidézte biztonsági kihívások kérdéskörével [12], [13], [14].

Az üzleti világ és a magánélet szokásait tekintve kijelenthető, hogy azokat napjainkban a digitalizáció és információtechnológia határozza meg, illetve alakítja át. A JP Morgan felmérése szerint 2026-ban a vállalatok többsége mesterséges intelligencia bevezetését tervezi, 62%-uk folyamatautomatizálás, 44%-uk elemzés, 42%-uk pedig piaci előrejelzés területen [15]. A Chase felmérése is ezt erősíti meg, mely eredménye szerint 2025-ben az MI felhasználása felgyorsult, és ez várható 2026-ban is [16]. A Forbes magazin egyik vonatkozó cikke is az MI térnyerését vetíti előre 2026-ra az üzleti életben, mely egyrészről egyes üzleti folyamatok automatizálását, másfelől MI alapú szolgáltatások nyújtását jelenti [17]. A digitalizáció és a technológia, azon belül is az MI növekvő használata szükségszerűen növekvő mértékben igényli ezen szolgáltatások mögötti IT eszközök üzemeltetését és rendelkezésre állását, hiszen ezek kiesése fennakadást idézhet elő az üzletmenetben, a vállalatok napi működésében [18], termeléskieséshez és pénzügyi veszteséghez is vezethet [19].

A 2026. év eleji iparági hírek és események az adatközponti infrastruktúra világából mindezt alátámasztják. A Digital Edge bejelentette, hogy az indonéziai Bekasi-ban 4,5 milliárd USD befektetéssel megépíti Indonézia egyik legnagyobb adatközpontját [20]. Az Oracle 50 milliárd USD -t tervez költeni 2026-ban MI-t támogató infrastruktúrára [21]. 2026. februári európai hír, hogy Franciaországban Bordeaux-ban épül új adatközpont 3,59 milliárd USD költséggel [22]. A Moody's becslése szerint 2026-2030 között a világon legalább 3 trillió USD-t fordítanak adatközponti infrastruktúra projektekre [23].

Az adatközpontok gyors terjedése még jobban előtérbe helyezi a létesítményi biztonság [24] és a kritikus infrastruktúrák védelmének kérdéskörét [25], [26], [27], [28], [29] valamint azon belül a tűzvédelem különböző aspektusait [30], [31], [32], [33]. Minthogy az adatközpontokban üzemelő, elektronikus szolgáltatásokat nyújtó és a digitalizált adatot tároló IT eszközök védelme és rendelkezésre állása kiemelt jelentőségűvé válik, természetes módon jelenik meg a magas szintű tűzvédelem követelménye ezen speciális létesítményekben, illetve merül fel a tűzvédelem fokozásának igénye.

Kutatási célok és módszerek

A kutatás célja iparági hírek és nyilvánosságra került megtörtént esetek, valamint témabeli tudományos publikációk feldolgozásával egyfelől az adatközpontok tűzvédelmi specialitásainak bemutatása, másfelől a védekezés terén az aktuális kutatási irányokból és

eredményekből leszűrhető következtetések levonása a téma mélyebb megértésének érdekében.

A kvalitatív módszerű, az aktuális kutatási irányok és eredmények felderítését célzó szakirodalmi kutatás a nemzetközi tudományos publikációk egyik kiemelt adatbázisának áttekintésével történt az alábbiak szerint.

- adatbázis: www.sciencedirect.com/
- keresés dátuma: 2026. március 20.
- keresési feltételek:
  - Title, abstract, keywords: „data centre fire“ (ugyanaz az eredmény született „data center“ keresőszóval is, tehát a brit és az amerikai angol alapján keresve nincs különbség)
  - típus: „Research articles“
- eredmény: 24 cikk, melyből 7 cikk releváns, a többi nem tűzvédelemhez kapcsolódik (például tűzfal kérdéskörével foglalkozó)

Az iparági hírek forrása a www.datacenterknowledge.com portál volt, kiegészítve nemzetközi gazdasági elemzőcégek jelentéseivel és hírportálokon megjelenő hírekkel.

ADATKÖZPONTI TŰZESETEK

Az iparági történésekről hírt adó Data Center Knowledge portál több tűzesetet is összegyűjtött [34]. Az amerikai Iowa államban a Google egyik legrégebbi és legnagyobb adatközpontjában tört ki tűz 2022-ben elektromos kisülés következtében, mely eredményeként három ember megsérült és IT szolgáltatásokban kiesés volt tapasztalható. 2021-ben Strassbourgban az OVH adatközpont egyik szerverterme égett le, napokra IT szolgáltatás nélkül hagyva a francia felhőszolgáltató kb. 65 ezer ügyfelét. A texasi AT&T telekommunikációs cég adatközpontjában történt 2018-as tűzeset egy elektromos kapcsoló hibájából, 12 órára internet- és telefonelérés nélkül hagyva ügyfeleit.

2024-ben Szingapúrban egy adatközpont Li-ion akkumulátorainál keletkezett tűzzel a katasztrófavédelem több, mint egy napig küzdött, a tűz okozta kiesést az IT szolgáltatásokban pedig több ázsiai nagyvállalat és vásárlói érezték meg, köztük az Alibaba ügyfelei is [35]. Egy dél-koreai kormányzati adatközpontban az egyik Li-ion akkumulátor csere közben felrobbant és gyorsan terjedő tüzet idézett elő [36]. A tűzeset következménye a kormányzati elektronikus szolgáltatásokban történő fennakadás mellett 125,000 köztisztviselő adatának és nyolc év kormányzati munkadokumentumnak az elvesztése.

Fenti néhány esetből látható, hogy még a kiemelt szerepük miatt különösen védettnek gondolt, és általában elzártan üzemeltetett adatközpontokban is előfordulnak tűzesetek, amiből következik az adatközponti tűzvédelem létjogosultsága és fejlesztési lehetőségei kutatásának a jelentősége.

ADATKÖZPONTOK SAJÁTOSSÁGAI A TŰZVÉDELEM SZEMPONTJÁBÓL

Az épületüzemeltetés és vagyonvédelem kérdésköre mellett kiemelt jelentőségű az adatközpontok biztonságának terén a tűzvédelem témája. Általánosságban elmondható, hogy a tűz az emberi életet is veszélyezteti, mely nyilvánvalóan a legsúlyosabb veszteség, ezen felül pedig anyagi kárt is okozhat. Adatközpontok esetében azonban további vesztesé-

gek is előfordulhatnak, hiszen egy tűz következménye lehet informatikai szolgáltatások kiesése, valamint adatvesztés. Ezért a magas szintű tűzvédelem jogos érdeke az üzemeltetőnek, illetve bérlőknek, továbbá jogos elvárása az IT szolgáltatásokat élvezőknek, végső soron az egész társadalomnak. Kiemelt jelentőséggel bír tehát az adatközponti tűzvédelem kérdésköre, melynél elengedhetetlen figyelembe venni az adatközpontok speciális jellegét.

Az adatközpontok specialitásaként kell említeni az egy helyen koncentrálódó IT eszközök magas számát: a szervereket és kommunikációs hálózati elemeket, valamint további eszközöket. Lényeges, hogy az IT eszközök működésük során hőt termelnek, mely hő elvezetése esszenciális, hiszen ezen eszközök a gyártók ajánlását alapul vevő iparági gyakorlat szerint 18 - 20 Celsius fok között üzemeltethetőek optimálisan [37], tehát az élettartamuk és megfelelő működésük érdekében az állandó hőmérséklet biztosítása kulcskérdés. Lényeges továbbá a páratartalom és a levegő pormentessége is. Ebből fakadóan az adatközpontban az épületüzemeltetési rendszer eszközeivel is számolni szükséges. Ezen felül figyelembe kell venni az IT eszközök képviselte értéket, mely kettő részből tevődik összse: a szerverek, hálózati eszközök értékes vagyonelemek, valamint a tárolt adatok is értéket képviselnek. Következésképpen az adatközpontokban jelen vannak vagyonvédelmi eszközök is a magas szintű létesítményi biztonság érdekében [38]. Ezen a ponton érdemes megemlíteni azon speciális védelmi eszközöket, melyek az IT eszközöket védelmezik a távolról való illetéktelen hozzáférés-, vagy az azok feletti irányítás megszerzése ellen [39]. Érthető tehát az egy helyen koncentrálódó, eltérő célú IT eszközök magas száma. Sándor és Nagy szerint egy adatközpont tűzkockázatát meghatározó tényező a szervertermek telítettsége a hőtermeléséből fakadóan, ugyanis az el nem vezetett hő okozta túlmelegedés növeli az elektromos tűzesetek bekövetkezési valószínűségét [40].

Az IT eszközök száma és az áramellátás biztosítása miatt az adatközpontokban a kábelek nagy mértékű jelenlétét is említeni kell. Az elektromos kábelek túlterhelés hatására felmelegednek, mely jelenség tüzet is képes okozni [41]. Már a gyulladási hőmérséklet alatt is képes károsodni a vezeték műanyag burkolata, és olyan folyamat kezdődik, mely során éghető gáz szabadul fel, fokozva a tűz kockázatát.

A túlmelegedés mellett tűzesetet indukálhat akkumulátor-probléma is. A folyamatos rendelkezésre állás érdekében az IT eszközök folyamatos áramellátását biztosítani szükséges, így alapvető feladat az akkumulátorok telepítése, szünetmentes tápellátási megoldás kiépítése. Az akkumulátorok tűzveszélyességére azonban már több eset is felhívta a figyelmet (pl. [42] és [43]).

Az adatközponti tűzvédelem tervezésekor figyelembe kell venni az IT eszközök magas számát. Mivel a vízzel oltó rendszerek (sprinkler) és a habbal oltó rendszerek az IT eszközöket károsíthatják, olyan alternatív megoldásokat kell alkalmazni, melyek a hűtés, illetve az oxigén kiszorítása során nem károsítják ezen IT eszközöket. Figyelembe kell venni ugyanis, hogy a fentebb említettek szerint az IT eszközök saját értékén túl a tárolt adatok is jelentőséggel bírnak, így összességében nagyon magas a védendő IT eszközök értéke.

Az adatközpontok további sajátosságának mondható, hogy egyes részeiben nem tartózkodik személyzet állandóan, csak alkalmi jelleggel, például karbantartás vagy eszközcsere idejére. Fizikailag és logikailag is elkülönülnek tehát a munkavállalók irodahelyiségei, a vezérlőtermek, és az IT eszközök üzemelési helyiségei, valamint az áramellátást biztosító

eszközök üzemelési helyiségei. Tűz kockázatának szempontjából is különböznek ezen helyiségek, így a tűzvédelem szempontjából is eltérések lehetnek, például irodahelyiségbe telepíthető vízzel oltó tűzoltó eszköz is, míg szerverteremben ezt a megoldást kerülni javasolt.

ADATKÖZPONTOK TŰZVÉDELMÉNEK KUTATÁSA A NEMZETKÖZI TUDOMÁNYOS SZAKIRODALOM ALAPJÁN

A kutatási célok és módszerek részben leírt szakirodalom-kutatás során feldolgozott tudományos cikkek eredményei az alábbiak szerint foglalhatóak össze.

Badhe és szerzőtársai 2025-ben közzétett tanulmányukban az adatközpontokban termelődő hő- és az IT eszközök működésük közbeni melegedésének a problémájára magukban az elektronikai eszközökben kerestek választ [44]. Olyan konstrukciós megoldást javasolnak, mely során LTCC kerámialapot integrálnak heterogén architektúrájú csipekre a termikus érintkezés kiküszöbölése érdekében, mellyel a hűtés hatékonysága növelhető. Prototípussal végzett kísérletükben kevesebb hűtő levegőre volt szükség, mint a hasonló teljesítményű Intel alátétlemez esetén.

Kim 2026-os cikkében olyan fűtési-, szellőztetési- és hűtési rendszert javasolt [45], amellyel moduláris, automatizációval integrált (emberi beavatkozás nélkül működtethető) füstmentesítő rendszer alakítható ki irányítóhelyiségekben. A már üzemelő tűzvédelmi rendszerek mellé gyorsan telepíthető megoldása belélegezhető levegőt biztosít a padlószinthez közel, ami az emberélet megóvását szolgálja.

Kareck és szerzőtársai 2026-os tanulmányukban az adatközponti tűzvédelem fokozására a megfelelő kockázatértékelést javasolják [46]. Módszertanukban figyelembe veszik a lehetséges kiváltó okokat, mint a túlfeszültség, az akkumulátor-probléma, a túlmelegedés és emberi hiba. Abból kiindulva, hogy mind a tűzvédelmi eszközök, mind az IT eszközök folyamatosan fejlődnek, a megtörtént tűzesetekből levont tanulságok felhasználása fontos eleme módszertanuknak.

Liang szerzőtársaival 2025-ben megjelentetett cikkükben az adatközpontokban is alkalmazott kábelek FR-PE (tűzgátló polimer) szigetelőanyagának tulajdonságaiban túláram hatására bekövetkező változásokat vizsgálták [47]. Túláram hatására a vezetőanyag melegedéséből fakadóan melegszik a szigetelő anyag is. Ez a hőmérséklet-emelkedés indukálhatja a szigetelőanyag polimerláncainak hasadását, a keresztkötött polimerek depolimerizációját és gyúlékony gázok keletkezését. A tanulmány szerzői szerint ezen folyamat mélyebb megértése az adatközpontok tűzvédelmének fokozását segítheti elő a tűz kockázatának pontosabb értékelése által.

Newman és szerzőtársai 2013-as publikációjukban adatközpontokban füstkár következményeként azonosítottak kettő esetet: a szivárgó áram kialakulását és a felületet károsítót (korrózióhoz vezetőt) [48]. Kísérletükben polikarbonát égésekor keletkező füst IT eszközök belsejében lerakódó maradványa okozta a legnagyobb mértékű áramszivárgást, míg a PVC égésekor keletkező füst eredményezte a legnagyobb mértékű korróziót a keletkező hidrogén-klorid miatt. Természetesen az áramszivárgás- és a korrózió mértéke a lerakódó füstmaradvány mennyiségével egyenesen arányos, de az elmondható, hogy potenciálisan kétféleképpen károsíthatja az IT eszközöket, illetve növelheti meg egy további tűz kockázatát, hiszen a szivárgó áram hőtermeléssel jár.

Yin szerzőtársaival 2026-ban publikált tanulmányukban az adatközpontokban széles körben használt előre gyártott, heptafluorpropán tűzoltó rendszer működését elemezte a

rendszer optimális beállításának támogatása érdekében [49]. Mivel a heptafluorpropán tiszta, elektromosan nem vezető és maga után maradványt nem hagyó gáz, alkalmas elektronikai berendezések, IT eszközök tűzvédelmére. Az ezen gázt használó tűzoltó rendszerek oltási hatékonyságát két tényező befolyásolja: a hőelnyelés és a gáz örvénylő áramlása. A kutatási mérések alapján kijelenthető, hogy a heptafluorpropán gáz kibocsátása olyan mértékű hőelnyeléssel jár a gáz terjedésének irányában, hogy ott a hőmérséklet akár -33 Celsius fokra is lehűlhet. A kutatás során vizsgálták a gázkifúvás magasságának hatását a tűzoltó képességre. Eredményük szerint a fúvókák optimális magassága 1,925 m, ekkor maximális ugyanis a hűtő hatás. A fúvókák további magasságának növelésével láthatóvá vált a természetes konvekció intenzitásának csökkenése, hiszen az IT eszközökhöz már kisebb sűrűségű heptafluorpropán gáz érkezett a tűzoltó rendszer működésbe lépésének kezdetén, így - a kezdeti időben - a hőelnyelési képesség is csökkent volt.

Zeng kutatótársaival 2021-ben megjelent cikkükben az IT eszközök tápellátását biztosító kábelek és az adatátviteli kábelek külső borításának éghetőségét vizsgálták [50]. Méréseik igazolták a PVC borítású kábelek égésekor keletkező gázok korrodáló voltát, míg az eredmények alapján az LSZH (alacsony füstkibocsátású halogénmentes) kábelek égésekor keletkező gázok nem, vagy csak csekély mértékben vezethetnek az elektronikai eszközök korróziójához. Az éghetőség szempontjából a vizsgált kábelek ellenállónak bizonyultak a lángterjedéssel szemben, kivéve a 6 mm átmérőjű, PVC külső borítású és magas polietilén tartalmú szigetelő burkolattal rendelkező kábelt, mely tűzállóságát a teszteredmények megkérdőjelezik.

KÖVETKEZTETÉSEK

A fentiek szerinti nemzetközi szakirodalmi kutatásunk alapján az egyértelműen megállapítható, hogy az adatközponti tűzvédelem témájával foglalkozik a nemzetközi tudományos közösség, megjelennek a témakör különböző kérdéseit tárgyaló publikációk. Lehetséges tehát ezen publikációkból következtetéseket levonni, bár azt meg kell jegyezni, hogy ez a kutatási terület a vizsgált adatbázisban elérhető publikációk száma alapján kicsinek mondható, ezért a növekvő bár, de még mindig kevés számú tanulmányból fakadóan a következtetésekkel óvatosnak kell lenni.

Első, és talán legfontosabb következtetésként kijelenthető, hogy a téma fontosságát és aktualitását elismerte a tudományos közösség, ami összhangban áll a nemzetközi hírekben megjelenő, világszerte bekövetkező adatközponti tűzesetekkel. A vizsgált publikációk 71%-a 2025-ben vagy 2026-ban jelent meg. Ez a terület tehát kutatott, a problémákra válasz keresését a nemzetközi tudományos közösség aktuálisnak tartja, a vonatkozó tudományos kutatások száma jelenleg növekvő ütemben gyarapszik.

További következtetéseink során az adatközpontok tűzvédelmi szempontú sajátosságaiból kiindulva azt vizsgáljuk, hogy a nemzetközi kutatási eredmények hogyan kapcsolódnak ezen specialitásokhoz? Tűzvédelmi szempontból az adatközpontok sajátossága 1) az IT eszközök és elektromos berendezések hőtermelése; 2) az elektromos kábelek gyulladásának fokozott veszélye; 3) az akkumulátorok tűzveszélyessége; 4) az IT eszközöket nem károsító oltórendszerek iránti igény; 5) az eltérő tűzvédelmi kockázatú és megoldást igénylő helyiségek.

1. Kijelenthetjük, hogy az adatközponti hőtermelés okozta problémával a tudományos közösség napjainkban is foglalkozik: a vizsgált publikációk közül [44] olyan megoldást javasol az IT eszközök felépítésére, mely kevesebb hőtermeléssel jár. Ugyanakkor az épület hűtési lehetőségeit elemző tanulmányt nem találtunk kutatásunk során, ami alapján csak annyit jelenthetünk ki, hogy ez a kérdéskör tűzvédelmi szempontból eddig nem kutatott. Mindez alapján az nem zárható ki az, hogy az adatközponti hűtés témájának zajlik más szempontból, például energiahatékonyság szempontjából történő kutatása. Ennek megállapítása egy másik - jövőbeli - kutatás eredménye lehet.
2. Igazolt az adatközpontokban nagy mennyiségben jelen lévő elektromos kábelek tűzveszélyessége, illetve azoknak tűz kockázatát növelő hatása. Fenti kutatásunk alapján elmondható, hogy ezt a problémát a nemzetközi tudományos közösség vizsgálja, hiszen vonatkozó kutatási eredmények megjelennek. [47] és [50] egyaránt megállapította, hogy a vezetőanyag melegedéséből fakadóan melegszik a szigetelőanyag is, ami indukálhatja a műanyag szigetelőanyag polimerláncainak hasadását, a keresztkötött polimerek depolimerizációját és gyúlékony gázok keletkezését. Ezen eredmények további kutatásoknak ágyaznak meg, és a hőnek és tűznek ellenálló elektromos kábelek kifejlesztésének irányába való haladásra engednek következtetni. [48] az elektromos kábelek melegedésének és égésének folyamatát, illetve hatását tanulmányozta. Ez a tudománynak nem csak az előbb említett irányba való haladását mutatja, hanem még arra is következtethetünk, hogy a megkezdődött a kábelek égésének elektronikai eszközökre gyakorolt káros hatásának mérséklésére vonatkozó lehetőségek kutatása.
3. Akkumulátorok tűzveszélyességének problémájával foglalkozó tanulmányt nem találtunk kutatásunk során. Ennek a jelenségnek a széles körben ismert volta, továbbá a bekövetkezett tűzesetek példája valószínűsíti, hogy a tudományos közösség kutatja ezen kérdéskört, de vagy nem jelent még meg kutatási eredmény, vagy nem adatközpontokra fókuszáló kutatások zajlanak. Ennek megállapítására jelen kutatásunk elégtelen, így további szakirodalmi kutatás szükségeltetik.
4. Adatközpontok tűzvédelmi szempontú sajátossága az egy helyen koncentrálódó IT eszközök magas száma, melynek következtében speciális tűzoltási megoldások szükségesek. [49] az adatközpontokban széles körben használt előre gyártott, heptafluorpropán tűzoltó rendszer működését elemezte és határozta meg a rendszer optimális beállítását. Mivel a heptafluorpropán nem károsítja az elektronikai eszközöket, adatközpontokban használható, így az optimális beállítás gyakorlatban alkalmazható kutatási eredménynek tekinthető. Ugyanakkor az adatközpontok terjedését figyelembe véve valószínűsíthető, hogy az eltérő építészeti megoldások okán további kutatások válnak szükségessé, mindenesetre az kijelenthető, hogy a tudományos közösség gyakorlatban alkalmazható speciális tűzoltási rendszerre vonatkozó eredményt publikált 2026-ban.
5. Az adatközpontok eltérő felépítésűek lehetnek, azonban az közös bennük, hogy egymástól fizikailag és logikailag is elkülönülő helyiségekre bonthatóak, melyek tűz kockázatának szempontjából is eltérő tulajdonságokat mutatnak. [45] olyan fűtési-, szellőztetési- és hűtési rendszert javasolt irányítóhelyiségek számára, mely az

ilyen célú helyiségek füstmentesítését és hűtését lehet képes biztosítani. Az ezt az adatközpontokban is alkalmazható megoldást bemutató publikáció igazolja, hogy a nemzetközi tudományos közösség foglalkozik a katasztrófahelyzetekben még fontosabbá váló vezérlőtermek, irányítóhelyiségek tűzvédelmi kérdéseivel. Ugyanakkor az is kijelenthető, hogy ezen tanulmány csak egy szempontot vizsgált, további, ide illeszkedő publikációt nem találtunk kutatásunk során, így ezen helyiségek sajátosságaiból fakadó tűzvédelmi tényezők feltárása a tudományos közösség számára további feladatot jelenthet.

Az adatközpontok sajátosságai mentén levont következtetések után felmerül a kérdés, hogy a tűz kockázatának értékelése terén is szükséges-e, javasolható-e speciális megoldás? A 2026-ban megjelent [46] egy konkrét kockázatértékelési módszertant javasol adatközponti tűzvédelemre, mely figyelembe veszi a fent említett sajátosságok mellett a megtörtént incidensekből levonható tanulságokat is. Ezek alapján kijelenthető, hogy a nemzetközi tudományos publikáció gyakorlati alkalmazásra javasol egy, az adatközponti tűzvédelem specialitásaihoz igazodó kockázatértékelési módszertant. Hozzá kell tenni azonban, hogy ennek a 2026-ban publikált módszertannak a gyakorlati alkalmazásából nem állhat rendelkezésre kellő számú tapasztalat, így annak vizsgálata jövőbeli kutatási témául szolgálhat.

ÖSSZEFOGLALÁS

A tűz elleni védekezés fontossága vitathatatlan, különösen az IT szolgáltatások miatt kiemelt jelentőségű adatközpontok esetében, melyek némelyike a kritikus infrastruktúra részévé válik. Az adatközponti tűzvédelem szükségességét világszerte megtörtént incidensek is alátámasztják.

Az adatközpontok sajátosságait is figyelembe vevő tűzvédelmi kérdéskör jelentőségét a nemzetközi tudományos közösség felismerte, a témában az elmúlt években növekvő számú publikáció jelenik meg. Az adatközponti tűzvédelemmel foglalkozó nemzetközi tudományos cikkek áttekintése után több következtetést is levontunk. Legfontosabb következtetésként kijelenthető, hogy a téma aktualitását felismerte a tudományos közösség, ami összhangban áll a nemzetközi hírekben megjelenő, világszerte bekövetkező adatközponti tűzesetekkel. A vizsgált publikációk 71%-a 2025-ben vagy 2026-ban jelent meg. Ez a terület tehát kutatott, a vonatkozó tudományos kutatások számossága jelenleg növekvő ütemben gyarapszik. Ugyanakkor a jelenleg kevés számú tanulmány alapján az is feltételezhető, hogy ezen kutatások még gyerekcipőben járnak, a gyakorlatban is használható eredményekre még várni kell. Véleményünk szerint az adatközponti tűzvédelem területét továbbra is kutatni szükséges.

FELHASZNÁLT IRODALOM

[1] Banga, K., Harbansh, P., Singh, S. „Digitalisation and Structural Change: Evidence from Cross-Country Analysis” *JOURNAL OF DIGITAL ECONOMY*, 2026, https://doi.org/10.1016/j.jdec.2026.03.003

[2] Dobos O., Csiszárik-Kocsir Á. „Project-oriented perceptions of research, development and innovation in Hungarian, Polish and Romanian enterprises” *TRANSFORMATIONS IN BUSINESS & ECONOMICS*, 24(1), 2025, https://www.transformations.knf.vu.lt/64/article/proj

[3] Altaleb, H., Rajnai Z. „5G Infrastructure Standardization, Integration, Industry 4.0 Applications in EU Precisely Germany, and the Future of Industry 5.0 and 6G: A Comprehensive Overview”, In: Kovács, Tünde Anna; Stadler, Róbert Gábor; Daruka, Norbert (szerk.) *The Impact of the Energy Dependency on Critical Infrastructure Protection : Proceedings of the 5th International Conference on Central European Critical Infrastructure Protection (ICCECIP 2023)*, Cham, Svájc : Springer Nature Switzerland (2025), https://doi.org/10.1007/978-3-031-78544-3_7

[4] Fabricius-Ferke Gy. „Jönnek helyettünk a robotok? Rutinszerű, vagy egyedi munka; számítógépes szoftverek, vagy kreatív mesterséges intelligencia?” *POLGÁRI SZEMLE*, 20(1-3), 2024, https://doi.org/10.24307/psz.2024.0815

[5] Forgács A., Lukács J., Csiszárik-Kocsir Á., Horváth R. „Az internetes vásárlás magatartásának vizsgálata fuzzy következtetési rendszer segítségével” *POLGÁRI SZEMLE*, 20(4-6), 2024, https://polgariszemle.hu/images/content/pdf/1024307psz20241110.pdf

[6] Yu, Z., Liu, J. „The digital revolution in banking: Unpacking risk management in the age of transformation” *INTERNATIONAL REVIEW OF ECONOMICS & FINANCE*, Vol 103, 2025, https://doi.org/10.1016/j.iref.2025.104444

[7] Marosi Gy. „Digitalisation and Innovation in Public Administration” *POLGÁRI SZEMLE*, 21(4-6), 2025, https://doi.org/10.24307/psz.2025.0915

[8] Codreanu, A., Vasilescu, C. „Distance Learning or Resident Educational and Training Programs? Possible Solutions to the Effectiveness Dilemma in Military Education” *ROMANIAN MILITARY THINKING*, 2024(1), 2024, https://doi.org/10.55535/RMT.2024.1.10

[9] Heitlerné Lehoczky M., Kollár Cs. „A mesterséges intelligencia múltja, jelene és jövője a senior és a junior szakértők szemszögéből: 1. rész” *BIZTONSÁGTUDOMÁNYI SZEMLE,* 4(1), 2022, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/208/184

[10] Scholtz E., Pántya P. „A mestersége intelligencia fejlődése és felhasználhatósága a katasztrófavédelemben” *POLGÁRI VÉDELMI SZEMLE*, 18, 2026, https://mpvsz.hu/pv_szemlek/pvszemle2026/index.html

[11] Mihajlović, I., Petrović, N., Spasojević Brkić, V., Milijić, N. „Artificial intelligence as a tool for item reduction in an organizational resilience questionnaire” *INTERNATIONAL JOURNAL OF OCCUPATIONAL SAFETY AND ERGONOMICS*, 31(140), 2025, https://doi.org/10.1080/10803548.2025.2465165

[12] Csercsa K., Rajnai Z. „Adatvédelem és információbiztonság: az online térben fellelhető veszélyforrások, adathalászati módszerek (social engineering)” *BIZTONSÁGTUDOMÁNYI SZEMLE*, 7(2), 2025, https://doi.org/10.12700/btsz.2025.7.2.49

[13] Kiss A., Kollár Cs. „Az információbiztonság időszerű kérdései a magyarországi kkvk körében” *SCIENTIA ET SECURITAS*, 4(2), 2024, https://doi.org/10.1556/112.2023.00166

[14] Besenyő J., Őszi A. „Sensing From the Skies: A Comprehensive Analysis of the Latest Sensors on Drones” *JOURNAL OF ROBOTICS*, 2025 : 1, 2025, https://doi.org/10.1155/joro/3896195
[15] JP Morgan. „Business Leaders Outlook - Leaders forge ahead in 2026”, 2026, https://www.jpmorgan.com/insights/markets-and-economy/business-leaders-outlook/2026-us-business-leaders-outlook
[16] Chase. „2026 Business Leaders Outlook: Reflections and predictions for what’s next”, https://www.chase.com/business/knowledge-center/manage/blo-2026
[17] Marr, B. „5 Business Trends Every Company Must Prepare For In 2026” 2025, https://www.forbes.com/sites/bernardmarr/2025/11/18/5-business-trends-every-company-must-prepare-for-in-2026/
[18] Michelberger P. „Folyamatalapú, szabványos irányítási rendszerek a biztonságos és rugalmas vállalati működésért” *SCIENTIA ET SECURITAS*, 3(4), 2023, https://doi.org/10.1556/112.2023.00136
[19] Krepuska A., Nagy R. „Tűzvédelem gazdasági vonatkozásai multinacionális környezetben” *BIZTONSÁGTUDOMÁNYI SZEMLE*, 7(2), 2025, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/552
[20] Data Center Knowledge. „Digital Edge to Develop 500 MW Data Center Campus in Indonesia” 2026, https://www.datacenterknowledge.com/data-center-construction/digital-edge-to-develop-500-mw-data-center-campus-in-indonesia
[21] Data Center Knowledge. „Oracle Eyes $50B for AI Infrastructure in 2026” 2026, https://www.datacenterknowledge.com/infrastructure/oracle-eyes-50-billion-for-ai-infrastructure-in-2026
[22] Data Center Knowledge. „New Data Center Developments: February 2026”, 2026, https://www.datacenterknowledge.com/data-center-construction/new-data-center-developments-february-2026#European%20Data%20Center%20Developments
[23] Data Center Knowledge. „Moody’s: $3 Trillion Data Center Investment by 2030 Amid Power Challenges”, 2026, https://www.datacenterknowledge.com/energy-power-supply/moody-s-3-trillion-data-center-investment-by-2030-amid-power-challenges
[24] Berek L., Steiner A. „A térfigyelő kamerarendszer helye, szerepe a bűnmegelőzésben” *BELÜGYI SZEMLE*, 73(5), 2025, https://belugyiszemlejournal.org/index.php/belugyi-szemle/article/view/2102
[25] Besenyő J., Todorović, B. „Influence of security requirements to engineering in process industry” In: SMEITS - SMEITS (szerk.) *38. Međunarodni kongres o procesnoj industriji*. Online kiadás, Nemzetközi : Savez masinskih i elektrotehnickih inzenjera i tehnicara Srbije (SMEITS) (2025) pp. 191-198., https://izdanja.smeits.rs/index.php/ptk/article/view/8221/8459
[26] Muhoray Á. „A védelmi és biztonsági események, a katasztrófák következményei felszámolásában a fokozatosság elve” *POLGÁRI VÉDELMI SZEMLE*, 17, 2025, https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html
[27] Vass Gy., Ambrusz J., Restás Á., Varga F., Kátai-Urbán L. „A katasztrófavédelmi kutatások eredményei és fejlesztése a rendészettudomány rendszerében” *BELÜGYI SZEMLE*, 72(5), 2024, https://doi.org/10.38146/BSZ-AJIA.2024.v72.i5.pp815-833
[28] Bojtos Z., Nagy R. „Some aspects of a complex urban defence” In: Ćeranić, Predrag (szerk.) *ЗБОРНИК РАДОВА VI међународни научни скуп „Савремени изазови и*

прије безбједности" Бања Лука, Република Српска, БиХ, 27. март 2026. године = ZBORNIK RADOVA VI međunarodni naučni skup „Savremeni izazovi i prijetnje bezbjednosti" Banja Luka, Republika Srpska, BiH, 27. mart 2026. godine, Banja Luka, Bosznia-Hercegovina : Univerzitet u Banjoj Luci, Fakultet bezbjednosnih nauka (2026)

[29] Sikimić, M. „Security of European critical infrastructures outside the European Union: a review of the Western Balkans national laws" *INSIGHTS INTO REGIONAL DEVELOPMENT*, 4(2), 2022, https://doi.org/10.9770/ird.2022.4.2(5)

[30] Bálint K., Berek T. „Possible Computerized, Modern Solutions for Fire Protection of the Universities in Subotica, Serbia" In: Borsos, É; Horák, R; Kovács, C; Némesztovszky, Zs (szerk.) *Mobilitás : A Magyar Tannyelvű Tanítóképző Kar tudományos konferenciáinak tanulmánygyűjteménye*. Szabadka, Szerbia : Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar (2019) 679 p. https://magister.uns.ac.rs/files/kiadvanyok/konf2019/ConfSubotica2019.pdf#page=42

[31] Mihály I., Bérczi L., Bognár B., Kátai-Urbán M., Tóth L., Kátai-Urbán L., Vass Gy. Varga F. „Experimental Study to Determine the Leakage Area of Single-Leaf Smoke Control Doors in the Design of Pressure Differential Systems" *FIRE*, 8(1), 2025, https://doi.org/10.3390/fire8010005

[32] Restás Á. „A légi tűzoltás hatékonyságának tűzoltástaktikai megközelítése" *HADITECHNIKA*, 58(2), 2024, https://honvedelem.hu/kiadvanyok/haditechnika-2024-2-szam.html

[33] Érces G., Tóth R., Vass Gy., Varga F. „Developing fire safety visualised by augmented reality" POLGÁRI VÉDELMI SZEMLE, 17, 2025, https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html

[34] Data Center Knowledge „How to Prevent Data Center Fires: Lessons from the Biggest Incidents" 2024, https://www.datacenterknowledge.com/outages/how-to-prevent-data-center-fires-lessons-from-the-biggest-incidents

[35] CNA „Fire at Loyang data centre, SCDF operations still ongoing after a day" 2024, https://www.channelnewsasia.com/singapore/fire-loyang-digital-realty-data-centre-scdf-operation-4599316

[36] BDRShield „South Korea Data Center Fire: A Critical Wake-Up Call for Data Resilience" 2025, https://www.bdrshield.com/blog/south-korea-data-center-fire-a-critical-wake-up-call-for-data-resilience/

[37] Zhang, Y., Li, H., Wang, S. „The global energy impact of raising the space temperature for high-temperature data centers" *CELL REPORTS PHYSICAL SCIENCE*, 4(10), 2023, https://doi.org/10.1016/j.xcrp.2023.101624

[38] Horváth T. „Design Principles of a Physical Protection System for Data Centres: Essential Requirements for the Security Staff in the Physical Protection System" *MAGYAR RENDÉSZET*, 20(2), 2020, https://doi.org/10.32577/mr.2020.2.9

[39] Gulyás O. „A kiberbiztonság és a banki kibervédelem fejlődése napjainkig" *BIZTONSÁGTUDOMÁNYI SZEMLE*, 4(2), 2022, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/218

[40] Sándor B., Nagy R. „Adatközpontok tűzbiztonságának vizsgálata" *VÉDELEM TUDOMÁNY*, 5(1), 2020, https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13375

[41] Gyöngyössy É.E. „Fire Hazard of Fire-Resistant Cables Below the Ignition Point” *MŰSZAKI KATONAI KÖZLÖNY*, 35(3-4), 2026, http://doi.org/10.32562/mkk.2025.3-4.9
[42] Trabelsi, O., Kovács T. A. „A lítium-ion akkumulátorok tűzoltása” *MŰSZAKI TUDOMÁNYOS KÖZLEMÉNYEK*, 20(20), 2024, https://doi.org/10.33895/mtk-2024.20.16
[43] Pántya P. „A li-ion akkumulátorok tűzoltásával kapcsolatos kutatási tapasztalatok, a tűzoltói beavatkozás lehetőségei” *VÉDELEM TUDOMÁNY*, 8(2), 2023, https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13493/10935
[44] Badhe, P. et al. „Experimental and numerical investigation of LTCC-based liquid cold plate for high-performance computing processors” *APPLIED THERMAL ENGINEERING*, 279, 2025, https://doi.org/10.1016/j.applthermaleng.2025.128052
[45] Kim, B. „A smart HVAC retrofit system to improve fire safety in mission-critical facilities” *CASE STUDIES IN THERMAL ENGINEERING*, 77, 2026, https://doi.org/10.1016/j.csite.2025.107330
[46] Kareck, T.L. et al. „From incident to insight: Fire risk in modern data centers” *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, 100, 2026, https://doi.org/10.1016/j.jlp.2025.105890
[47] Liang, S. et al. „Pyrolysis and gas evolution behavior of overloaded flame-retardant polyethylene cable insulation” *CASE STUDIES IN THERMAL ENGINEERING*, 75, 2025, https://doi.org/10.1016/j.csite.2025.107223
[48] Newman, J.S., Su, P., Yee, G.G., Chivukula, S. „Development of smoke corrosion and leakage current damage functions” *FIRE SAFETY JOURNAL*, 61, 2013, http://dx.doi.org/10.1016/j.firesaf.2013.08.016
[49] Yin, Q. et al. „Field distribution characteristics and performance optimization of heptafluoropropane spraying and stratification in prefabricated fire-extinguishing systems” *CASE STUDIES IN THERMAL ENGINEERING*, 81, 2026, https://doi.org/10.1016/j.csite.2026.107935
[50] Zeng, D. et al. „Evaluation of flammability and smoke corrosivity of data/power cables used in data centers” *FIRE SAFETY JOURNAL*, 120, 2021, https://doi.org/10.1016/j.firesaf.2020.103094

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