ISSN 2676-9042

Vol 8, No 1, 2026.

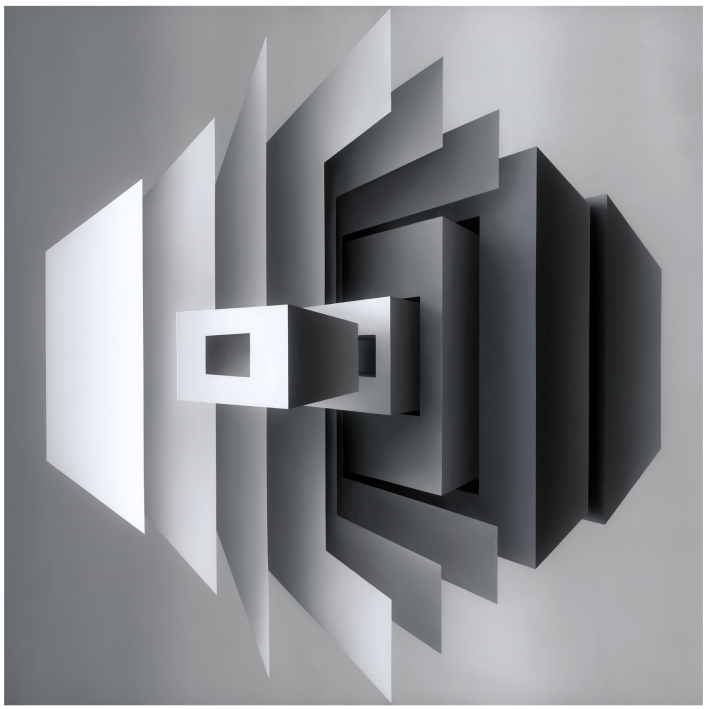
2026, VIII. évf. 1. szám

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 I. painting | **Kockahámozás I.** 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 1, 2026. | **2026. VIII. évf. 1. szám**

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

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 of 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.

BURAI István György

burai.istvan@bgk.uni-obuda.hu

István György BURAI is an Assistant Lecturer at the Donát Bánki Faculty of Mechanical and Safety En-

BURAI István György tanársegéd az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki

gineering, Óbuda University, Department of Manufacturing Technology. He teaches in the field of mechanical engineering, with a focus on CNC technology and computer-aided manufacturing. He is currently pursuing his PhD at the Doctoral School on Safety and Security Sciences of Óbuda University. His research examines the integration of artificial intelligence into education and its related security risks. His work focuses on the theoretical and empirical analysis of the AI–Education–CNC framework, including AI-based G-code generation and intelligent assistant systems. He has published on AI applications in education, SWOT-based strategic analysis, and the relationship between AI and CNC technologies, and has participated in an industrial digitalization project involving CNC data integration.

Kar, Gyártástechnológiai Intézeti Tanszékén. Gépészmérnöki szakterületen oktat, különös tekintettel a CNC-technológiára és a számítógéppel támogatott gyártástervezésre. Doktori tanulmányait az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában folytatja, ahol kutatási témája a mesterséges intelligencia oktatási adaptációja és annak biztonsági kockázatai. Tudományos munkája az MI–Oktatás–CNC hármas rendszerének vizsgálatára irányul, elméleti modellalkotás és empirikus kutatások keretében. Publikációi a mesterséges intelligencia oktatási alkalmazásával, SWOT-alapú stratégiai elemzésével, valamint az MI és CNC technológia kapcsolatával foglalkoznak. Részt vett ipari digitalizációs projektben, amely a CNC rendszerek adat- és folyamatintegrációjára irányult.

KISS Gábor

kiss.gabor@bgk.uni-obuda.hu

Prof. Dr. habil. Gábor KISS is a university professor at the Institute of Safety Science and Cybersecurity, Óbuda University. He received the PhD. degree in Mathematics and Computer Science from Debrecen University in 2013 and the Habilitation in Safety and Security Science from Óbuda University in 2020. Prof. Dr. KISS was guest scientist at the Faculty of Computer Science Freie Universität Berlin in 2003 and Universität Paderborn in 2006. He has published more than 210 refereed papers in Journals and Proceedings. He serves as an Editorial board member more Journals. Prof. Dr. KISS is a member of the Hungarian Academy of Sciences and more Hungarian and International Societies in Computer Science. Prof. Dr. KISS is an external expert of Bureau of Education, Hungary, National Research, Development and Innovation Office of Hungary. His research interests include computer science education, information security awareness, AI in self-driving vehicles and Healthcare.

Prof. Dr. habil. KISS Gábor egyetemi tanár az Óbudai Egyetem Biztonságtudományi és Kibervédelmi Intézetében. A Debreceni Egyetemen 2013-ban szerzett PhD fokozatot Matematika és Számítástudományból, 2020-ban pedig az Óbudai Egyetemen habilitált Katonai Műszaki Tudományból. Prof. Dr. KISS Gábor 2003-ban a Freie Universität Berlin Informatikai Karán, 2006-ban az Universität Paderborn Informatikai Karán volt vendégkutató. Több mint 210 referált tanulmány szerzője folyóiratokban és konferenciakiadványokban, valamint több folyóirat szerkesztő bizottsági tagja. Prof. Dr. KISS Gábor tagja a Magyar Tudományos Akadémiának, valamint több magyar és nemzetközi számítástechnikai társaságnak. Prof. Dr. KISS Gábor külső szakértője az Oktatási Hivatalnak, a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatalnak. Kutatási területe az informatika oktatás, információbiztonságtudatosság, a mesterséges intelligencia felhasználása az önvezető járművekben, valamint az egészségügyben.

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,

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

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.

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.

MANDIĆ Dorottya

mandic.dorottya@gmail.com

My name is Dorottya MANDIĆ, and I graduated from the Technical College of Applied Sciences in Bachelor of Management Engineering in Subotica, Serbia. I received my master's degree in Mechatronical Engineering from the Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering. I received my final certificate (absolutorium) at the Óbuda University Doctoral School in Safety and Security Sciences. My research area is the analysis of the security of smart devices.

MANDIĆ Dorottyának hívnak, és a Műszaki Szakfőiskolán fejeztem be a tanulmányaimat Szabadkán, Szerbiában, mint mérnök menedzser. A mesterképzést az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnika Mérnöki Karán szereztem meg, mint okleveles mechatronikai mérnök. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolában szereztem meg a végbizonyítványt (abszolutórium). A kutatási témám az okoseszközök biztonságának elemzésével foglalkozik.

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 vagyonvédelmi szervező szakirányon. Ezt követően ugyan ezen intézményben végezte el a munkavédelmi szakmérnöki képzést Először a vagyonvédelem területén dolgozott, mely után a munkavédelem területére váltott. Jelenleg az Opella Healthcare Hungary Kft. cégnél dolgozik, mint munkavédelmi mérnök. Doktori tanulmányain belül a mesterséges intelligencia (AI) felhasználását tervezi kutatni a munkavédelmen belül.

MÁRTON Zoltán

marton.zoltan@uni-obuda.hu

Zoltan MARTON is the head of the STEAM Office at Obuda University and the director of the Hungarian STEM Platform. He holds degrees in safety technology engineering and engineering education, and he is currently pursuing his PhD in Doctoral School on Security and Safety Sciences at Obuda University. His professional and research focus centers on STEAM-based curriculum development, skill-building for cyberspace-based protection strategies, and innovative, digitally supported teaching methods. He has been actively involved in coordinating and leading several international projects, including Erasmus+ initiatives and projects focused on digital skills, STEAM education, and gamified learning experiences. Through these roles, he contributes to advancing interactive and safety-focused educational content in Hungary and beyond.

MÁRTON Zoltán az Óbudai Egyetem STEAM Irodájának vezetője és a Magyarországi STEM Platform igazgatója. Biztonságtechnikai mérnöki és mérnök-pedagógiai diplomával rendelkezik, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában hallgató. Szakmai és kutatási fókuszában a STEAM-alapú tananyagfejlesztés, a kibertér-alapú védelmi stratégiák készségfejlesztése és az innovatív, digitálisan támogatott oktatási módszerek állnak. Aktívan részt vett több nemzetközi projekt koordinálásában és vezetésében, többek között Erasmus+ kezdeményezésekben és a digitális készségekre, a STEAM-oktatásra és a játékosított tanulási tapasztalatokra összpontosító projektekben. E szerepkörök révén hozzájárul az interaktív és biztonságközpontú oktatási tartalmak fejlesztéséhez Magyarországon és azon túl is.

NAGY Gergely

gergely.nagy777@gmail.com

The author is an information security expert and currently serves as Cybersecurity Business Manager at a Hungarian software development and IT security company. During his professional career, he has worked in corporate IT security, and prior to that held positions in public administration and diplomacy for more than a decade in Hungary and abroad, where he dealt with security policy and strategic issues. His research focuses on facility and information security, as well as the theory and practice of hybrid warfare, with particular emphasis on its information security, critical infrastructure protection, and migration-related dimensions. In his professional work, he strives to integrate technological, regulatory, and geopolitical perspectives in a comprehensive analytical framework.

A szerző információbiztonsági szakértő, jelenleg egy magyar fejlesztő és IT-biztonsági vállalat kiberbiztonsági üzletágának vezetője. Szakmai pályafutása során nagyvállalati IT-biztonsági területen dolgozott, ezt megelőzően pedig több mint egy évtizeden át államigazgatási és diplomáciai pozíciókat töltött be Magyarországon és külföldön, ahol biztonságpolitikai és stratégiai kérdésekkel foglalkozott. Kutatási területe a létesítmény- és információbiztonság, valamint a hibrid hadviselés elmélete és gyakorlata, különös tekintettel az információbiztonsági, kritikus infrastruktúra-védelmi és migrációs összefüggésekre. Szakmai munkájában a technológiai, szabályozási és geopolitikai dimenziók integrált elemzésére törekszik.

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

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 Országosl Katasztrófavédelmi Főigazgatóság Veszélyhelyzetkezelési Főosztályának helyettes vezetője lett. Summa cum laude minősítéssel szerzett PhD fokoza-

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.

tot 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.

OLÁH Róbert

olah.robert.oe@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 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 the 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.

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

PETŐ Richárd

peto.richard@bgk.uni-obuda.hu

Dr. Richard Peto has been an assistant professor at the Bánki Donat Faculty of Mechanical and Safety Engineering at Obuda University since 2015 and an associate professor since 2017. He obtained his doctorate in military engineering at the Doctoral School of Security Sciences. His main areas of research are criminal explosive activities and defense against them, as well as occupational safety. Both fields are linked to security technology in several ways, including technical equipment and human resource management.

Dr. PETŐ Richárd 2015-től az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar tanársegédje majd 2017-től adjunktusa. Doktori fokozatát Biztonságtudományi Doktori Iskolában katonai műszaki tudományok ágazatában szerezte. Fő kutatási területe a bűnös célú robbantásos tevékenységek és az ellenük történő védekezés, valamint a munkavédelem. Mindkét szakterület több ponton kapcsolódik a biztonságtechnikához, azon belül a technikai eszközök, valamint a humán erőforrás kezeléséhez.

RAJNAI Zoltán

rajnai.zoltan@uni-obuda.hu

Prof. Dr. Zoltan RAJNAI is currently the National Cyber Coordinator of Hungary and professor at the Obuda University. Previously Dr. RAJNAI served as Colonel in Hungarian Defense Forces (1981-2013)

Prof. Dr. RAJNAI Zoltán Magyarország nemzeti kiberkoordinátora, az Óbudai Egyetem professzora, 2015-tól az Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karának dékánja. A Biz-

and was professor at the National Defense University in the field of Information, info-communication, and telecommunication systems (1993-2013). Since 2013, Dr. RAJNAI also is the Dean of faculty of Mechanical and Safety Engineering, Head of Doctoral School on Safety and Security Sciences with main responsibilities in the field of Cyber Security, Information Security, info-communication, and telecommunication systems. Dr. RAJNAI received education from the High School at the Hungarian Defense Forces (1981-1985), the Military Academy (1990-1993), the Doctoral School on Military Sciences (1997-2000), and the Joint Security College-Paris, France (2003-2004).

tonságtudományi Doktori Iskola alapítója, vezetője, kutatási területe a kiberbiztonság, az információbiztonság, az infokommunikáció és a távközlési rendszerek fejlesztése. Korábban (1981–2013) ezredesként szolgált a Magyar Honvédségben, 1993–2013 között a Zrínyi Miklós Nemzetvédelmi Egyetem tanáraként fő szakterülete az információs, kommunikációs és távközlési rendszerek szervezése és azok biztonsága volt. RAJNAI professzor a katonai főiskolai és egyetemi tanulmányait követően a Hadtudományi Doktori Iskolában (1997–2000) és a párizsi Összhaderőnemi Védelmi Kollégiumban (CollègeInterarmées de Défense – CID) tanult.

RUCSKA András

rucska.andras@uni-nke.hu

András RUCSKA is a police major and master teacher at the Department of Forensic Science, Faculty of Law Enforcement, Ludovika University of Public Service. He has been teaching in the field of criminalistics for more than ten years. His research topics include modern biometric identification procedures and various image capture methods, including three-dimensional capture and photogrammetry. He is researching the law enforcement applications of virtual reality glasses. He is the leader of the national law enforcement VR working group, within which he organizes practical professional forums for representatives of various fields of law enforcement science. At these forums, they jointly analyze the potential applications of VR glasses in law enforcement, exploring areas where the technology can effectively support their work. The aim is to integrate VR into law enforcement practice and education, promoting innovation and knowledge sharing among professionals. His professional activities are enriched by publications in English and Hungarian in domestic and international scientific journals. In addition, he has given numerous conference presentations in both languages.

RUCSKA András rendőr őrnagy, a Nemzeti Közszolgálati Egyetem Rendszertudományi Kar Kriminál-technikai Tanszék mesteroktatója. Több mint tíz éve tanít a kriminalisztika területén. Kutatási témái a modern biometrikus személyazonosítási eljárások, valamint a különböző képrögzítési módszerek, köztük a háromdimenziós rögzítés, és a fotogrammetria. Kutatja a virtuális valóság szemüvegek rendészeti jellegű alkalmazhatóságát. Az országos rendészeti VR munkacsoport vezetője, melynek keretein belül a rendészettudományi terület különböző szakterületeinek képviselői számára szervez gyakorlati jellegű szakmai fórumokat. Ezeken közösen elemzik a VR szemüveg rendészeti alkalmazási lehetőségeit, feltárva azokat a területeket, ahol a technológia hatékonyan támogathatja a munkát. Célja a VR integrálása a rendészeti gyakorlatba, valamint az oktatásba, elősegítve az innovációt és a tudásmegosztást a szakemberek között. Szakmai tevékenységét angol és magyar nyelvű publikációk gazdagítják hazai, valamint nemzetközi tudományos folyóiratokban. Emellett számos konferenciaelőadást tartott mindkét nyelven.

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 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

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, 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

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.

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 1, 2026. | 2026. VIII. évf. 1. szám

CONTENT | TARTALOM

Security Systems column | Biztonságtechnika rovat

Security Awarenesscolumn | Biztonságtudatosság rovat

Health Security column | Egészségbiztonság rovat

Information Security column | Információbiztonság rovat

Legal and Social Security column | Jog- és társadalombiztonság rovat

Facility Security column | Létesítménybiztonság rovat

DOI: https://doi.org/10.12700/btsz.2026.8.1.1

THREE-DIMENSIONAL IMAGE CAPTURE METHODS AND VR VISUALIZATION IN THE FIELD OF CRIMINALISTICS

HÁROMDIMENZIÓS KÉPRÖGZÍTÉSI MÓDSZEREK ÉS VR-SZEMLÉLTETÉS A KRIMINALISZTIKA TERÜLETÉN

RUCSKA András[1]

Abstract

The study examines three-dimensional image capture technologies that can be used in crime scene documentation. Its aim is to compare these methods according to a uniform set of criteria in terms of accuracy, scene applicability, costs, data management, evidential value, and virtual reality compatibility, with a particular emphasis on applications optimized for the Meta Quest 3 device. The study shows that while laser scanning and photogrammetry provide the highest measurement reliability, 360° systems and drone photogrammetry are primarily suitable for quick, immersive overviews and global reconstruction of large sites. Neural, NeRF-based solutions appear to be a promising complementary tool for visualization, but their validation for forensic purposes is still limited. The study provides practical recommendations for integrating 3D models into VR environments and highlights that hybrid approaches offer the most balanced solution for forensic practice.

Keywords

three-dimensional image recording, crime scene, VR glasses, virtual reality, forensic science

Absztrakt

A tanulmány a bűnügyi helyszíndokumentálásban alkalmazható 3D képrögzítési technológiákat vizsgálja. Célja, hogy egységes szempontrendszer mentén hasonlítsa össze e módszereket pontosság, terepi alkalmazhatóság, költségek, adatkezelés, bizonyító erő és virtuális valóság kompatibilitás szempontjából, különös hangsúllyal a Meta Quest 3 eszközre optimalizált felhasználási lehetőségeken. A vizsgálat bemutatja, hogy míg a lézerszkennelés és a fotogrammetria biztosítja a legmagasabb méretezési megbízhatóságot, addig a 360°-os rendszerek és a drónos fotogrammetria elsősorban gyors, immerszív áttekintésre, nagy kiterjedésű helyszínek globális rekonstrukciójára alkalmasak. A neurális, NeRF-alapú megoldások ígéretes kiegészítő eszközként jelennek meg a szemléltetésben, de kriminalisztikai célú validációjuk még korlátozott. A tanulmány gyakorlati javaslatot ad a 3D modellek VR-környezetbe történő integrálására, és rámutat arra, hogy a hibrid megközelítések kínálják a legkiegyensúlyozottabb megoldást a kriminalisztikai gyakorlat számára.

Kulcsszavak

háromdimenziós képrögzítés, bűnügyi helyszín, VR szemüveg, virtuális valóság, krimináltechnika

[1] rucska.andras@uni-nke.hu | ORCID: 0000-0002-1431-7258 | master teacher, Ludovika University of Public Service, Faculty of Law Enforcement, Department of Forensic Sciences | mesteroktató, Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Krimináltechnikai Tanszék

BEVEZETÉS

A bűnügyi helyszínek dokumentálása a modern krimináltechnika egyik alapvető feladata, amelyre a hagyományos eszközök – jegyzőkönyv, helyszínvázlatrajz, fénykép- és videódokumentáció – évtizedeken keresztül önmagukban is elegendőnek bizonyultak. E módszerek közös jellemzője azonban, hogy a helyszín térbeli viszonyait csupán közvetetten, kétdimenziós ábrázolás révén jelenítik meg, ami a perspektívatorzulás, a takarások miatt korlátozza az értelmezhetőséget. A büntetőeljárás résztvevői – különösen a döntéshozók – számára ez megnehezítheti az események térbeli rekonstrukcióját, a cselekmény lefolyásának elképzelését és a bizonyítékok egymáshoz viszonyított helyzetének értékelését is.

Az elmúlt másfél évtized technológiai fejlődése ezen korlátokra egyre komplexebb válaszokat kínál: a háromdimenziós helyszíndokumentálás mára több, egymástól jelentősen eltérő megoldással érhető el, tehát már nem az a kérdés, hogy készítünk-e 3D felvételt, hanem az, hogy milyen módszerrel tesszük azt. A professzionális lézerszkennerek milliméteres pontossággal rögzítik a térbeli geometriát, míg a fotogrammetria – akár földi, akár légi (UAV) platformról – nagy pontosságú, textúrázott modellek előállítását teszi lehetővé már viszonylag széles körben hozzáférhető eszközökkel, mint egy egyszerű digitális fényképezőgép. Ezzel párhuzamosan elterjedtek a kézi 3D szkennerek, a 360°-os képalkotó rendszerek, valamint a mindennapi eszközök – okostelefonok, akciókamerák, sőt kiterjesztett valóságot támogató szemüvegek – által kínált, különböző szintű 3D rekonstrukciós lehetőségek.

A technológiák sokfélesége ugyanakkor új típusú problémákat vet fel a kriminalisztikai gyakorlat számára. Az egyes módszerek eltérnek egymástól a mérési pontosság, a terepen történő alkalmazhatóság, az eszközigény, a költségek, az adatkezelési követelmények és nem utolsósorban a bizonyítási eljárásban betölthető szerep szempontjából. A szakirodalomban és a gyakorlatban egyre több publikáció és esettanulmány foglalkozik egyes technikák – elsősorban a fotogrammetria és a lézerszkennelés – alkalmazásával, ugyanakkor jóval kevesebb olyan munka található, amely egységes keretben, azonos szempontok mentén hasonlítaná össze a különböző 3D dokumentációs eljárásokat.

További kihívást jelent, hogy a háromdimenziós modellek hasznosítása egyre inkább túllép a statikus megjelenítésen és a síkbeli kivetítésen. A virtuális valóság eszközei – különösen a széles körben elérhető, önálló működésre képes eszközök, mint a Meta Quest 3 – lehetővé teszik a bűnügyi helyszínek immerszív, bejárható formában történő megjelenítését. Ezzel új távlatok nyílnak a nyomozás, a helyszíni szemle utólagos elemzése, a szakértői munka, valamint a tárgyalótermi szemléltetés számára. Felmerül a kérdés, hogy a jelenleg elérhető 3D dokumentációs technológiák kimenete milyen mértékben és milyen kompromisszumokkal illeszthető ehhez a felhasználási módhoz.

Jelen tanulmány célja, hogy szisztematikus áttekintést adjon a bűnügyi helyszíndokumentálás szempontjából releváns háromdimenziós adatgyűjtési módszerekről, különös tekintettel a fotogrammetriára, a lézerszkennelésre, a kézi 3D szkennerekre, a 360°-os képalkotó rendszerekre, a mobil eszközökkel végzett 3D rekonstrukcióra és az újabb neurális alapú megoldásokra. Az elemzés középpontjában az egyes technológiák mérési pontossága, terepi alkalmazhatósága, eszközigénye, költségvonzata, adatkezelési sajátosságai és kriminalisztikai bizonyító ereje áll. A vizsgálat speciális fókusza annak feltárása, hogy a különböző módszerekkel előállított 3D modellek milyen mértékben és milyen – technikai, jogi, metodikai – feltételek mellett integrálhatók olyan virtuális valóság alapú bejárási környezetbe, amely Meta Quest 3 eszköz segítségével a gyakorlatban is alkalmazható.

A tanulmány a bevezetést követően röviden ismerteti a vizsgált technológiák működési elvét, majd összehasonlító módon elemzi azokat a fenti szempontok mentén. Ezt követi a VR-alapú megjelenítésre, különösen a Meta Quest 3-ra vonatkozó kompatibilitási kérdések tárgyalása, végül a gyakorlati ajánlások és a további kutatási irányok bemutatása.

RELEVÁNS HÁROMDIMENZIÓS ELJÁRÁSOK

Fotogrammetria

A fotogrammetria olyan képalkotó eljárás, amely több fényképfelvételből geometriai és képfeldolgozási módszerek segítségével állít elő mérhető, háromdimenziós modelleket. Forenzikus alkalmazásban a módszer alkalmas teljes bűnügyi helyszínek, részletek — például vérnyom-mintázatok, lövési csatornák — valamint emberi testek és holttestek dokumentálására, nagyfokú részletesség és pontosság mellett. A hazai szakirodalomban is dokumentált, hogy a fotogrammetria kiválóan alkalmazható kriminalisztikai helyszínrekonstrukciókra, holttestek és tárgyak térbeli modellezésére [1]. A legújabb vizsgálatok szerint a gondosan megtervezett közeli fotogrammetria gyors, költséghatékony és a gyakorlatban is reprodukálható alternatívája lehet bizonyos optikai szkennereknek, miközben a létrehozott modellek fotorealisztikus megjelenítést is biztosítanak [2]. A módszer pontossága függ többek között a kamera felbontástól, az alkalmazott optikától, a felvételek számától és geometriájától, valamint a fényviszonyoktól, amelyekre a helyszíni protokoll kialakításakor kiemelt figyelmet kell szentelni**.**

Háromdimenziós lézerszkennerés

A lézerszkennelés olyan aktív távérzékelési technika, amely a vizsgált objektum vagy helyszín felszínéről visszaverődő lézerimpulzusok idő- vagy fázismérésén alapuló távolságmérés révén nagy sűrűségű, háromdimenziós pontfelhőt hoz létre. A bűnügyi helyszínek dokumentálásban a 3D lézerszkennelők előnye a nagy kiterjedésű terek gyors, kvázi teljes körű, milliméteres pontosságú felmérése, amely lehetővé teszi a geometriai viszonyok és távolságok utólagos, objektív rekonstrukcióját. Több tanulmány kiemeli, hogy a lézerszkennelt pontfelhőkből előállított modellek a hagyományos fényképes dokumentációhoz képest pontosabb méréseket és részletesebb térbeli áttekintést biztosítanak, ami különösen fontos komplex bűnügyi helyszínek — vagy akár közlekedési balesetek — rekonstrukciójánál [3]. Ugyanakkor az eszköz magas költsége, a speciális képzés és a nagy mennyiségű adat kezelése olyan korlátok, amelyek befolyásolják a technológia szélesebb körű gyakorlati elterjedést.

360°-os képalkotás és virtuális túrák

A 360 fokos képalkotó rendszerek - egy- vagy több objektívvel rendelkező panorámakamerák - egyetlen álláspontról teljes gömbpanorámát rögzítenek, amelyből interaktív, virtuális bejárás jellegű megjelenítés valósítható meg. A kriminalisztikai gyakorlatban ezek a megoldások különösen a helyszín vizuális összképének gyors, kontaminációt mérséklő rögzítésére és a későbbi, távoli bejárhatóság biztosítására bizonyultak hasznosnak. A szakirodalom szerint a 360 fokos virtuális túrák támogatják a nyomozók, szakértők és bírósági szereplők térbeli orientációját, ugyanakkor a mérések pontossága és metrológiai megbízhatósága rendszerint elmarad a lézerszkennelő vagy fotogrammetriai rögzítési módszerektől [4]. Mindezek ellenére a technológia alacsony eszközigénye, gyors alkalmazhatósága és

erős szemléltető ereje miatt fontos kiegészítő eszközzé válhat hazánkban is a bizonyítási folyamatban.

Kézi 3D szkennerek és felszíni optikai szkennelés

A kézi, hordozható 3D szkennerek - jellemzően strukturált fényen alapuló felszíni szkennerek - kisebb objektumok, releváns tárgyak, anyagmaradványok nagy felbontású, mérhető 3D dokumentálására szolgálnak. Kriminalisztikai szempontból különösen fontos szerepe lehet a sérülések, lőcsatornák és egyéb morfológiai jegyek részletes rögzítésében, illetve a boncolás vagy exhumálás során végzett vizsgálatok kiegészítéseként. A kutatások azt mutatják, hogy a felszíni optikai szkennerek és a fotogrammetria kombinációja lehetővé teszi a külső és belső — például CT-alapú — információk integrálását, ezáltal komplex, multimodális 3D rekonstrukciók létrehozását a testek és sérülések vizsgálatára [5]. A kézi szkennerek ugyanakkor érzékenyek a mozgásra, fényviszonyokra és a kezelő ügyessége is kiemelten fontos, ezért alkalmazásuk egységes protokollokhoz és megfelelő képzéshez kötött.

Légieszközökkel végzett 3D dokumentálás

A pilóta nélküli légi járművekre (UAV, drón) szerelt kamerák és szenzorok lehetővé teszik a nagy kiterjedésű, nehezen megközelíthető helyszínek - például közlekedési balesetek, természeti katasztrófák - gyors, háromdimenziós dokumentálását. A mikro-UAV-vel végzett fotogrammetriai rekonstrukciókról szóló vizsgálatok rámutatnak, hogy viszonylag rövid idő alatt, minimális személyi jelenlettel és költséghatékony módon hozhatók létre részletes 3D modellek, amelyek alkalmasak a helyszín részleteinek utólagos elemzésére és mérésére [6]. A légi alapú felvételek különösen hasznosak a helyszín teljes geometriájának, a járművek, nyomok és objektumok egymáshoz viszonyított helyzetének áttekintésében, de az apróbb részletek - például kisebb nyomok, vércseppek - dokumentálása mindenképpen földi kiegészítő eljárásokat igényel. A jogi és légtérhasználati korlátok, valamint az időjárási és fényviszonyok szintén fontos tényezők a technológia kriminalisztikai alkalmazhatóságának értékelésekor.

Multimodális és újabb (neurális) megoldások

Az utóbbi években egyre nagyobb hangsúlyt kapnak a különböző 3D technológiákat - például CT, MRI, lézerszkennelés és fotogrammetria - integráló multimodális megközelítések, amelyek célja az egyéb releváns elváltozások minél teljesebb rekonstrukciója. Ezzel párhuzamosan megjelentek olyan neurális reprezentációkon alapuló eljárások — például neurális sugármezők (NeRF) — amelyek hagyományos képi adatokból képesek fotorealisztikus, interaktív 3D megjelenítést biztosítani, bár a mérési megbízhatóságuk és forenzikus validációjuk még korlátozott [7]. A szakirodalom jelenlegi állása szerint ezek az új módszerek ígéretes kiegészítő eszközök lehetnek a szemléltetés és a törvényszéki vizualizáció terén, ugyanakkor alkalmazásuk során fokozottan indokolt az alapadatok, a rekonstrukciós eljárás és a mérhetőség kritikus értékelése.

KUTATÁSI EREDMÉNYEK

Az alábbiakban ezeket az eljárásokat hasonlítom össze. A megfelelő átláthatóság érdekében két külön szempontrendszerű táblázatban jelenítem meg az eltéréseket.

Technológia	Pontosság	Költség	Terepi idő	Adatméret	Kezelői kompetencia
Fotogrammetria	0,5–2 mm	Alacsony	15–60 perc	Közepes (0,5–5 GB)	Közepes
Lézerszkennelés	1–5 mm	Magas	30–120 perc	Nagy (5–50 GB)	Magas
360° képalkotás	5–20 mm	Alacsony	5–20 perc	Közepes (0,5–3 GB)	Alacsony
Kézi 3D szkenner	0,1–1 mm	Közepes	10–30 perc	Közepes (1–10 GB)	Közepes
UAV/drón 3D	1–10 mm	Közepes	10–40 perc	Közepes (1–10 GB)	Közepes
Neurális (NeRF)	1–5 mm (vizuális)	Alacsony (szoftver)	10–30 perc	Nagy (modellfüggő)	Magas

1. táblázat Technikai paraméterek és költségek (saját szerkesztés)

Technológia	VR/Quest 3	Bizonyító erő	Fő előnyök	Fő hátrányok
Fotogrammetria	Kiváló (OBJ/GLB)	Magas	Fotorealisztikus, olcsó	Fénytől függ
Lézerszkennelés (TLS)	Jó (E57→OBJ)	Nagyon magas	Pontos, teljes lefedettség	Drága, nehéz
360° képalkotás	Kiváló (VR tour)	Közepes	Gyors, immerszív	Gyenge pontosság
Kézi 3D szkenner	Kiváló (PLY/OBJ)	Magas	Finom részletek, hordozható	Mozgási artefaktum
UAV/drón 3D	Jó (fotogrammetria)	Közepes-magas	Nagy terület	Időjárásfüggő
Neurális (NeRF)	Kísérleti	Alacsony	Fotorealisztikus, új	Mérhetőség bizonytalan

2. táblázat: Alkalmazhatóság és értékelés (saját szerkesztés)

Összehasonlító elemzés kriminalisztikai szempontok szerint

A vizsgált háromdimenziós dokumentációs technológiák összehasonlítását a kriminalisztikai gyakorlat számára meghatározó szempontok mentén végeztem: pontosság, költség, gyorsaság (helyszíni tevékenységgel eltöltött idő), kezelhetőség, adatkezelés, bizonyító érték és VR-kompatibilitás.

Mérési pontosság és reprodukálhatóság

A pontosság tekintetében a kézi 3D szkennerek (0,1--1 mm) és a fotogrammetria (0,5--2 mm) bizonyultak a legmegbízhatóbbnak finom részletek - például sérülések, nyomok - rögzítésére [2][8], míg a lézerszkennelés (1--5 mm) nagy kiterjedésű helyszínek teljes geometriájának milliméteres pontosságú felméréséra alkalmas. A 360 fokos rendszerek (5-

-20 mm) és UAV-alkalmazások (1-10 mm) a globális térbeli viszonyok szemléltetésére elegendők, de méréstechnikai validációhoz nem nyújtanak megfelelő megbízhatóságot. A neurális módszerek vizuális pontossága ígéretes, azonban mérettudományi reprodukálhatóságuk kriminalisztikai célra nem elfogadható, vagyis jelenleg nem minősül hiteles eszköznek.

Költség és gazdasági hatékonyság

Költségszempontból a fotogrammetria és 360 fokos képalkotás kiemelkedik: mindkét módszer alapfelszerelése (kamerák, szoftverek) 1000-5 000 EUR körüli beruházást igényel, így széles körben elérhetővé teszi a 3D dokumentációt kisebb költségvetésű rendőri szervek számára is [9]. Ezzel szemben a lézerszkennelés (20 000--100 000 EUR) és kézi szkennerek (5 000-30 000 EUR) jelentős kezdeti befektetést követelnek, míg az UAV-rendszerek (2 000-20 000 EUR) és neurális megoldások (szoftver-alapú) középkategóriába sorolhatók. Költséghatékony számítás során azonban a lézerszkennelő magas pontossága és hosszú élettartama indokolhatja a kiemelkedő árat speciális egységek számára.

Terepi alkalmazhatóság és gyorsaság

A 360 fokos képalkotás (5-20 perc) a leggyorsabb, így ideálisak a helyszín korai fázisában, mielőtt jelentős beavatkozás történik [4]. A kézi szkennerek (10-30 perc) lokális, kisméretű elváltozások, tárgyak rögzítésére szolgálnak, így a megjelenített időtartam nem releváns, hiszen nem az egész helyszín feltérképezésére irányul. A fotogrammetria (15-60 perc) és UAV (10-40 perc) közepes időtartamot igényel, míg a lézerszkennelés (30-120 perc) alapos előkészítést és több álláspontot követel meg. A neurális rekonstrukciók felvételi ideje rövid, de a számítási igény jelentős üzenetet hordoz. A kezelői kompetencia követelménye szintén döntő: míg a 360° automatikus, a lézerszkennelés és neurális módszerek speciális képzést igényelnek.

Adatkezelés és utófeldolgozás

A 360 fokos rendszerek kisebb adatmérete (0,5-3 GB) azonnali megtekintést tesz lehetővé, míg a lézerszkennelés (5-50 GB) és neurális modellek nagy volumene specializált tárolást, tömörítést és feldolgozást igényel [10]. A fotogrammetria és kézi szkennerek közepes méretű (1-5 GB) texturázott mesh-jei (OBJ, PLY) a legelterjedtebb formátumok, így könnyen integrálhatók meglévő programokba - például RealityCapture, Meshroom. A pontfelhő-adatok (E57, LAS) konvertálása mesh/VR-célra elengedhetetlen, ami további időt és szakértelmet kíván.

Bizonyító érték és jogi megfontolások

A lézerszkennelés és fotogrammetria rendelkezik a legmagasabb bizonyító erővel, mivel mindkettőnél standardizált metrológiai protokollok és validációs eljárások állnak rendelkezésre, amelyek megfelelnek annak az elvnek, hogy büntetőeljárásban a rögzített objektum bizonyítékként felhasználható legyen [11]. A kézi szkennerek dokumentációi kiemelkedőek, míg a 360° elsősorban szemléltetésre alkalmas. Az UAV és neurális módszerek alkalmazása jelenleg korlátozott a szabályozási (légtérhasználat) és validációs (algoritmus-függő torzítás) kérdések miatt.

Virtuális valósággal való kompatibilitás

A fotogrammetria, kézi szkennerek és 360 fokos rendszerek natívan támogatják a virtuális szemüvegek rendszerét OBJ/GLB exporton keresztül [12]. A lézerszkennelés

E57/PLY/OBJ konverzió után hasonlóan működik, míg az UAV fotogrammetriai kimenete azonos ezzel. A neurális (NeRF) modellek speciális splat-rendereket igényelnek, amelyek még kísérleti stádiumban vannak a virtuális szemüvegek platformján. A 360 fokos kamera felvételei azonnal használhatók VR-szemüvegen, minimális utómunkával.

Meta Quest 3 kompatibilitás

A Meta Quest 3 önálló VR-headsetként kiválóan alkalmas a bűnügyi helyszínek immerszív bejárására, mivel natívan támogatja a modern 3D formátumokat (GLB/GLTF, OBJ, FBX), amelyek közvetlenül importálhatók VR-alkalmazásokba. A kriminalisztikai jellegű 3D modellek megtekintéséhez azonban a nyers kimeneteket (pontfelhő, fotogrammetriai mesh) megfelelő formátumra kell konvertálni, ami technológiánként eltérő nehézségi fokot jelent [13].

Natívan támogatott technológiák, mint a fotogrammetria és kézi 3D szkennerek kimenete (OBJ, PLY, GLB) közvetlenül kompatibilis: RealityCapture vagy Meshroom szoftverekkel texturázott mesh-eket lehet létrehozni, amelyeket Unity/Unreal motorokba importálva Quest 3-ra telepíthetők önálló APK-ként (Android operációs rendszer alkalmazáscsomag-fájlformátuma). A 360 fokos képalkotás natív VR-túrája a formátumának köszönhetően — például Matterport, Kuula — böngésző-alapú streaminggel azonnal működik Quest 3-on, minimális utófeldolgozással [14]. Ezeknél a módszereknél - érzékelhetőségi szempontból - a jelenlét kiemelkedő, könnyen rögzíthető a fotorealisztikus textúra és a természetes mozgás.

A konverzió-igényes technológiák, mint a lézerszkennelés nagy pontfelhői (E57, LAS) először PLY/OBJ mesh-re konvertálandók - például CloudCompare, ReCap -, majd optimalizálva Quest 3-ra. Szakértői vizsgálatok szerint a konvertált pontfelhők Quest 3-on kiválóan alkalmasak helyszíni rekonstrukcióra, különösen Resolve vagy hasonló VR viewer appokkal, PC-streaminggel [15]. Az UAV/drón fotogrammetriai modelljei hasonló munkafolyamatot követnek, mint a földi fotogrammetria.

Az igazságszolgáltatás területén alkalmazható előnyök és korlátok

A Quest 3 lehetővé teszi a tárgyaltermi immerszív szemléltetést, ahol a döntéshozók természetes skálában, valós perspektívából vizsgálhatják a helyszínt, jelentősen javítva a térbeli megértést. Korlátok: a nagy modellek (>1 GB) teljesítményproblémákat okoznak önálló módban - PC streaming ajánlott -, valamint a jogi validáció némely esetben még kialakulóban van. Összességében a fotogrammetria és a 360° hibrid kínálja a legjobb egyensúlyt gyorsaság, minőség és Quest 3-kompatibilitás között az igazságszolgáltatás számára.

KÖVETKEZTETÉSEK, JAVASLATOK

A vizsgált háromdimenziós helyszíndokumentációs technológiák átfogó elemzése alapján megállapítható, hogy egyetlen „legjobb" megoldás sem létezik a kriminalisztikai gyakorlatban. A választás mindig a helyszín típusától, a rendelkezésre álló erőforrásoktól, a vizsgálati céltól és a bizonyítási követelményektől függ. A Meta Quest 3 VR szemüveg bevezetése forradalmasíthatja a nyomozók, az igazságügyi szakértők munkáját, emellett a tárgyalótermi szemléltetést is, hiszen közelebb hozhatjuk a döntéshozókhoz a bűnügyi helyszínt.

A jövőben érdemes lenne azzal kapcsolatos kutatásokat végezni, hogy kialakításra kerüljön egy olyan protokoll rendszer, ami figyelembe veszi a rögzítendő objektum sajátosságait, időjárási körülményeit, valamint az adott szervezeti egység gazdasági helyzetét.

ÖSSZEFOGLALÁS

A tanulmány szisztematikus áttekintést ad a kriminalisztikai helyszíndokumentációban alkalmazható háromdimenziós képkészítési technológiákról – fotogrammetria, lézerszkennelés, kézi 3D szkennerek, 360° képalkotás, UAV/drón-felmérések és neurális rekonstrukciók -, egységes szempontok (pontosság, terepi alkalmazhatóság, költségek, adatkezelés, bizonyítékérték, VR-kompatibilitás) szerinti összehasonlításukkal, különös hangsúllyal a Meta Quest 3 VR szemüvegre optimalizált alkalmazásokra. A következtetés szerint nincs egyetlen univerzális legjobb módszer, mert a választás a helyszín típusától, rendelkezésre álló erőforrásoktól, vizsgáló céltól és bizonyítási követelményektől függ; a lézerszkennelés és fotogrammetria kínálja a legmagasabb mérési megbízhatóságot komplex helyszíneken, a 360° rendszerek és drónok gyors immerszív áttekintésekre, a kézi szkennerek finom részletekre, míg a neurális (NeRF) megoldások ígéretesek vizualizációra, de forenzikus validációjuk korlátozott. Hibrid megközelítéseket - különösen lézerszkennelés, fotogrammetria és 360° VR-túrák kombinációját - javasol a legkiegyensúlyozottabb megoldásként, amelyek a virtuális szemüvegekkel forradalmasíthatják a nyomozásokat, szakértői munkát és tárgyalótermi szemléltetéseket.

FELHASZNÁLT IRODALOM

[1] D. Metzger, M. Újvári, és Z. Gárdonyi, „A fotogrammetria kriminalisztikai célú alkalmazása: helyszínek, holttestek, tárgyak rekonstrukciója három dimenzióban," *Belügyi Szemle*, 2020. [Online]. Elérhető: https://belugyiszemlejournal.org/index.php/belugyiszemle/article/view/743.

[2] F. Dedouit et al., „The current state of forensic imaging – perspectives," *Int. J. Legal Med.*, vol. 139, no. 6, pp. 2819–2827, Mar. 2025. [Online]. Elérhető: https://pmc.ncbi.nlm.nih.gov/articles/PMC12532732/.

[3] „Crime Scene Documentation: Weighing the Merits of Three-Dimensional Laser Scanning," *NIJ*, 2020. [Online]. Elérhető: https://nij.ojp.gov/topics/articles/crime-scene-documentation-weighing-merits-three-dimensional-laser-scanning.

[4] „360 Virtual Tours in Crime Scene Investigation," *CSI 360*, 2023. [Online]. Elérhető: https://www.csi360.net/blog/360-photography/360-virtual-tours-in-crime-scene-investigation.

[5] C. Villa, N. Lynnerup, és C. Jacobsen, „A Virtual, 3D Multimodal Approach to Victim and Crime Scene Reconstructions," *Forensic Sci. Int.*, vol. 325, Oct. 2021. [Online]. Elérhető: https://pmc.ncbi.nlm.nih.gov/articles/PMC10894066/.

[6] „Micro-Quadcopter UAV for Crime Scene Documentation," *ETASR*, vol. 12, no. 6, pp. 9626–9630, 2022. [Online]. Elérhető: https://www.etasr.com/index.php/ETASR/article/view/6260.

[7] J. T. Kajiya és B. P. Von Herzen, „Ray tracing volume densities," *SIGGRAPH Comput. Graph.*, vol. 18, no. 3, pp. 165–174, Jul. 1984. [Online]. Elérhető: https://www.sciencedirect.com/science/article/abs/pii/S2212478017300916.

[8] C. Herke, „A mesterséges intelligencia kriminalisztikai aspektusai," *Belügyi Szemle*, vol. 69, no. 10, pp. 1709–1724, 2021. [Online]. Elérhető: https://belugyiszemlejournal.org/index.php/belugyiszemle/article/download/888/889/1396.

[9] „3D Documentation Methods Comparison," *Learning Gate*, vol. 5, no. 2, pp. 45–59, 2022. [Online]. Elérhető: https://learning-gate.com/index.php/2576-8484/article/download/1717/594.

[10] C. Villa, N. Lynnerup, és C. Jacobsen, „Multimodal 3D Reconstruction in Forensic Science," *Forensic Sci. Int.*, 2023. [Online]. Elérhető: https://pmc.ncbi.nlm.nih.gov/articles/PMC10894066/.

[11] D. Metzger, M. Újvári, és Z. Gárdonyi, „Forenzikus 3D dokumentáció validációja," *Belügyi Szemle*, vol. 68, no. 11, pp. 57–70, 2020. [Online]. Elérhető: https://real.mtak.hu/117021/1/Metzger-Ujvari-GardonyiBelugyi-Szemle2020.evi11.szam57-70..pdf.

[12] „Meta Quest 3 GLB Format Support," *Meta*, 2024. [Online]. Elérhető: https://www.meta.com/experiences/glimpse-glb/25467602739525995/.

[13] „Download 3D Scanning & Photogrammetric 3D Models in GLB and USDZ," *AR Code*, Jan. 2024. [Online]. Elérhető: https://ar-code.com/blog/download-3d-scanning-photogrammetric-3d-models-in-glb-and-usdz.

[14] „360 Virtual Tours in Crime Scene Investigation," *CSI 360*, 2023. [Online]. Elérhető: https://www.csi360.net/blog/360-photography/360-virtual-tours-in-crime-scene-investigation.

[15] „Micro-Quadcopter UAV for Crime Scene Documentation," *ETASR*, vol. 12, no. 6, pp. 9626–9630, 2022. [Online]. Elérhető: https://www.etasr.com/index.php/ETASR/article/view/6260.

DOI: https://doi.org/10.12700/btsz.2026.8.1.11

INTERACTIVE DEFENSE MECHANISMS: INTEGRATING PROTECTION AGAINST SOCIAL ENGINEERING INTO INCIDENT MANAGEMENT PROCESSES

INTERAKTÍV VÉDELMI MECHANIZMUSOK: A PSZICHOLÓGIAI MANIPULÁCIÓ ELLENI VÉDEKEZÉS INTEGRÁLÁSA AZ INCIDENSKEZELÉSI FOLYAMATOKBA

MÁRTON Zoltán[1] – RAJNAI Zoltán[2] – PETŐ Richárd[3]

Abstract

This study analyzes social engineering as a systemic risk and strategic challenge. It highlights that technical defenses alone cannot ensure digital immunity, as most attacks exploit the human factor. The paper examines leadership accountability under NIS2 and the dependence of Return on Security Investment (ROSI) on human resilience. It demonstrates that without addressing cognitive vulnerabilities, the efficiency of technical controls declines. As a solution, an innovative Minecraft-based gamified methodology is presented, built on "cognitive slowing." Empirical results prove that through experiential learning, the manipulation success rate can be reduced from 60% to 20%, significantly enhancing organizational resilience and security culture.

Keywords

social engineering, resilience, security awareness training (SAT), proactive incident management, gamified learning environments (GLE), human-centric security management

Absztrakt

A tanulmány a pszichológiai manipulációt (social engineering) rendszerszintű kockázatként és stratégiai kihívásként elemzi. Rávilágít, hogy a technikai védelem önmagában nem garantál digitális immunitást, mivel a támadások az emberi tényezőt célozzák. Vizsgálja a NIS2 szerinti vezetői felelősséget és a biztonsági megtérülés (ROSI) függőségét a humán rezilienciától. Igazolja, hogy a kognitív sebezhetőségek kezelése nélkül a technikai kontrollok hatékonysága romlik. Megoldásként innovatív, Minecraft-alapú gamifikált módszertant mutat be, amely a „kognitív lassítás” elvére épít. Az eredmények bizonyítják, hogy a tapasztalati tanulás révén a manipulációs sikerességi ráta 60%-ról 20%-ra csökkenthető, érdemben növelve a szervezeti ellenálló képességet.

Kulcsszavak

pszichológiai manipuláció, reziliencia, biztonságtudatossági képzés, proaktív incidenskezelés, gamifikált tanulási környezetek, emberközpontú biztonságmenedzsment

[1] marton.zoltan@uni-obuda.hu | ORCID: 0009-0006-7795-076X | PhD Student, Doctoral School on Safety and Security Sciences Obuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola
[2] rajnai.zoltan@uni-obuda.hu | ORCID: 0000-0002-9139-736X | professor, Obuda University, Banki Donat Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
[3] peto.richard@bgk.uni-obuda.hu | ORCID: 0000-0002-6757-0863 | adjunct professor, obuda University Banki Donat Faculty of Mechanical and Safety Engineering | egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az informatikai rendszerek biztonságmenedzselése során a technológiai védelmi rétegek – mint a tűzfalak vagy a behatolásjelző rendszerek (IDS/IPS) – elsődleges szerepe vitathatatlan, azonban a védelem önmagában már nem képes garantálni a szervezet teljes körű digitális immunitását [1]. Napjaink kiberbiztonsági incidenseinek domináns hányada nem technikai hiányosságokra, hanem az emberi tényező célzott kihasználására vezethető vissza. Ez a felismerés a pszichológiai manipulációt (social engineering, SE) fokozottan kritikus, rendszerszintű kockázattá emelte [2].

Ebben a megközelítésben az információbiztonság már nem csupán informatikai, hanem stratégiai vállalatirányítási kérdés, ahol a humán sebezhetőségek kezelése a kockázatmenedzsment szerves részét képezi. A biztonságmenedzsment alapvető célja az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának (CIA triád) fenntartása [1]. A menedzsment feladata a kockázatok precíz azonosítása, ahol a kockázat mértéke (K) a fenyegetettség (F), a sebezhetőség (S) és az eszközérték (E) szorzataként határozható meg ($K = F \times S \times E$). A pszichológiai manipuláció során a támadó a humán erőforrás kognitív sebezhetőségeit aknázza ki, megkerülve a robusztus technikai kontrollokat.

Jelen tanulmány célja a pszichológiai manipuláció anatómiájának feltárása döntéshozói nézőpontból. Vizsgáljuk az adathalászat (phishing) és az online félrevezetés (pretexting) hatásait az üzleti folytonosságra, valamint rávilágítunk a NIS2 irányelv által támasztott kiterjesztett vezetői felelősségre [3]. A dolgozat keretében bemutatjuk a manipuláció kognitív hátterét és egy innovatív, gamifikált módszertant, amely képes mérhetően növelni a szervezeti rezilienciát.

PSZICHOLÓGIAI MANIPULÁCIÓ, MINT RENDSZERSZINTŰ KOCKÁZAT

Az informatikai rendszerek biztonságának menedzselése során a technológiai védelmi rétegek (a tűzfalak vagy a behatolásjelző rendszerek) elsődleges szerepe vitathatatlan, azonban önmagukban elégtelenek a szervezet teljes körű védelméhez [1]. A kiberbiztonsági incidensek szignifikáns része nem szoftveres bug-okra, hanem az emberi tényező célzott kihasználására vezethető vissza, ami a pszichológiai manipulációt (social engineering-et) elsődleges fenyegetési vektorrá emeli [2].

Ebben a kontextusban az információbiztonság már nem csupán IT-üzemeltetési, hanem stratégiai menedzsmentet érintő kérdés, ahol a humán sebezhetőségek azonosítása és mitigálása a kockázatkezelési folyamat integráns részét kell, hogy képezze. Jelen fejezet célja a pszichológiai manipuláció mechanizmusainak feltárása vezetői nézőpontból, rávilágítva arra, hogy az adathalászat és az online félrevezetés típusú támadások miként veszélyeztetik az informatikai rendszerek integritását és az üzletmenet-folytonosságot (Business Continuity) [3].

A rendszerszintű megközelítés keretében vizsgáljuk a humán sebezhetőségek hatását a kritikus infrastruktúrák védelmére [5], valamint a NIS2 irányelv által támasztott új típusú vezetői elszámoltathatóságot a biztonságtudatosság növelése terén [3]. A következőkben részletesen elemezzük a nagy gyakorisággal előforduló támadási vektorokat és azokat a pszichológiai mechanizmusokat, amelyek a védelmi protokollok sikeres kijátszását teszik lehetővé.

Adathalászat, online félrevezetés és a menedzseri kontrollok

Az informatikai biztonságmenedzsment alapvető célja az információs eszközök bizalmasságának, sértetlenségének és rendelkezésre állásának (CIA követelményrendszer) fenntartása [1]. A menedzsment feladata a kockázatok azonosítása, ahol a kockázat mértéke (K) a fenyegetettség (F), a sebezhetőség (S) és az eszközérték (E) szorzataként határozható meg:

$$K = F \times S \times E$$

A pszichológiai manipuláció során a támadó nem a szoftverekben rejlő biztonsági réseket, hanem a humán erőforrás pszichológiai sebezhetőségeit használja fel a rendszerbe való bejutáshoz, így a szervezet különösen nehezen kiismerhető pontját támadja [2]. A pszichológiai manipuláció támadások egyik széles körben elterjedt formája az adathalászat, amely során a támadó legitimnek tűnő forrásból származó elektronikus kommunikáció útján próbál bizalmas adatokat vagy jelszavakat megszerezni [3].

Ennél specifikusabb a szigonyozás (spear phishing), amely során a támadó előzetes információgyűjtést követően egy konkrét személyt vagy munkaköri csoportot céloz meg, jelentősen növelve az üzenet hitelességét [3]. Az online félrevezetés során a támadó egy előre kidolgozott forgatókönyvre vagy ürügyre alapozva próbálja megnyerni a felhasználó bizalmát, gyakran olyan szerepbe bújva (rendszergazda vagy éppen hatósági ellenőr), amely felhatalmazza őt a biztonsági protokollok ellenőrzésére vagy megkerülésére [3]. A menedzsment szempontjából e támadások közvetlen hatással vannak az incidenskezelési folyamatokra, mivel a sikeres manipuláció révén a támadó legitim jogosultságokkal rendelkező „belső” szereplőként tűnhet fel, ami kritikusan megnehezíti a behatolás észlelését [6]. Az incidens átlagos észlelési idejének (Mean Time to Detect) növekedése a kritikus infrastruktúrák és a közszolgálat esetében hatványozott kockázatot hordoz, ahol a hierarchikus felépítés és a tekintélytisztelet megkönnyítheti a felsőbb vezető nevében elkövetett visszaéléseket [7]. A proaktív kontrollok hiánya ilyen környezetben nem csupán informatikai hiba, hanem a rendszerszintű biztonsági kultúra hiányossága, amelynek fejlesztése a Magyar Honvédség és más rendvédelmi szervek esetében is kiemelt prioritás [8].

PSZICHOLÓGIAI MECHANIZMUSOK ÉS HUMÁN SEBEZHETŐSÉGEK

A pszichológiai manipuláció sikeressége nem a technikai ismeretek hiányán, hanem az emberi gondolkodás, az észlelés, a megismerés, az információfeldolgozás mentális folyamatai és a szociálpszichológiai automatizmusok célzott kihasználásán alapul. Az informatikai rendszerek biztonságmenedzsmentje során a humán sebezhetőséget olyan komplex kockázati faktorként kell definiálni, amely az egyéni kognitív architektúra és a szervezeti kultúra interakciójából fakad [1], [2].

A kritikus infrastruktúrák védelmében a pszichológiai manipuláció különösen veszélyes, mivel a támadók a rendszert üzemeltető személyzet bizalmát és segítőkészségét használják fel a fizikai vagy logikai védelem megkerülésére [5], [9].

A Kognitív Kettős Folyamat elmélet alkalmazása

A manipuláció megértéséhez a Kognitív Kettős Folyamat elmélet (Dual-Process Theory) alkalmazása nyújt megfelelő keretet. Az emberi információfeldolgozás két, egymástól eltérő működésű rendszerre bontható: az 1. rendszerre, amely gyors, intuitív és érzelmi alapú, valamint a 2. rendszerre, amely lassabb, analitikus és logikus működésű. [10].

A pszichológiai manipuláció során a támadók manipulatív ingerek - például sürgető adathalász e-mailek vagy vészhelyzetet imitáló hívások - alkalmazásával elsősorban az 1. rendszer aktiválására törekednek (lásd: 1. ábra). Ez a rendszer heurisztikákra, érzelmi reakciókra (sürgetés, félelem) és tekintélyelvű mintákra támaszkodik, ami lehetővé teszi a 2. rendszer kritikus elemző és ellenőrző funkcióinak megkerülését. Ennek következtében elmaradhat a biztonsági szabályzatok tudatos ellenőrzése és az információk hitelesítése, ami közvetlenül hozzájárulhat rosszindulatú cselekvésekhez (például linkekre való kattintás, érzékeny adatok felfedése) [10].

A folyamatot tovább erősítik a különböző kognitív heurisztikák, ahogyan az 1. ábra is szemlélteti és torzítások (biases), mint a túlzott magabiztosság (overconfidence bias), a megerősítési torzítás, illetve az optimizmus-torzítás, amelynek hatására a munkavállalók hajlamosak alábecsülni saját szervezetük kitettségét a kiberbiztonsági fenyegetésekkel szemben [11]. Ez a kognitív „rövidzárlat” jelentősen csökkenti az éberségi szintet, és növeli a manipuláció sikerességének esélyét.

1. ábra - A kognitív kettős folyamat elmélet alkalmazása pszichológiai manipuláció során (saját ábra)

Az egyéni sebezhetőséget jelentősen befolyásolják a személyiségjegyek is. A kutatások szerint a „Big Five” személyiségmodell elemei közül a magas barátságosság (agreeableness) és az extraverzió szignifikánsan növelheti a manipulációval szembeni kitettséget, mivel az ilyen jegyekkel rendelkező egyének hajlamosabbak a gyors bizalomépítésre [12]. Ezzel szemben a lelkiismeretesség (conscientiousness) gyakran védelmi faktorként jelenik meg, mivel a szabálykövetőbb magatartás szorosabb összefüggést mutat a biztonsági protokollok betartásával [12].

A menedzsment számára ez azt jelenti, hogy a biztonságtudatossági stratégiákat nem lehet uniformizáltan kezelni, hanem figyelembe kell venni a munkavállalói állomány

pszichológiai heterogenitását. A hierarchikus szervezetekben, különösen a közigazgatásban és a rendvédelmi szerveknél, a tekintélynek való engedelmesség és a társas megfelelési kényszer válik a legfőbb sebezhetőségi ponttá [7], [8]. A támadók a legitimáció látszatával és az időkényszer alkalmazásával olyan érzelmi állapotot hoznak létre, amelyben a munkavállaló hajlamosabb a szabályok áthágására egy „felsőbb cél" vagy sürgős vezetői kérés érdekében [4].

A hagyományos biztonságtudatossági programok gyakran vallanak kudarcot, mert csupán az elméleti tudásátadásra fókuszálnak, és nem kezelik ezeket a mélyen gyökerező viselkedési automatizmusokat [13]. Az incidenskezelés proaktív szakaszában a menedzseri kontrolloknak ki kell terjedniük ezen pszichológiai kiváltó okokra (trigger-ekre), azok monitorozására és szimulált tesztelésére [6]. A reziliencia kialakításához olyan interaktív módszertanra van szükség, amely a kognitív lassítás elvét alkalmazva képessé teszi a felhasználót a manipulációs technikák valós idejű (real-time) felismerésére és a 2. rendszer tudatos aktiválására.

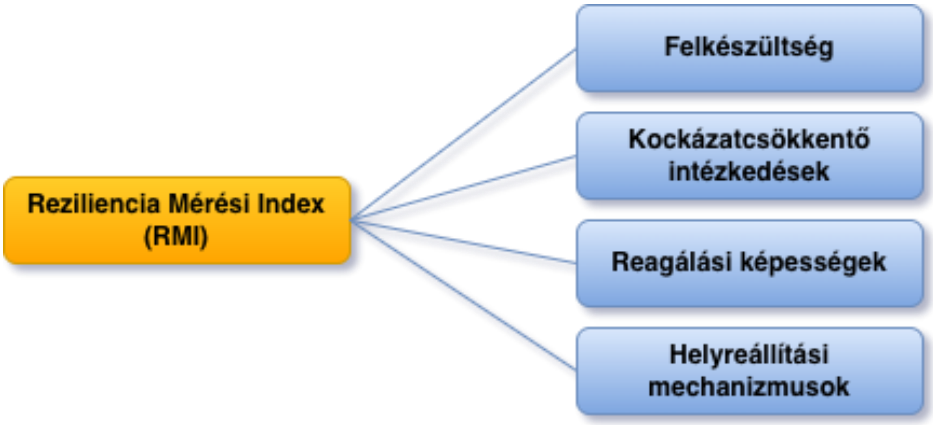
A MANIPULÁCIÓ HATÁSA AZ INFORMATIKAI RENDSZEREK BIZTONSÁGÁRA

A pszichológiai manipuláció nem csupán elszigetelt incidens, hanem olyan rendszerszintű fenyegetés, amely az informatikai architektúra alapvető biztonsági pilléreit támadja. A pszichológiai manipuláció alapú támadások jelentősége abban rejlik, hogy képesek megkerülni a korszerű technikai védelmi rendszereket is, mivel nem a szoftveres sebezhetőségeket, hanem a humán interakciók bizalmi láncát kompromittálják [14].

Incidenskezelési aspektusok és észlelési nehézségek

Az incidenskezelés során a pszichológiai manipuláció alapú behatolások azonosítása jelenti a legnagyobb kihívást. Mivel a támadók sikeres manipuláció révén érvényes felhasználói hitelesítő adatokat szereznek, tevékenységük a hagyományos behatolásjelző rendszerek számára legitim felhasználói viselkedésnek tűnhet [15]. Az észlelés elhúzódása kritikus kockázatot jelent a kritikus infrastruktúrákban, ahol a válaszadási idő minimalizálása alapvető fontosságú az üzletmenet-folytonosság szempontjából [5], [9].

A modern észlelési stratégiáknak ezért túl kell lépniük a statikus szabályokon, és olyan vizualizációs eszközöket vagy viselkedéselemző algoritmusokat kell alkalmazniuk, amelyek képesek az anomáliák felismerésére a *felhasználó–forrás–célpont* triász mentén [15]. A kritikus infrastruktúrák ellenálló képességének mérésekor a Reziliencia Mérési Index (Resilience Measurement Index - RMI) alkalmazása elengedhetetlen, amely a felkészültséget, a mérséklési intézkedéseket, valamint a válaszadási és helyreállítási képességeket összesíti (lásd: 2. ábra). A pszichológiai manipuláció közvetlenül rontja ezeket a mutatókat, mivel a humán sebezhetőség gyengíti a megelőző kontrollok hatékonyságát, így növelve a rendszer helyreállítási idejét és költségeit.

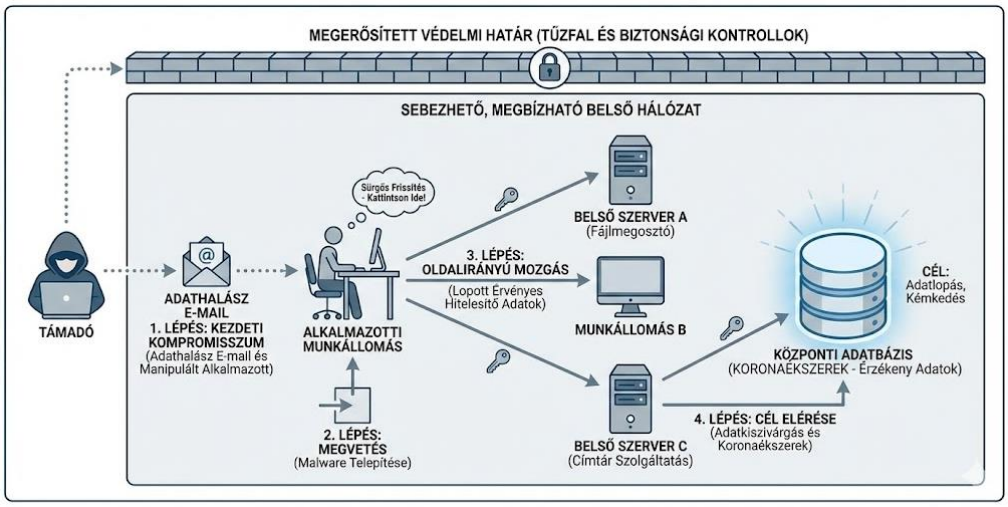


2. ábra - A Rezlliencia Mérési Index (RMI) 1. szintű összetevői (saját szerkesztés) [17]

Hálózati integritás és laterális mozgás

A hálózati integritás szempontjából egyetlen manipulált munkavállaló a teljes rendszer kompromittálódásának forrásává válhat. A pszichológiai manipulációs támadások során az áldozat nem csupán adatokat ad át, hanem egy „hídfőállást" (foothold) biztosít a támadónak a belső hálózaton [15]. A laterális mozgás (lateral movement) fázisában a támadó már nem kívülről próbál áttörni a tűzfalon, hanem a megszerzett, legitimnek tűnő jogosultságokkal „belülről" navigál az erőforrások között - ahogyan ezt a 3. ábra is mutatja.

Siadati és munkatársai rámutatnak, hogy az észlelés kulcsa a kontextuális anomáliák figyelése: ha egy legitim felhasználó szokatlan forrásból szokatlan célpontot próbál elérni, az laterális mozgásra utal [15]. A pszichológiai manipuláció taxonómiája szerint a támadók rétegzett módszereket alkalmaznak a jogosultságok kiterjesztésére, szisztematikusan kihasználva a hálózati szegmentáció hiányosságait [14].



3. ábra - A manipuláció alapú behatolás és a laterális mozgás folyamata a vállalati hálózatban
Forrás: Saját szerkesztés Zaoui et al. [14] és Siadati et al. [15] alapján

Adatbiztonság, üzleti folytonosság és megtérülés (ROSI)

A manipulációból eredő adatvesztés hatásai messze túlmutatnak a közvetlen gazdasági károkon. A szervezeti bizalom elvesztése – mind belső, mind külső, ügyféloldali szempontból - olyan immateriális kár, amely hosszú távon veszélyezteti a piaci pozíciót. A menedzsment számára a legnagyobb kihívást az jelenti, hogy a technikai védelembe fektetett tőke nem hoz arányos megtérülést, ha a humán faktor tudatossága és rezilienciája elmarad a fenyegetettségi szinttől .

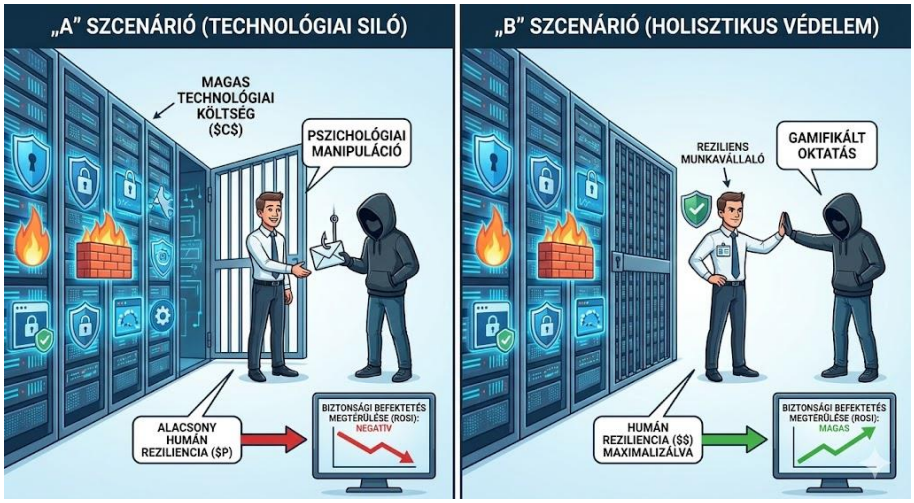
A kiberbiztonsági beruházások gazdasági racionalitása a biztonsági befektetések megtérülési mutatójával (Return on Security Investment - ROSI) szemléltethető legpontosabban, amely figyelembe veszi a védelmi intézkedések kockázatcsökkentő hatását:

$$ROSI = \frac{(ALE \times P) - C}{C}$$

A képletben az **ALE** (Annual Loss Expectancy) az éves várható veszteséget jelöli, a **C** a védekezés költsége, míg a **P** (Mitigation Factor) a védelmi intézkedés - jelen esetben a humán reziliencia-fejlesztés - hatékonyságát mutatja.

Amennyiben a munkavállalók manipulálhatósága miatt a P értéke alacsony marad (például a felejtési görbe miatt a hagyományos oktatás után), úgy a technikai eszközökbe fektetett tőke megtérülése is romlik. A gamifikált oktatás gazdasági előnye éppen a P tényező időbeli stabilizálásában rejlik: az élményalapú tanulás mélyebb memórianyomokat hagy, így a védekezés hatékonysága hosszabb távon is magas marad, javítva a ROSI mutatót (lásd: 4. ábra).

A NIS2 irányelv értelmében a kiberbiztonsági kockázatkezelésnek ki kell terjednie a teljes ellátási láncra, felismerve, hogy a manipuláció nemcsak a belső állományt, hanem a beszállítókat és partnereket is célba veheti [3].



4. ábra - A biztonsági befektetések megtérülésének (ROSI) összefüggései a humán faktor függvényében
Forrás: Saját szerkesztés Kostic [16] alapján

A GAMIFIKÁLT TANULÁSI KÖRNYEZETEK SZEREPE A PREVENCIÓBAN

A kiberbiztonsági tudatosság növelésének egyik akadálya a hagyományos, frontális oktatási módszerek használata, amely ritkán vezet tartós viselkedésváltozáshoz [13]. Ezzel szemben a gamifikáció és a játékalapú tanulás (Game-Based Learning - GBL) olyan innovatív megközelítést kínál, amely a tanulást kötelezettség helyett élménnyé alakítja. A módszertan pedagógiai alapjai John Dewey tapasztalati tanulásról alkotott nézeteire és Csíkszentmihályi Mihály flow-elméletére vezethetők vissza. A flow-állapotban a tanuló annyira elmélyed a tevékenységben, hogy a tanulás érdekessé és kihívást jelentővé válik, a nehézségek pedig nem elriasztják, hanem megoldásra inspirálják.

A tapasztalati tanulás és a biztonságtudatosság

A gamifikált környezetek, így a mesterséges intelligencia (MI) alapú szimulációk vagy virtuális valóság tréningek, valós idejű visszacsatolást biztosítanak a tanulóknak, lehetővé téve a pszichológiai manipulációs támadások mechanizmusainak biztonságos megtapasztalását. A kutatások igazolják a módszer hatékonyságát: míg a képzetlen személyzet körében a manipuláció sikerességi aránya elérheti az 58–64%-ot, addig a célzott tréningek után ez az arány 19–20%-ra csökkenthető.

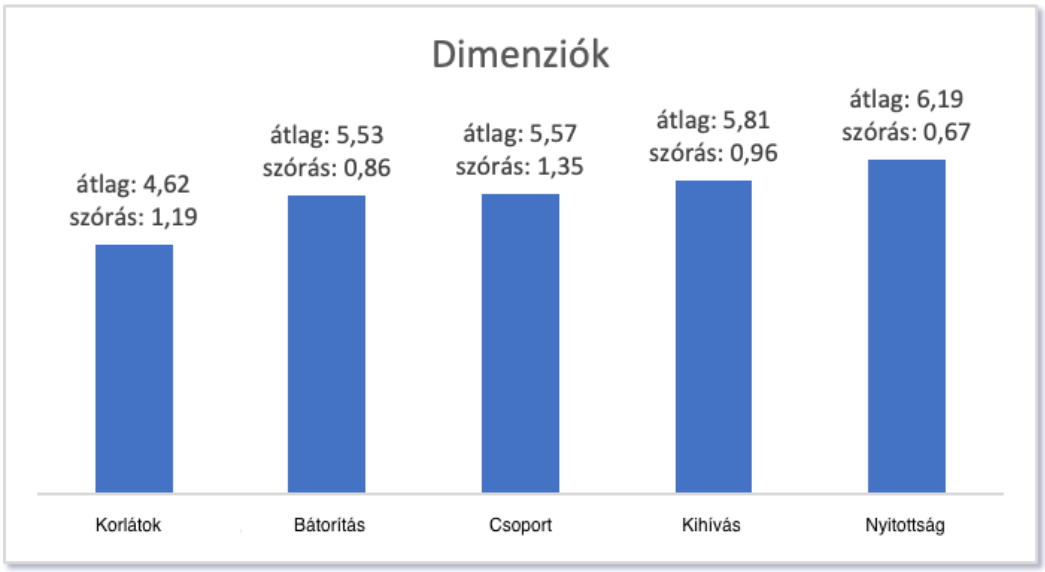
A játék elemei – többek között a pontrendszerek és ranglisták – fenntartják a motivációt és ösztönzik az analitikus (2-es típusú) gondolkodás aktiválását kritikus helyzetekben. A gamifikáció hatása közvetlenül mérhető a korábban bemutatott ROSI képlet P (mérséklési tényező) elemében is. A tapasztalati tanulás során a munkavállaló aktív részese lesz a védelmi folyamatnak, így képessé válik az olyan kognitív torzítások korrigálására, mint az optimizmus-torzítás vagy a tekintélynek való automatikus engedelmesség.

A Minecraft, mint a komplex rendszerek modellezésének eszköze

A Minecraft „sandbox” típusú videojáték kiváló platformot biztosít a biztonságtechnikai ismeretek és a kritikus infrastruktúrák védelmének oktatásához. A szoftver módosításával (esetünkben 50–60 speciális „mod” használatával) a valósághoz hű szimulációk hozhatók létre, ahol a résztvevők intelligens épületeket, megújuló energiaforrásokat vagy objektumvédelmi rendszereket tervezhetnek és üzemeltethetnek.

A kutatásunk egyik legfontosabb megállapítása, hogy a Minecraft-ban végzett erőforrás-menedzsment és a logikai áramkörök építése **kognitív lassítást** eredményez. Ez a mentális állapot homlokegyenest ellentétes azzal a „sürgetett” állapottal, amit az adathalász támadások igyekeznek előidézni. A játék során a felhasználók megtanulják vizuálisan azonosítani az anomáliákat a térben, ami transzferálható képességként jelenik meg a hálózati log-ok vagy e-mail fejlécek vizuális ellenőrzésekor.

Az oktatási kísérleteink során a résztvevők 55,6%-a számolt be a problémamegoldó képesség szubjektív fejlődéséről. Bár ez önbevalláson alapuló adat, a kompetenciaérzet növekedése (self-efficacy) pozitív korrelációt mutat a valós biztonságtudatos viselkedéssel, mivel a magabiztosabb felhasználó kevésbé hajlamos a pánikszerű (1. rendszer) reakciókra egy incidens során (lásd: 5. ábra). A gamifikált módszer előnye, hogy a tanulók büntetlenül hibázhatnak a virtuális térben, miközben megtapasztalják döntéseik súlyát és a biztonsági protokollok betartásának jelentőségét.



5. ábra - A gamifikált tanulási környezet kreatív klímájának dimenziói
Forrás: Saját szerkesztés Holik et al. [20] és Kersánszki et al. [21, 22] alapján

ÖSSZEGZÉS

A kutatás rávilágított arra, hogy a pszichológiai manipuláció nem elszigetelt incidensek sorozata, hanem olyan rendszerszintű fenyegetés, amely az informatikai architektúra humán bizalmi láncát kompromittálja [14]. A kognitív kettős folyamat elmélet alkalmazásával bizonyítottuk, hogy a támadók módszeresen az intuitív, érzelemalapú „1. rendszert" aktiválják, ezzel iktatva ki a logikus és analitikus kontrollt végző „2. rendszert" [10].

A menedzsment számára kritikus felismerés, hogy a technikai védelembe fektetett tőke megtérülése (ROSI) drasztikusan romlik, ha a humán faktor mérséklési képessége (P) alacsony marad. A tanulmányban bemutatott összefüggés rávilágít arra, hogy a biztonságtudatosság nem csupán elméleti elvárás, hanem gazdasági és üzletmenet-folytonossági kényszer.

A hagyományos, statikus oktatási módszerek kudarca után a játékalapú tanulás (Game-Based Learning) és a Minecraft-alapú szimulációk új utat mutatnak a prevencióban. Az empirikus eredmények igazolták, hogy a gamifikált környezetben végzett tréningek hatására a manipuláció sikerességi aránya szignifikánsan csökkenthető. Zárásként megállapítható, hogy a NIS2 irányelvnek való megfelelés és a kritikus infrastruktúrák védelme megköveteli a proaktív biztonsági kultúra kialakítását. A humán reziliencia ily módon a modern kiberbiztonsági stratégia megkerülhetetlen pillérévé válik.

FELHASZNÁLT IRODALOM

[1] A. Bodáné Kendelényi, "Kiberbiztonság menedzseri szemmel," oktatási segédanyag, Nemzeti Közszolgálati Egyetem, Budapest, 2023.
[2] Cs. Kollár, "A biztonság megjelenése a humán tudományokban (3. rész)," Biztonságtudományi Szemle, vol. 6, no. 4, pp. 1–14, 2024, doi: 10.12700/btsz.2024.6.4.1.

[3] Á. Kiss and Cs. Kollár, "Az információbiztonság időszerű kérdései a magyarországi kkv-k körében," Scientia et Securitas, vol. 4, no. 2, pp. 98–107, 2023, doi: 10.1556/112.2023.00010.
[4] Z. Németh and Z. Völgyi, "A kritikus információs infrastruktúra védelem pszichológiai szempontú megközelítése (Humán biztonsági kockázatelemzés)," Hadtudományi Szemle, vol. 11, no. 3, pp. 324–337, 2018.
[5] M. Kis, A. Bódi, and R. Számadó, "A NIS2 hazai bevezetésének folyamata és kockázatai," Hadmérnök, vol. 19, no. 3, pp. 115–130, 2024, doi: 10.32567/hm.2024.3.8.
[6] I. Jagodics and Cs. Kollár, "21. századi social engineering támadások, védekezés és szervezeti hatások Európában," Belügyi Szemle, vol. 71, no. 1, pp. 115–134, 2023, doi: 10.38146/BSZ.2023.1.7.
[7] L. Kovács, „Kibervédelmi kihívások a közszolgálat személyi állományában," Publikáció, 2024.
[8] Z. Szabó, „Az emberi tényező szerepe az információbiztonság megvalósítása és erősítése terén. Az információbiztonsági kultúra fejlesztésének lehetőségei a Magyar Honvédségben," doktori értekezés, 2023.
[9] V. Greavu-Şerban, F. Constantin, and S.-C. Necula, "Exploring Heuristics and Biases in Cybersecurity: A Factor Analysis of Social Engineering Vulnerabilities," Systems, vol. 13, no. 4, art. no. 280, Apr. 2025, doi: 10.3390/systems13040280.
[10] F. Bano, M. A. Ghazanfar, and A. Alqahtani, "Understanding Social Engineering Through the Lens of Human Cognition: A Systematic Literature Review," IEEE Access, vol. 12, pp. 11046–11062, 2024, doi: 10.1109/ACCESS.2024.3353456.
[11] M. K. Alshaikh, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—A Systematic Literature Review," IEEE Access, vol. 11, pp. 113327–113345, 2023, doi: 10.1109/ACCESS.2023.3323490.
[12] I. Ghafir, J. Saleem, M. Hammoudeh, et al., "Security threats to critical infrastructure: the human factor," The Journal of Supercomputing, vol. 74, no. 10, pp. 4986–5002, Oct. 2018, doi: 10.1007/s11227-018-2337-2.
[13] S. Uebelacker and S. Quiel, "The Social Engineering Personality Framework," in 2014 Fourth International Workshop on Socio-Technical Aspects in Security and Trust (STAST), Vienna, Austria, 2014, pp. 24–30, doi: 10.1109/STAST.2014.12.
[14] M. Zaoui, Y. Belfaik, Y. Sadqi, Y. Maleh, and A. Mamouni, "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies," IEEE Access, vol. 12, pp. 72224–72241, 2024, doi: 10.1109/ACCESS.2024.3403197.
[15] H. Siadati, B. Saket, and N. Memon, "Detecting Malicious Logins in Enterprise Networks Using Visualization," in 2016 IEEE Symposium on Visualization for Cyber Security (VizSec), Baltimore, MD, USA, 2016, pp. 1–8, doi: 10.1109/VIZSEC.2016.7739582.
[16] L. C. Kostic, "Information Security Awareness Techniques that Reduce Data Breaches Caused by Social Engineering Attacks." Order No. 27832769, Capella University, United States -- Minnesota, 2020.
[17] F. D. P. Petit, G. W. Bassett, R. Black, et al., "Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience," Argonne National Laboratory, Argonne, IL, USA, Tech. Rep. ANL/DIS-13-1, Apr. 2013, doi: 10.2172/1087819.

[18] Z. Rajnai, L. Berek, and Z. Márton, „Social engineering az objektum-védelemben: a biztonsági személyzet befolyásolhatóságának vizsgálata," Biztonságtudományi Szemle, vol. 7, no. 1, pp. 95–106, 2025, doi: 10.12700/btsz.2025.7.1.95.
[19] Z. Márton and Z. Rajnai, „A social engineering fejlődése és jövője: a pszichológiai sebezhetőségek kihasználása a digitális korban," Biztonságtudományi Szemle, vol. 6, no. 4, pp. 45–56, 2024, doi: 10.12700/btsz.2024.6.4.45.
[20] I. Holik, T. Kersánszki, I. D. Sanda, and Z. Márton, "Improving Security and Environmental Awareness through Game-Based Learning with Minecraft", Int. J. Eng. Ped., vol. 14, no. 4, pp. pp. 90–107, May 2024.
[21] T. Kersánszki, Z. Márton, K. Fenyvesi, Z. Lavicza, and I. Holik, „Implementation of Minecraft in Education to Introduce Sustainable Development Goals: Approaching Renewable Energy Through Game-Based Learning," in Smart Learning Ecosystems as Engines of the Green and Digital Transition, M. Dascalu, Ó. Mealha, and S. Virkus, Eds. Singapore: Springer, 2023, pp. 219–232, doi: 10.1007/978-981-99-5540-4_13.
[22] T. Kersánszki, I. Holik, and Z. Márton, "Minecraft Game as a New Opportunity for Teaching Renewable Energy Topics", Int. J. Eng. Ped., vol. 13, no. 5, pp. pp. 16–29, Jul. 2023.

DOI: https://doi.org/10.12700/btsz.2026.8.1.23

SOME ASPECTS OF HEALTHCARE CRISIS PLANNING

AZ EGÉSZSÉGÜGYI VÁLSÁGHELYZETI TERVEZÉS EGYES ASPEKTUSAI

NAGY Rudolf [1]

Abstract

Preparing for emergency response requires more effective methods and easily mobilizable infrastructure on the part of healthcare organizations. Therefore, specially developed capabilities, as well as integrated care systems featuring a large number of medical devices due to increased demand for care and infrastructure elements with expanded functions, serve the purposes of transitioning to a special legal regime. As a result, any threat with territorial implications must be dealt with in a fundamentally unified organizational order, involving all available health resources. Therefore, existing reserves, infrastructure capacity, service providers, and professional staff in all affected areas must be integrated in a coordinated manner into health crisis planning.

Keywords

emergency situation, healthcare, special legal order, crisis situation, planning

Absztrakt

A veszélyhelyzeti reagálásra történő felkészülés hatékonyabb módszereket és könnyen mobilizálható infrastruktúrát kíván az egészségügyi szervezetek részéről. Ezért speciálisan kialakított képességeket, valamint a nagyobb ellátási igény okozta nagyszámú orvostechnikai eszközt, illetőleg kibővített funkcióval ellátott infrastruktúra elemeket felvonultató integrált ellátó rendszerek szolgálják a különleges jogrendi állapotra való átállás céljai. Ezeknek köszönhetően bármely területi hatállyal párosuló fenyegetettség kérdését alapvetően egységes szervezeti rendben kell kezelni, valamennyi rendelkezésre álló egészségügyi erőforrás bevonásával. Tehát minden érintett területen meglévőtartalékot, infrastrukturális képességet és szolgáltatót, valamint szakszemélyzetet az egészségügyi válsághelyzeti tervezésben összehangoltan kell integrálni.

Kulcsszavak

veszélyhelyzet, egészségügyi ellátás, különleges jogrend, válsághelyzet, tervezés

[1] nagy.rudolf@uni-obuda.hu | ORCID: 0000-0001-5108-9728 | habilitated associate professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary | habilitált docens, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A védelmi és biztonsági igazgatás alapvetően koordinációs tevékenység lévén, a különleges jogrendi helyzetek kapcsolatos események kezelésének kérdéskörét az ország biztonságát fenyegető veszélyekkel szembeni védelem megszervezése során játszott, sajátos válságkezelési szerepéből kiindulva közelíti meg. A válságok téren a lakosság közegészségügyi eredetű fenyegetettségére és a katasztrófák egészségügyi következményeinek kihívásaira adott válaszok mind minőségében, mind pedig feltételrendszerében speciálisnak mondhatóak más ágazatok szerepköréhez viszonyítva.

Ezen összefüggések vizsgálata során világosan látható, hogy a válságok, veszélyhelyzetek és krízisek egészségügyi hatásai elleni védekezés hatékonyságát befolyásoló tényezők között meghatározó tényező a reagálási idő. A fejlett országokban például a közegészségügyi szakigazgatás igen komoly és nagyhatékonyságú preventív intézkedéseinek köszönhetően a járványterjedést befolyásoló folyamatok súlyos kimenetelű lezajlásához a legpesszimistább forgatókönyveket is figyelembe véve hetek kellenek. Ellenben a hasonlóan komoly egészségügyi ellátási problémákkal járható katasztrófaesemények hatásténye-zői a szcenáriók eszkalációs dinamikáját lényegesen megváltoztató körülményekkel párosulva ennek töredékét igénylő idő alatt is előállhatnak.

Azonban védelmi és biztonsági igazgatás oldaláról nézve az egészségügyi veszélyhelyzetekkel kapcsolatos válságreagálás elkülönült felelősséggel és hatáskörrel rendelkező ágazati kompetenciák mentén valósul meg. Az intézményi szféra alapvetően a reagálást valamennyi szervezeti szinten az eredeti vezetés, irányítás szerepkörét betöltő személyi kör bevonásával felállított válságmenedzsment megszervezésével oldja meg. Így a jogszabályok által nevesített veszélyeket magában hordozó események bekövetkezésére reagáló és a hatáskörrel rendelkező miniszter által kijelölt egészségügyi ellátó intézmény általában köteles saját egészségügyi válsághelyzeti felkészülése keretében plusz kapacitást képességet és ezekhez társuló feltételrendszert is tervesíteni. Ezt eszkaláció esetén a megnövekedett ellátási igényeket normálidőszaki reagálásra felkészített saját állománnyal és eseti jelleggel az egészségügyi szolgálati jogviszony adta kirendelésekkel pótlandó szakszemélyzettel elégítik ki. Végső esetben a különleges jogrendi helyzetekben bevezethető anyagi és gazdasági szolgáltatási kötelezettség magán egészségügyi szolgáltatókra történő kiterjesztésével felszabadítható további humánerőforrást is bevonhatnak. [1]

A felvázoltakból kitűnik, hogy a hazai egészségügyi válságkezelés rendszere és a gyakran üzleti életben meghonosodott üzletmenetfolytonosságra kiélezett rendszerek filozófiája alapvetően eltérő. Az első a külső társadalmi rendkívüli ellátási igényektől befolyásolt, míg a másik ellenben a belső profitorientált kényszerítő hatásoktól vezérelt. Vagyis az egészségügyi válsághelyzetek kezelésére kialakított rendszer a nemzeti érdekek mentén és azok egészére kiterjesztve vizsgálja a különleges jogrendi helyzeteket. Ennek középpontjában a Kormány és a végrehajtó államapparátus költségvetési szervekre támaszkodhat elsősorban, kiegészítve a válságreagálás tartalékait képező erőforrásaival a gazdasági és anyagi szolgáltatási kötelezettség vonatkozásában. Az egészségügyi válsághelyzeti ellátás jelentkező feladatok megvalósítására a kormányhivataloknak és az egészségügyi államigazgatási szervnek, valamint a védelmi és biztonsági igazgatásnak a közigazgatás rendszerében betöltött szerepük átfedéseiből kiindulva nyílhat mód.

VÁLSÁGREAGÁLÁS EGÉSZSÉGÜGYI VETÜLETEI

A válságreagálási tevékenységének szélesedése tükrében az egészségügyi veszélyhelyzeti tervezés és válságkezelés során megvalósuló szervezett védelmi együttműködés jelentősége a COVID-járványt követően különösen felértékelődött. Az állam szervezete fontos lépéseket tett az ezen új igényeket is kielégítő válságreagálási rendszerek létrehozásának irányába. [2]

A rendkívüli helyzetekben aktivizálandó védelmi és biztonsági igazgatás válsághelyzeti funkciói a fegyveres és rendvédelmi intézkedések mellett egyre jelentősebb mértékű polgári válságkezelési teendőket is tartalmaznak. Ez annak is betudható, hogy egyfelöl a társadalom fenyegetettségét jelentő kihívásokkal szembeni események kezelése céljából történő rendvédelmi fellépés során a biztonság megteremtése szinte minden esetben együtt járnak az egészségügyi képességekkel történő támogatás igénybevételével. Elég hacsak a migrációhoz köthető járványügyi kockázatok kezelésének kérdését vesszük.

Másfelöl a közbiztonság, környezetbiztosság helyreállítására kialakított válaszreagálási rendszer feladata, hogy a veszélyhelyzetek megkövetelte válaszintézkedések érdekében az államigazgatás különleges működési rendre való átállításával szavatolja a lakosság élet- és vagyonvédelmének hatékony megszervezését.

A feladatok inverz vetülete, hogy az ország, vármegye és település egészségügyi válság sújtotta lakossága ellátásbiztonsága fenntartása érdekében a védelmi és biztonsági igazgatás rendszere kapacitásaival támogatást nyújtson a bekövetkező egészségügyi krízisek kezelésében. Az egészségügyi átmeneti diszfunkciók felszámolása érdekében veszélyhelyzetben nyújtandó támogatás érdekében a védelmi és biztonsági igazgatás szerveinek is tervezniük kell képességeikkel az egészségügyi válsághelyzetekben jelentkezhető infrastrukturális károk és működési zavarok elhárítását szolgáló közreműködésük érdekében. Az egészségügyi válsághelyzetek felszámolásában a tartalékkapacitások bevonása kapcsán központi szinten is az induló készletek kiegészítésének alapelvét alkalmazzák. Azaz ilyen körülmények között az átcsoportosított képességek, támogatások csupán az egészségügyi oldal részéről támasztott igénynek történő megfelelésre kell szorítkoznia. Az ezen feladatok megoldását szolgáló válságkezelés szervezeti hatása egyik eredményeként valamennyi érintett intézményben készenlétbe helyezik az operatív működés strukturális elemeit.

Az egészségügyi válsághelyzetek kezelésére meghozott ideiglenes intézményi intézkedések abból az alapvető tényből indulnak ki, hogy az orvosszakmai kihívásokkal összhangban nem csak az ellátásbiztonság megingásának veszélye, de a működésbiztonság szempontjából kedvezőtlen, egyenlőtlen személyi leterheltséget okozható túlmunka miatti változások nagyságrendje is fokozódik. Az ezekhez köthető kérdéskörök kezelése felöleli valamennyi szervezeti egység egészségügyi szakállományát.

Az ezen komplex megközelítés ellenére fennmaradó, le nem fedett képességekhez társulnak a kihirdetett veszélyhelyzeti intézkedési jogkörök alkalmazásával felszabadítható többletkapacitások. [3] Ez a kifejezetten csak az egészségügyi válsághelyzeti intézkedésekhez kötődő, valamint az annak koordinációjának tárgyhoz tartozó kérdés köröket kell az egészségügyi válsághelyzeti tervezés során azonosítani és a védelmi és biztonsági igazgatás rendszerében kezelni.

Azonban tekintettel arra, hogy a rendkívüli jogrendi helyzetek adta felhatalmazás alapján megvalósítandó intézkedések fogalmi vonatkozásban a válságkezelés a haváriától kezdve, a katasztrófán át a terrorcselekményekig stb. terjedő különféle krízíseket ölelhetnek

fel, ezek egy sor egymást átfedő feladatrendszert takarhatnak. Ezek számos jogi és eljárási problémát vethetnek fel, melyekről első közelítésben azt kell feltételezni, hogy a békeidőszaki rendben is létező és működtetett egészségügyi intézmények oldják meg a feladatok nagy részét. Ehhez társulnak a tervezéshez kiadott szempontrendszer szerint felálló többletkapacitásokat keletkeztető intézményi elemek vagy az eseti intézkedések nyomán létesülő ideiglenes ellátást biztosítani képes infrastrukturális létesítmények, mint például a COVID pandémia alkalmával létesült járványkórház.

Különleges jogrend, mint vonatkoztatási alapmérték

A jogalkotó az ország biztonságának szavatolására törvényben [4] is deklarált módon nemzeti ügyként tekint. Ezt az alapelvet követve az idevonatkozó egészség-ügyi válságok elleni fellépés kérdését sem háríthatja a végrehajtó hatalmat gyakorló Kormányzat kizárólag az egészségügyi intézmény-rendszerre. Ezért az elv megvalósulásának biztosítéka, hogy nem csak az egészségügyi államigazgatási szerv, hanem a védelmi és biztonsági igazgatás rendszerével karöltve a válsághelyzetek kezelésének minden érintett szereplőjét össztársadalmi szinten aktivizálják a sikeres válaszintézkedések realizálása érdekében.

A rendszer alapvetően a válsághelyzetekre történő reagálásban az alulról fel-felé építkezve biztosítja a fokozatosság, illetve az arányos és elégséges beavatkozás feltételeit, követve a válsághelyzetek lehetséges eszkalációjának folyamatát.

A válságkezelési feladatok megoldásához a jogalapot elsődlegesen az Alap-törvényben, másodsorban az egyéb jogi kereteket szabályozó törvényekben lefekte-tettek teremtik meg. A következmények kezelésének a veszélyhelyzeti szolgálatok forrásain felül jelentkező többlet szükségleteit, valamint pénzügyi hátterét az Alap-törvényben definiált különleges jogrend bevezetésével megnyíló tartalékok adják. Az Alaptörvény az állam és állappolgárai biztonságát veszélyeztető körülmények fel-számolását szolgáló különleges jogrendi működésének jogintézményeiként nevesíti:

- hadiállapot;
- szükségállapot;
- veszélyhelyzet. [5]

EGÉSZSÉGÜGYI VÁLSÁG ÉS KÜLÖNLEGES JOGREND

Az egészségügyi válságkezelés olyan összetett feladat, amely védelmi és biztonsági igazgatási, adminisztratív és lakosságtájékoztatási aktusoktól kezdve egészen a rendkívüli működésre való áttérésig terjed. Az ezen kategóriába sorolt, a lakosságot vagy magát az egészségügyi ellátó rendszert fenyegető eseményekkel összefüggésben kihirdethető időszakok a különleges jogrend eszközeit igénybe véve biztosítanak a jogszabályban nevesített védelmi igazgatási vezető részére kellő hatáskört és hatékony döntéshozatali mechanizmust. A vonatkozó törvényi rendelkezések emellett egyben megszabják a szükséges korlátokat és az alkotmányos kontroll mikéntjét. Ezekhez kapcsolódóan az egészségügyi ellátó rendszer működtetésében az alábbi válságreagálási alternatívákkal számolhatunk:

- egészségügyi veszélyhelyzet (katasztrófaveszély indokolta egészségügyi feladatok);
- egészségügyi válsághelyzet (járványügyi szükséghelyzet, katasztrófa vagy egyéb különleges jogrendi állapot).

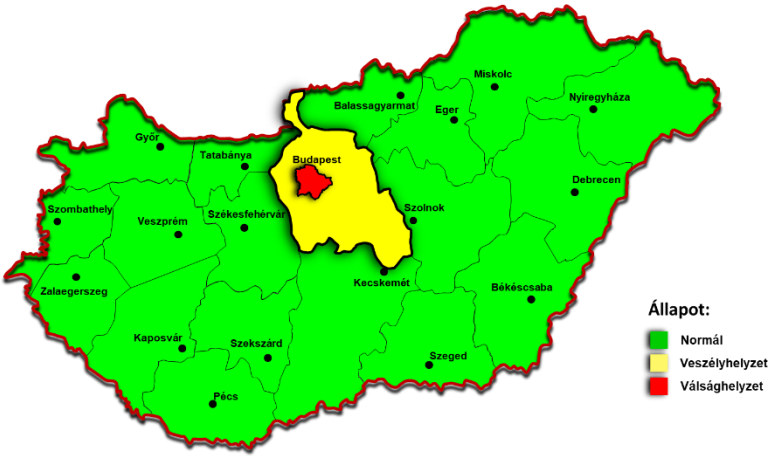
Előbbi az ellátásbiztonság fenntartása végett eszközölt, maximum 10 napig fenntartható megelőző állapotot takar, a várható katasztrófa egyészségügyi feladataira történő felkészülést szolgálja. Akár átmenetet is képezhet az egészségügyi válsághelyzetre való áttéréshez. Utóbbi pedig már ténylegesen kihirdetett különleges jogrendi körülmények egészségügyi ellátás feltételeit hivatottak garantálni.

1. ábra: Egészségügyi válságreagálás szintjei.
Forrás: Szerkesztette a szerző

Mind az egészségügyi válságkezeléshez köthetően az alaptörvényből levezethető módon az egészségügyi ellátórendszer reagálásának mindkét az 1. ábrán megjelölt esetében lehetőséget teremt a közigazgatás normál jogrend szerinti reagálásán túlmutató válaszintézkedések megtételére. Ugyanakkor akár elkülönülten, akár egymást követően kerülnek bevezetésre szavatolják az az egészségügyi válsághelyzet vagy egyéb védelemegészségügyi reagálásnál alkalmazott fokozatosság elvének érvényesülését is. Mivel az egészségügyi válsághelyzeti tervezésben meghatározott feladatok akár részlegesen is életbe léptethetők. Így egy készenléti helyzetet meghaladó méretű súlyosabb különleges jogrend kihirdetésével járó esemény esetén további, a reagálás és annak különböző fokozatai léptethetők életbe.

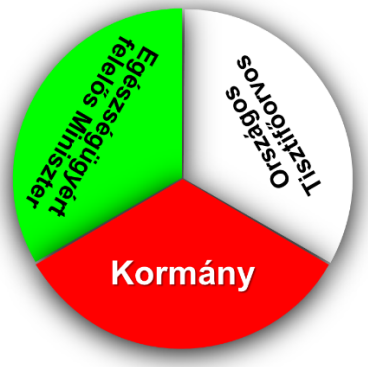
2. ábra: Az egészségügyi válsághelyzetek lehetséges kiváltó okai.
Forrás: Szerkesztette a szerző

A vonatkozó felhatalmazó rendelkezések is ezt a fokozatosságot erősítik. Első, katasztrófaveszély [6] állapotához társítható egészségügyi veszélyhelyzet esetben a kihirdetésre jogosult a fővárosi és vármegyei kormányhivatal. A kihirdethet egészségügyi veszélyhelyzetről „haladéktalanul értesíteni szükséges a minisztert, illetve az országos tisztifőorvost". [3] Az egyben azt is jelenti, hogy ennek kihirdetése lehetséges csupán akárcsak az ország egyetlen egy területi közigazgatási egységét jelentő valamely vármegyére, amint azt a 3. ábra szemlélteti. Vagy közigazgatási egységenként eltérő jogrendi helyzet is életbe léptethető.



3. ábra: Egészségügyi veszélyhelyzet területi hatályának tartalma.
Forrás: Szerkesztette a szerző

Amennyiben bevezetett rendelkezéseivel nem érhető el a helyzet konszolidálása, úgy a Kormány [7] kihirdetheti az egészségügyi válsághelyzetet vagy különleges jogrend bevezetésével egyidejűleg dönt az egészségügyi válsághelyzeti intézkedések végre-hajtásáról külön proklamált egészségügyi válsághelyzet nélkül. Normál eljárásrend-ben az egészségügyi válsághelyzet bevezetésére az országos tisztifőorvos tesz javas-latot és az egészségügyi miniszter előterjesztése nyomán a Kormány hirdeti ki.



4. ábra: Az egészségügyi válsághelyzetek személyi felelősségi körei.
Forrás: Szerkesztette a szerző

A TERVEZÉS ALAPPILLÉREI

A lakosság egészségügyi válsághelyzeti ellátása minden helyzetben átfogóan - az állami egészségügyi intézmények és a lehetőségek függvényében magán egészségügyi szolgáltatók stb. feladata. A helyi egészségügyi intézményektől és létesítményektől függetlenül felállíthatók szükséggyógyintézetek, szükségkórházak, vagy járványkórházak is.

Egészségügyi válsághelyzetben, katasztrófák bekövetkezésekor – tömegesen jelentkező beteg vagy sérült ellátásának szükségessége esetén - ha korlátozott mértékben is a sérültek ellátásában az egészségügyi szolgáltatók intézményei, de akár rendelőintézeti szakrendelők stb. is részt vesznek.

A válsághelyzeti ellátás tervezésének felügyeletét szakmai oldalról a szabályozás a vármegyei kormányhivatalok szervezetében található népegészségügyi fő-osztályok tevékenységi körébe utalja. A vonatkozó kormányrendelet egészségügyért felelős miniszterhez [8] telepíti az igénybe vehető intézmények tervezési feladatainak meghatározását. Ehhez kapcsolódva a szabályozási keretek megteremtik a tömeges sérültellátáshoz járványügyi védekezéshez, illetőleg egyéb válsághelyzetekben szükséges ellátási és ápolási feltételeket, ideértve akár a tömeges migráció következtében jelentkezhető egészségügyi veszélyek okozta fenyegetettség kezelésének fel-tételeit is.

Kétségtelen tény azonban, hogy egészségügyi válsághelyzetet nem csak az áldozatok nagy száma miatti túlterhelés vagy átmeneti kapacitás hiány jelenthet. Az egészségügyi intézménynek magának a működését veszélyeztető diszfunkciók is keletkeztethetnek megoldandó válsághelyzeti feladatokat, amely még a teljes intézmény áttelepítését is jelentheti.

Az egészségügyi ellátás zavartalansága nagyban függ a szakorvosi és egyéb szakszemélyzet rendelkezésre állásától vagy orvostechnikai eszközök meglététől. Ezek szükségszerinti kiegészítésére a válsághelyzet adta felhatalmazás nyomán a Kormány rendeleti úton felszabadíthat más kapacitásokat és:

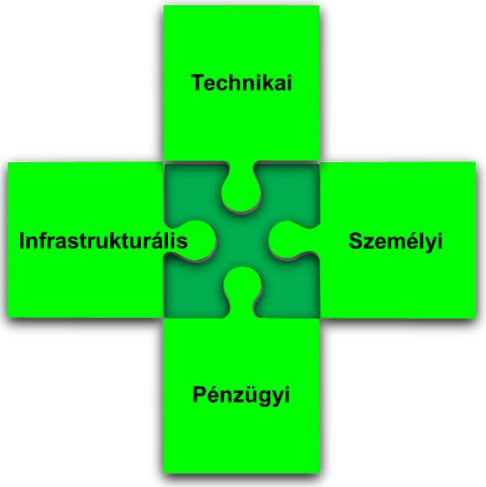
- elrendelheti az egészségügyi szolgáltatók részére a gazdasági és anyagi szolgáltatási kötelezettség teljesítését
- kirendelheti az egészségügyi dolgozókat,
- intézkedik a Magyar Honvédség és a rendvédelmi szervek bevonásáról
- egészségügyi anyag és eszközök felhasználását az Állami Egészségügyi Tartalékból. [9]

Az egészségügyi válsághelyzeti terv elkészítésének és az abban meghatározott feladatok végrehajtásának elsődleges célja a potenciális és egyéb veszélyhelyzetek következményeinek, hatásainak csökkentése, megszűntetése. Továbbá az adott egészségügyi intézményben gyógykezelt betegek és dolgozók életének, anyagi javainak az intézményi ingatlan és ingó vagyontárgyainak védelme, mentése, illetőleg a kialakult rendkívüli helyzetek eszkalációjának megakadályozása, valamint a veszélyhelyzetet követően az eredeti működési állapot visszaállítása a gyógyító tevékenység folyamatos fenntarthatóságának biztosítása mellett.

Az egészségügyi válsághelyzeti terv szolgálja ezen felül a szükséges feltételek megteremtését a kialakult káresemény következményeinek felszámolásában résztvevő szervezetekkel történő együttműködés hatékony megvalósítása érdekében.

A terv alapot képez az egészségügyi intézmény egészségügyi válsághelyzeti reagálásához, az ellátási területén élő lakosságot fenyegető bármilyen civilizációs veszély és

elemi csapás egészségügyi következményeinek felszámolását érdekében, valamint a gyógyító és járóbeteg-ellátó tevékenység rendkívüli események elmúltával történő újra indításához az intézményi anyagi-technikai, pénzügyi és humán, valamint infrastrukturális feltételek megteremtésével, amint azt az 5. ábra illusztrálja.



5. ábra: Alapvető szempontok az egészségügyi válsághelyzeti tervezésben.
Forrás: Szerkesztette a szerző

A tervezés követelményeit – az intézményi sajátosságokhoz igazodva – az egészségügyi válsághelyzeti ellátásról szóló 521/2013. (XII. 30.) Korm. rendelet, továbbá a vonatkozó ágazat rendelet előírásai állapítják meg, melynek felülvizsgálatára évenként a tárgyév március 31-ig kerül sor. [10]

A hatóságilag kötelezett intézmény válsághelyzeti tervezésével kapcsolatos feladatok elrendelése értelmében el kell végeznie részterveinek összeállítását, de az intézményi infrastruktúra bázisán felállítandó szükséggyógyintézet gyanánt, vagy Orvosi Segélyhely kialakítását és működtetésének szervezését, is be kell építenie az Intézmény Egészségügyi Válsághelyzeti Tervébe.

Ehhez megfelelő számban és szakképzettséggel rendelkező egészségügyi személyzetet kell biztosítania a tervbe foglalva. Amennyiben ennek kijelölése meg-történt és az alkalmazási készenlétbe helyezésének elrendeléséhez nem rendelkezik az intézmény megfelelő számban szakszemélyzettel, akkor annak biztosítását kell kezdeményeznie a tervet véleményező egészségügyi hatóság útján a vármegyei védelmi bizottságtól. Kérve más szervezetektől az ellátást végző egészségügyi személyzet válsághelyzeti kirendelését. Ugyan ez vonatkozik a technikai eszközök lebiztosítására is a magán egészségügyi szolgáltatók számára elrendelhető gazdasági és anyagi szolgáltatási kötelezettség teljesítése által.

Ezt hivatottak támogatni az egészségügyi válsághelyzeti tervezés jogilag deklarált követelményei, és csak az így elkészült terv intézkedései léphetők csak életbe, amennyiben biztosítottak annak humán, anyagi, szervezeti és infrastrukturális feltételei. A válsághelyzeti intézkedések tervesítésének alapját képezi a jogszabályilag deklarált fenyegetettségek kockázatainak és a védelmi lehetőségek értékelése és az azokhoz rendelve meglévő vagy más

forrásból biztosítandó képességek, melyeket egyebek mellett az alábbi szempontok szerint célszerű mérlegelni:

- az egészségügyi szolgáltató kapacitásai;
- a válságkezelés célja, szándéka;
- a bevezetendő intézkedések jellege;
- az infrastrukturális paraméterek;
- az orvostechnikai eszközök száma és azok állapota;
- a saját meglévő humán erőforrás létszáma és szakmai képzettsége;
- egyéni védelmi eszközökkel való ellátottság;
- a reagálási képesség, és hatékonyság;
- stb.

KÖVETKEZTETÉSEK

A COVID világjárvány óta az egészségügyi válságkezelésnek és az ahhoz társuló válsághelyzeti tervezésnek kétségtelenül a legfontosabb elemei a lakosság egészségének a védelme és a hasonló járványhelyzetek elleni védekezés tervezése. Azonban ennek elidegeníthetetlen része az egészségügyi ellátó rendszer működőképességének fenntartását szolgáló védelmi és biztonsági igazgatás általi támogatásának a szervezése is.

Az ezt megalapozó tervezés szakasza magában foglalja az olyan elemző, értékelő és koordinációs, valamint együttműködési döntés előkészítő munkát, amely felépíti a gyakorlatban megvalósítható egészségügyi válsághelyzetekre történő reagálás alapjait, kereteit és részleteit.

FELHASZNÁLT IRODALOM

[1] 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről
[2] MÉSZÁROS, I., (2023) A kórház – mint kritikus infrastruktúra – biztonságának aktuális kérdései, Belügyi szemle, Vol. 71, (6), pp. 1059-10727, https://belugyiszemlejournal.org/index.php/belugyiszemle/article/view/1265 , Letöltve: 2026. január 06.
[3] 1997. évi CLIV. törvény az egészségügyről
[4] 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról
[5] Magyarország Alaptörvénye
[6] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
[7] 521/2013. (XII. 30.) Korm. rendelet az egészségügyi válsághelyzeti ellátásról;
[8] 182/2022. (V. 24.) Kormányrendelet a Kormány tagjainak feladat- és hatásköréről;
[9] Major L. (2010) A katasztrófafelszámolás egészségügyi alapjai. Semmelweis Kiadó és Média Kft., ISBN: 9789633311172, 157. o.
[10] 43/2014. (VIII. 19.) EMMI rendelethez az egészségügyi intézmények egészségügyi válsághelyzeti terveinek tartalmi követelményeiről, valamint egyes egészségügyi tárgyú miniszteri rendeletek módosításáról

DOI: https://doi.org/10.12700/btsz.2026.8.1.33

IT EDUCATION CURRICULUM IN HUNGARY AND SLOVAKIA

INFORMATIKAI OKTATÁSI TANANYAG MAGYARORSZÁGON ÉS SZLOVÁKIÁBAN

MANDIĆ Dorottya[1] – KISS Gábor[2]

Abstract

IT plays an increasingly significant role in our everyday lives, as the use of smart devices has become an important part of our lives. Therefore the safe and conscious use of smart devices is becoming increasingly important. Information security education in primary and secondary schools has become essential in a digital society. In the study, we examined whether the IT education curriculum of the two countries includes the development of information security awareness and whether there is a difference between the IT education curriculum and password usage habits.

Keywords

education, IT, information security, smart devices, password usage

Absztrakt

Az informatikának egyre jelentősebb szerepe van a mindennapi életünkben, hiszen az okoseszközök használata az életünk részévé vált, ezért egyre fontosabbá válik az okoseszközök biztonságos és tudatos használata. Az információbiztonság oktatása az általános és középiskolákban már elengedhetetlenül fontossá vált, hiszen digitális társadalomban élünk. A tanulmányban azt vizsgáltuk, hogy a két ország informatikai oktatási tananyagában van-e információbiztonsági tudatosság fejlesztése, valamint az informatikai oktatási tananyag és a jelszóhasználati szokások között található-e különbség.

Kulcsszavak

oktatás, informatika, információbiztonság, okoseszközök, jelszóhasználat

[1] mandic.dorottya@gmail.com | ORCID: 0000-0002-3384-5590 | PhD Student, Óbuda University Doctoral School on Safety and Security Science | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] kiss.gabor@bgk.uni-obuda.hu | ORCID: 0000-0002-0447-937 | full time professor, Óbudai University | egyetemi tanár, Óbudai Egyetem

BEVEZETÉS

Az informatikai oktatás fontossága ma már elengedhetetlen a mai világban, ahol napi szinten használunk különféle okoseszközöket. Az informatikai tudás ma már szinte mindenki számára szükséges. [1] A különféle okoseszközök iránt egyre nagyobb a kereslet a hétköznapi életben, ezért egyre fontosabbá válik az eszközök biztonságos használata, hiszen az információbiztonságban a leggyengébb láncszem az egyén. [2], [3] Az okoseszközök elterjedésével az átlagos felhasználók információbiztonsági kockázatokkal néznek szemben. [4], [5], [6] 2024-ben az IoT eszközök száma 18,5 milliárd volt és 2025-ben 14%-kal megnőt a számuk.[7] „A mai digitális társadalomban, amelyben együtt van jelen a virtuális és a valós környezet, fontos az egyének megfelelő és felelősségteljes bevonása és hogy tudatában legyenek a technológia kínálta lehetőségeknek és kockázatoknak”. [8] Egyes tanulmányok szerint az információbiztonság tudatosságának oktatását akkor kellene elkezdeni tanítani, amikor valakinek először a kezébe kerül egy informatikai eszköz, és hogy a gyermekek oktatását minél korábban kellene elkezdeni. [9] Egyes tanulmányok szerint azok, akik nem gyermekkortól kezdik elsajátítani az informatikai alapismereteket hátrányba kerülhetnek a társaikhoz képest. [10] Az általános és középiskolákban az információbiztonság oktatása kiemelten fontos. [11] Magyarországon az informatikai tanterv követelményei a Művelődési Minisztérium tantervében jelent meg 1988-ban. A külön tantárgyra való igény a 80-as évek végén kezdett egyre fontosabb lenni. Az informatika 1998-ban jelent meg, mint önálló műveltségterület.[12] Majd 2020-ban az informatika tantárgyat felváltotta a digitális kultúra tantárgy.[13] A módosítás azért történt meg, hogy a gyerekek minél hamarabb megismerkedjenek a „digitalizáció eszközrendszerével, a digitális kultúra elnevezésű tantárgy keretein belül.”[14] „Szlovákiában a nemzeti tanterveket a Szlovák Köztársaság Oktatásügyi, Tudományos, Kutatási és Sportminisztériuma adja ki”.[15] Szlovákiában a kerettantervben le van írva évfolyamok szerint az informatika órák száma, hogy hány óra lenne szükséges. Az iskoláknak lehetőségük van dönteést hozni arról, hogy például mely tantárgyakat szeretnék több óraszámban oktatni.[16] Jelen tanulmányban betekintést kapunk Magyarország és Szlovákia informatikai oktatási tananyagában, valamint a felmérésben résztvevők közül megtudhatjuk hányan használnak okoseszközöket nemek és korcsoport szerint, és hogy az okoseszköz használóknak milyen jelszóhasználati szokásaik vannak.

Magyarország és Szlovákia informatikai oktatási tananyaga

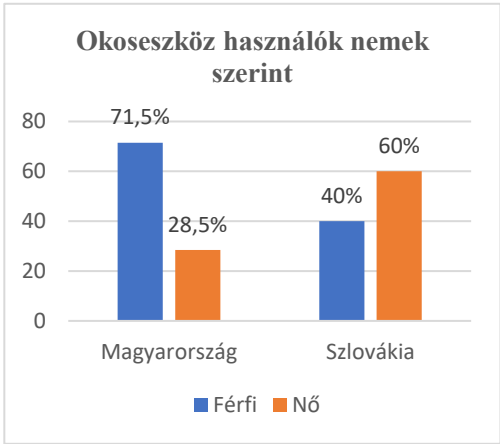
Magyarországon 2020-ban az informatikát felváltotta a digitális kultúra tantárgy és a középiskolások számára kötelezővé vált. A digitális kultúra tantárgy célja, hogy „a diákok ne csak az eszközhasználatot sajátítsák el, hanem mélyebb megértést szerezzenek a digitális technológiák társadalmi, kulturális és gazdasági hatásairól, valamint, hogy felkészüljenek a digitális világ kihívásaira.”[17] A 3–4. évfolyam számára az óraszám 72 órából áll, és olyan témakörökről tanulnak, mint például „a digitális eszközök használata, védekezés a digitális világ veszélyei ellen.” [18] Az 5. évfolyam részére a digitális kultúra tantárgy alapóraszáma 34 óra. A 6. évfolyam részére a digitális kultúra tantárgy alapóraszáma szintén 34 óraszámból áll. [19] A 7-8. évfolyam számára a tananyag az 5–6. évfolyam tananyagához kapcsolódik. A 8. évfolyam tananyaga kapcsolódik 7. évfolyam tananyagához, amely szintén 34 órából áll. [20] A középiskolában a tanulók a digitális kultúra tantárgy által olyan témakörökkel foglalkoznak, mint például „az okos eszközök okos használatára, tudatos felhasználói és vásárlói magatartás alakítására.”[21]

Szlovákiában a „Szlovák Köztársaság Oktatási, Tudományos, Kutatási és Sportminisztériuma adja ki és teszi közzé" minden oktatási szintre vonatkozóan. Ezen kívül a témakörhöz „teljesítmény és tartalmi standard tartozik". Az előírások alapján pedig az iskola eldöntheti, hogy bizonyos tananyagokat mikor fogja oktatni. A kerettantervben le van írva az informatika órák száma évfolyamok szerint. Az általános iskola alsó tagozat számára az informatikai óraszám 2 óra, a 3–4. évfolyam számára 1 óra. A felsőtagozat óraszáma az 5–7. évfolyam számára 4 óra, az 8. évfolyam számára pedig 1 óra. A gimnáziumok számára pedig 3 óra. Az alsó és felső, valamint a gimnázium számára meg van határozva a kötelező óraszám. Szlovákiában a 4. évfolyam végére a tanulóknak tudniuk kell beszélni az internet veszélyeiről. A 6. évfolyamban pedig már olyan témakörökről tanulnak, mint például az adatok védelmére vonatkozó szabályok, kiberbűnözés, kockázatok az interneten, biztonságos és etikus viselkedés az interneten. A gimnáziumimban pedig olyan témakörökről tanulnak, ahol a diákok megtanulják például felmérni a rosszindulatú szoftvereket és felismerni a számítógépes bűnözést.[16]

MAGYARORSZÁG ÉS SZLOVÁKIA JELSZÓHASZNÁLATI SZOKÁSAI A FELMÉRÉS ALAPJÁN

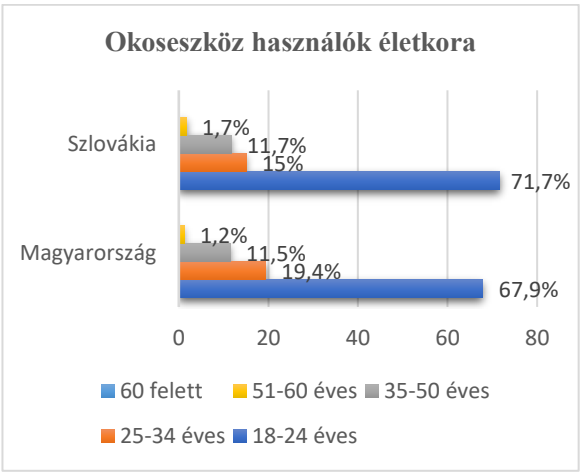
A felmérést Magyarországon és Szlovákiában végeztünk az okoseszköz használók körében. A felmérésben Magyarországon összesen 166-an vettek részt, és ebből a férfiak közül 118-an (71,5%), míg a nők 47-en (28,5%) vettek részt. Szlovákiában a felmérésben összesen 62-en vettek részt, és ebből 25 férfi (40,3%), és 37 nő (59,7%). A felmérésben összesen 229-en vettek részt Magyarországon és Szlovákiában. A kérdőív kitöltése online névtelenül és önkéntes alapon történt. Magyarországon a felmérésben résztvevők közül 98,5%-a válaszolta, hogy használ legalább egy okoseszközt, míg Szlovákiában a válaszadók 98,4%-a válaszolta..

Az 1.ábrán láthatjuk, hogy a felmérés alapján Szlovákiában válaszolták legtöbben a nők, hogy okoseszközöket használnak, míg Magyarországon a férfiak.



1. ábra: Az okoseszköz használók nemek szerint Magyarországon és Szlovákiában.Forrás: Saját szerkesztés

Ami az életkort illeti a felmérés alapján az okoseszköz használók Magyarországon és Szlovákiában is a 18-25 éves korosztály válaszolta legtöbben, hogy használ okoseszközt. A 2. ábrán láthatjuk az okoseszköz használók életkorát Magyarországon és Szlovákiában.



2. ábra: Az okoseszköz használók életkora Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Megfigyelhetjük, hogy Magyarországon a legtöbben a 18-24 éves korosztály válaszolta, hogy használ okoseszközt (67,9%), majd ezt követi a 25-34 éves korosztály (19,4%), majd a 35-50 éves korosztály (11,5%), végül pedig az 51-60 éves korcsoport (1,2%). Szlovákiában megfigyelhető, hogy szintén a 18-24 éves korosztály (71,7%) válaszolta, hogy használ okoseszközöket, majd ezt követi 24-34 éves korosztály (15%), majd a 35-50 éves korosztály (11,7%) és az 51-60 éves korcsoport (1,7%) válaszolta, hogy használ okoseszközt.

A felmérésben vizsgáltuk a jelszóhasználati szokásokat az okoseszköz használók körében mint például a jelszó tartalmát illetően, valamint hogy használják-e ugyan azt a jelszót több helyen, illetve milyen hosszú jelszavakat használnak, és hogy milyen gyakran változtatják a jelszót, amit használnak.

Az 1. táblázatban láthatjuk Magyarország és Szlovákia jelszóhasználati szokásait az okoseszköz használók körében a felmérés alapján.

Jelszóhasználati szokások az okoseszköz használók körében	**Magyarország (%)**	**ia (%)**
Jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktereke	93,3%	93,4%
Jelszó személyes információkat tartalmaz	24,2%	32,8%
Jelszó értelmes szót tartalmaz	51,5%	67,2%
Ugyan azt a jelszót több helyen használja	66,3%	70,5%
Jelszó változtatás gyakorisága		
Napi szinten	0%	0%
Heti szinten	1,2%	0%
Minden hónapban	4,9%	11,5%
Félévenként	17,8%	18,1%
Évenként	44,2%	31,1%
Soha	31,9%	39,3%

Jelszóhasználati szokások az okoseszköz használók körében	Magyarország (%)	ia (%)
A jelszó hossza		
Kevesebb mint 8 karakter	3,1%	4,9%
8-10 karakter	55,2%	44,3%
12 vagy ennél is több karakter	41,7%	50,8%

1. táblázat: Az okoseszköz használók jelszóhasználati szokásai Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

Magyarországon a felmérésben résztvevők 93,3%-a válaszolta, hogy a jelszó amit használ kis és nagybetűket, számokat és speciális karaktereket tartalmaz, míg Szlovákiában a válaszadók 93,4%-a. Magyarországon 24,2% válaszolta, hogy a jelszó, amit használnak tartalmaz értelmes szót, addig Szlovákiában 32,8%-a válaszolta. Megfigyelhetjük, hogy Magyarországon a felmérésben résztvevők 51,5%-a válaszolta, hogy a jelszó, amit használ tartalmaz értelmes szót, addig Szlovákiában 67,2%-a válaszolta. Magyarországon a felmérésben résztvevők 66,3%-a válaszolta, hogy ugyanazt a jelszót több helyen használja, addig Szlovákiában a felmérésben résztvevők 70,5%-a válaszolt igennel. Láthatjuk, hogy Magyarországon a jelszó változtatás gyakoriságánál a válaszadók 1,2%-a válaszolta, hogy napi szinten változtatja meg a jelszavát, 4,9%-a válaszolta, hogy heti szinten, 17,8%-a minden hónapban, 44,2%-a válaszolta, hogy félévenként és 31,2%-a válaszolta, hogy soha nem változtatja meg a jelszavát. Szlovákiában a válaszadók 11,5%-a válaszolta, hogy heti szinten változtatja, 18%-a válaszolta, hogy minden hónapban, és 31,1%-a válaszolta, hogy fél évenként, valamint 39,3% válaszolta, hogy soha nem változtatja meg a jelszót.

A Mann-Whitney U-tesztet használtuk, hogy összehasonlítsunk „két csoportot, hogy szignifikánsan különböznek-e egymástól.” [22] A Mann-Whitney próbát alkalmazzuk abban az esetben „ha folytonos változó esetén a változó nem normál eloszlású a kétmintás t-próba helyett.” Abban az esetben, ha a „ $p<0,05$ azt jelenti, hogy jelentős különbség van a két minta között.” [23] A statisztikai teszt számításának a feltétele, hogy „a két változó két értéket vagy is két csoportot vesz fel, valamint a két csoport elemei függetlenek egymástól, és a független változó folytonos vagy ordinális.” [24]

A 2. táblázatban láthatjuk, hogy Magyarországon és Szlovákiában van-e különbség a jelszóhasználati szokások között nemek szerint.

Mann-Whitney U teszt	p
A jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktereket	0,001
A jelszó személyes információkat tartalmaz	0,004
A jelszó értelmes szót tartalmaz	0,001
Ugyan azt a jelszót több helyen használja	0,724
A jelszó változtatás	0,158

Mann-Whitney U teszt	p
A jelszó hossza	0,497

2. táblázat: Mann-Whitney U teszt Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Megállapíthatjuk, hogy a jelszóhasználatkor, amikor a jelszó tartalmát nézzük, hogy a jelszó kis és nagybetűket, számokat és speciális karaktereket használnak, valamint személyes információt és értelmes szót szignifikáns különbség van nemek szerint. Elmondhatjuk, hogy a jelszóhasználat esetében, amikor a jelszó tartalmát nézzük meg, hogy az okoseszköz használók Magyarországon szignifikánsan összetettebb jelszavakat használnak a jelszó tartalmát illetően, ezáltal biztonságosabb az azonos hosszúság esetén a brute force támadás esetén. Láthatjuk, hogy Szlovákiában szignifikánsan többen használnak olyan jelszót, amely személyes információkat tartalmaz. Addig Magyarországon láthatjuk, hogy szignifikánsan kevesebben használnak olyan jelszót, ami értelmes szót tartalmaz. Láthatjuk, hogy nincs szignifikáns különbség a jelszó hossza és a jelszóváltoztatás gyakorisága között, valamint ugyanaz a jelszó használata esetében, amikor több helyen használják ugyanazt a jelszót. Láthatjuk, hogy ugyanaz a jelszó használata esetében több helyen az okoseszköz használók Magyarországon és Szlovákiában is ugyanúgy több helyen használják ugyanazt a jelszót. A jelszóváltoztatás esetében pedig Magyarországon és Szlovákiában is az okoseszköz használók ugyanúgy ritkán változtatják meg a jelszót, amit használnak. A jelszó hossza esetében pedig látható, hogy mindkét országban ugyanannyian kevesen használnak 12 vagy ennél is több karaktert tartalmazó jelszót.

ÖSSZEFOGLALÁS

Több tanulmány is foglalkozik informatikai oktatási tananyaggal és az információbiztonság oktatásának fontosságával, ami alapján elmondható, hogy az információbiztonságot minél korábban kellene elkezdeni oktatni. Láthatjuk, hogy az informatikai oktatási tananyagban különbség található Magyarország és Szlovákia informatikai oktatási tananyagának az óraszámában az általános és középiskolában. Ami alapján elmondható, hogy Magyarországon nagyobb hangsúlyt fektetnek az informatikai óraszámra, mint Szlovákiában. Ezen kívül eltérés található a témaköröknél is, mivel Szlovákiában például nagyobb hangsúlyt fektetnek a biztonság témakörére, mint Magyarországon. Megállapíthatjuk azt is, hogy mindkét országban az információbiztonság megtalálható az informatikai oktatási tananyagban, így mindkét országban a diákok az információbiztonságról tanulnak, csak az óraszám és egyes témakörökre helyezett hangsúly tér el. [11] Láthatjuk azt is, hogy Magyarországon nemek szerint a jelszóhasználatkor, amikor a jelszó tartalmát figyeljük meg, akkor Magyarországon szignifikánsan összetettebb jelszavakat használnak a jelszó tartalmát illetően. Megfigyelhetjük, hogy Szlovákiában szignifikánsan többen használnak nemek szerint olyan jelszót, amely személyes információkat tartalmaz, addig Magyarországon láthatjuk, hogy szignifikánsan kevesebben használnak nemek szerint olyan jelszót, ami értelmes szót tartalmaz. Ami alapján elmondható, hogy Magyarországon tudatosabban használják az okoseszköz használók nemek szerint az olyan jelszavakat, melyek kis és nagybetűket, számokat és speciális karaktereket tartalmaz és értelmes szót, ami az informatikai oktatás magasabb óraszámának köszönhető, hiszen Magyarországon az informatikai oktatás óraszáma

az általános és középiskolákban is magasabb óraszámból áll, mint Szlovákiában, ezért a diákok a szükséges ismereteket jobban eltudják sajátítani.

FELHASZNÁLT IRODALOM

[1] Czinege Monika és Erdélyi Éva, „Módszertani alapozással a fenntartható oktatásért: az elengedhetetlen informatika", in Integrált gondolkodás és integrált vállalati jelentés: Fenntarthatósági kockázatok a gazdasági és energetikai válság árnyékában - BGE Magyar Tudomány Ünnepe konferencia kötet 2023, Budapesti Gazdasági Egyetem, 2023, o. 19–32. doi: 10.29180/978-615-6342-50-8_2.

[2] Mandić Dorottya és Kiss Gábor, „Informatikai oktatási tananyag Magyarországon és Szerbiában", Hadmérnök, köt. 19, sz. 4, o. 143–152, 2024, doi: 10.32567/hm.2024.4.10.

[3] Mandić Dorottya, „Az okoseszközök veszélyei", Biztonságtudományi Szemle, 5, köt. 3, sz. 37–45, o. 9, 2023.

[4] Koller Marco és Kerti András, „Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása", Hadmérnök, köt. 16, sz. 4, o. 145–156, 2021, doi: 10.32567/hm.2021.4.11.

[5] Mandić Dorottya és Kiss Gábor, „Az okoseszközök és vírusvédelem használata Magyarországon és Szerbiában", 30th Anniversary conference of the safety and security enineering education: A biztonságtechnikai mérnök képzés 30évi jubileumi konferenciája, Budapest, Magyarország (2023) 127p. pp. 64-75.,12p., ISBN:9789634493297 sz. 64–75, o. 12, 2023.

[6] Mandić Dorottya, Kiss Gábor, és Rajnai Zoltán, „Password Usage among Users of Smart Devices in Hungary and Serbia", in 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania: IEEE, máj. 2024, o. 000309–000314. doi: 10.1109/SACI60582.2024.10619863.

[7] „State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally". [Online]. Elérhető: https://iot-analytics.com/number-connected-iot-devices/

[8] A Digitális biztonságról. PROMPT-H Számítástechnikai, Oktatási, Kereskedelmi és Szolgáltató Kft. [Online]. Elérhető: https://mek.oszk.hu/23600/23634/23634.pdf

[9] Stranszki Péter és Nyári Norbert, „Az információbiztonság-tudatosság fejlesztése", BSZ, köt. 73, sz. 5, o. 1067–1078, máj. 2025, doi: 10.38146/bszajia.2025.v73.i5.pp1067-1078.

[10] „IKT az oktatás kezdő szakaszában". [Online]. Elérhető: https://ofi.oh.gov.hu/tudastar/gyermekinformatika/ikt-oktatas-kezdo

[11] Pásztor Bence, „Az információbiztonság oktatásának összehasonlítása Szlovákiában és Magyarországon", in Conference Proceedings, J. Selye University, 2023, o. 181–186. doi: 10.36007/4782.2023.181.

[12] „Az Informatika helyzete és fejlesztési feladatai". [Online]. Elérhető: https://ofi.oh.gov.hu/tudastar/tantargyak-helyzete/informatika-helyzete

[13] „Informatika helyett jön a digitális kultúra óra - a diákok már ötödikben robotokat programozhatnak". [Online]. Elérhető: https://eduline.hu/kozoktatas/20200716_digitalis_kultura_ora

[14] „A digitális kultúra oktatásának fogalmi tisztázásai, kívánatos propedeutikai megalapozása”. [Online]. Elérhető: https://nyelvorzo.hu/blog/2021-08-21/a-digitalis-kultura-oktatasanak-fogalmi-tisztazasai-kivanatos-propedeutikai-megalapozasa
[15] Zentai Gabriella, Borbélyová Diana, Bencéné Fekete Andrea, Nagyová Alexandra, Horváth Kinga, Orsovics Yvette, Józsa Krisztián, „A szlovákiai és a magyar általános iskolai tantervek összehasonlító vizsgálata a DIFER-készségek fejlesztése szempontjából A comparative study of the Slovak and Hungarian primary school curricula from the point of view of the development of DIFER skills”, Eru-Edu, köt. 18., sz. 3, o. 78–94, 2023, doi: 10.36007/eruedu.2023.3.078-094.
[16] Pásztor Bence, „Az információbiztonság megjelenése a Csehországi és a Szlovákiai tantervben”, Gradus, köt. 11, sz. 1, 2024, doi: 10.47833/2024.1.CSC.009.
[17] „A digitális kultúra tantárgyról”. [Online]. Elérhető: https://digikultura.hu/digitalis_kultura
[18] „Helyi tanterv NAT 2020 alapján”. [Online]. Elérhető: https://andor-ilona.baptistaoktatas.hu/files/104/modules/item_menu/5681/files-1/helyi-tanterv_nat2020_ai_alt_2023.pdf
[19] „Mintaterv: Digitális kultúra 5-6. évfolyam”. [Online]. Elérhető: https://www.oktatas2030.hu/wp-content/uploads/2020/09/digitalis-kultura-mintatanterv-5-6.pdf
[20] „Mintaterv: Digitális kultúra 7-8. évfolyam”. [Online]. Elérhető: https://www.oktatas2030.hu/wp-content/uploads/2020/09/digitalis-kultura-mintatanterv-7-8.pdf
[21] „Kerettanterv a gimnáziumok 9–12. évfolyama számára”. [Online]. Elérhető: https://www.oktatas.hu/kozneveles/kerettantervek/2020_nat/kerettanterv_gimn_9_12_evf
[22] „Interpret the key results for Mann-Whitney Test”. [Online]. Elérhető: https://support.minitab.com/en-us/minitab/help-and-how-to/statistics/nonparametrics/how-to/mann-whitney-test/interpret-the-results/key-results/
[23] Németh Anikó, Adatelemzés statisztikai módszerekkel. [Online]. Elérhető: https://eta.bibl.u-szeged.hu/458/1/EFOP343_AP2ETSZK_jegyzet_N%C3%A9meth_Anik%C3%B3_Adatelemz%C3%A9s_statisztikai_m%C3%B3dszerekkel_20180620.pdf
[24] „Paraméteres és nem paraméteres próbák alkalmazása több csoport összehasonlítására folytonos változók esetén”. [Online]. Elérhető: https://semmelweis.hu/kutlab/files/2023/04/Csoportok_osszehasonlitasa_2023_SGy.pdf

DOI: https://doi.org/10.12700/btsz.2026.8.1.41

HUNGARISM – FROM ITS ORIGINS AS A THREAT TO THE STATE (FROM ITS EMERGENCE TO THE EXPERIENCE OF REGIME CHANGE)

HUNGARIZMUS – KEZDETEKTŐL AZ ÁLLAM ELLEN (A KIALAKULÁSTÓL A RENDSZERVÁLTÁS MEGÉLÉSÉIG)

BOROSS Zsigmond Attila[1]

Abstract

Hungarism represents the Hungarian manifestation of National Socialism. Due to its radically left-wing elements, it stands in opposition to right-wing conservatism. During the Horthy era, its dangerous nature was recognised, and law enforcement authorities treated it as a form of extremism. In the second half of the 1930s, its popularity increased dynamically among certain segments of society. The counter-intelligence services sought to limit and obstruct the spread of Hungarism and its attempts to seize power through active measures. Discrediting operations, the use of provocateurs, criminal proceedings initiated against political leaders, and imprisonments contributed to the strengthening of a sense of persecution. The analysis examines the challenges associated with Hungarism from the perspective of societal security and the responses of law enforcement agencies. Each of these periods posed different types of risks to Hungarian society.

Keywords

Hungarism, nationalsocialism, extremism, counter extremism, social security, emigration

Absztrakt

A hungarizmus a nemzetiszocializmus magyar gyakorlata. Radikálisan baloldali elemei miatt a jobboldali konzervativizmus ellenfele. A Horthy-korszakban felismerték veszélyességét és a rendvédelem extrémizmusként kezelte. Az 1930-as évek második felében népszerűsége dinamikusan nőtt a társadalom egyes rétegeiben. Az elhárító szerv aktív intézkedésekkel igyekezett korlátozni, akadályozni a hungarizmus térnyerését, hatalomra törését. Lejárató akciók, provokátorok alkalmazása, politikai vezetők ellen indított büntetőeljárások, bebörtönzések segítették az üldöztetés-tudat térnyerését. Az elemzés a társadalombiztonság és a rendvédelmi szervek válaszai fókuszából vizsgálja a hungarizmushoz kapcsolódó kihívásokat. Mindegyik időszak más-más kockázatot hordozott a magyar társadalom számára.

Kulcsszavak

hungarizmus, nemzetiszocializmus, extrémizmus, extrémizmus-elhárítás, társadalombiztonság, emigráció

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

BEVEZETÉS

Egy állam zavartalan működését és a társadalmi béke állapotát számos nemkívánatos törekvés sértheti. [1] Az extrémizmus mindenkori fenyegetése leginkább abban rejlik, hogy követői indokoltnak tartják akár az erőszak alkalmazását is céljaik elérése érdekében. [2] A politikai szélsőség táborába tartozó hungaristák több alkalommal kísérelték meg a hatalom átvételét, természetesen a fegyveres fellépés lehetőségével számolva. A hungarizmus bal- és jobboldali elemeket egyaránt tartalmazó antidemokratikus ideológiája rugalmas hivatkozási lehetőséget biztosít napjaink szélsőségesei számára is. A tanulmány – két része – mintegy nyolc évtized történéseinek áttekintése révén kívánja szemléltetni, hogy a hungarizmusból fakadó, nemzetbiztonsági súlyú fenyegetés a régmúlt és a közelmúlt után a jelen és a jövő számára is feladatként jelentkezik az egész társadalom számára. A gyűlöletbűncselekményekben megjelenő, végül államellenes-és terrorcselekményekben kiteljesedő problémakör hatékony korlátozása, esetleg felszámolása az eddigi rendvédelmi felfogáson és gyakorlaton túlmutató interdiszciplináris szemlélet érvényesítését igényli. [3]

Az elemzés célkitűzése, hogy túlmutasson a hungarizmus, illetve veszélyei bemutatásán. A társadalmi bizonytalansággal és nyitottsággal szemben a rendvédelem következetes fellépését is igyekszik szemléltetni. A választójog korlátozása, büntetőeljárások folyamatos lebegtetése és elindítása a hatalom következetes szembenállását tükrözi. A hungarista ideológia filozofikus emelkedettsége és a gyakorlati megvalósulás kegyetlen brutalitása szintén a téma dialektikus dinamizmusát biztosítja. A feltárt összefüggések és a levont tapasztalatok a klasszikus szakértői elemzői tevékenység „termékei". Megkezdett kutatásunkban – a későbbi publikációkban – azt mutatjuk majd be, hogy a mesterséges intelligencia bevonásával az extrémizmushoz kapcsolódó kockázatok feltárása miként haladja meg jelenlegi képességeinket.

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

A HUNGARIZMUS, MINT A NEMZETISZOCIALIZMUS MAGYAR GYAKORLATA

Politikai ideológiák meghatározása során egyes eszmék viszonyát vizsgáljuk a társadalom főbb alrendszereihez és intézményeihez. A radikális nézetek követői a fennálló viszonyok gyökeres átalakítását sürgetik, és érdekérvényesítésük érdekében a többség által felvállalhatatlannak vélt fellépési formákat is alkalmaznak. A szélsőségesek, az extrémizmus képviselői ezt meghaladva – önmagukat egy kisebbségi elitcsapatnak titulálva – a többséggel szemben, akár erőszakot is alkalmazva lépnek fel. Ideológiájuk megkérdőjelezi a működő intézmények és folyamatok létjogosultságát, így azokat elvetve, gyökeresen új (az előzőeket tagadó) viszonyok kialakítására törekednek. Térnyerésük egyaránt elfogadhatatlan az éppen regnáló, akár autoriter hatalom, de a demokratikus parlamentarizmus számára is.

Az első világháború veszteségei, valamint a trianoni békediktátum társadalmi szintű sokkhatása a nemzeti túlélés és megújulás párhuzamos igényét fogalmazta meg. A Horthy nevével fémjelzett politikai értékrend és szellemiség a meglévő társadalmi berendezkedés

megszilárdítására törekedett, így a hatalmi/politikai elit is ennek fenntartásában volt érdekelt. [4] A meglévő viszonyokkal szemben álló forradalmi szemléletet elutasították, amelyhez segítséget nyújtott a Tanácsköztársaság akkor még közelinek számító emléke. A társadalomnak azonban volt több olyan hátrányos helyzetű rétege/csoportja, amely fogékony volt a radikális, vagy extrém politikai eszmék iránt. Az 1920-as évek kezdetén, főként Gömbös Gyula közvetítésével Magyarországra is eljutott a fasizmus ideológiája. A nemzetiszocializmus olasz alapjának megismerését követően, az 1930-as évek közepére – az ellenfelei által következetesen örménynek titulált – Szálasi Ferenc által kidolgozásra került a magyar gyakorlat: a hungarizmus. Szálasi Ferencet (1897-1946) is minden eszközzel igyekezett lejáratni az akkori politikai hatalom. Apai ágon örmény származására utalva Salesian, Szalosján neveken szerepeltette az állami sajtó, ezzel szemben már nagyapja magyarosított (Szálasi) néven harcolt 1848-49-ben. Anyai ágon szlovák és ruszin vér is csörgedezett ereiben. Ebből adódhat, hogy nem a fajvédelem nézeteit hirdette. [5]

Maga a megnevezés nem újkeletű. Már az első világháborút megelőző évszázadokban kialakult egy mai értelemben vett nemzeti gondolkodáson felülemelkedő identitás, a „hungarus-tudat", amely a történelmi Magyarország területén, a Szent Korona fennhatósága alatt élő személyek (nemesek) – etnikai alaptól független – politikai egységét támasztotta alá.

Ehhez kapcsolódott későbbaz Osztrák-Magyar Monarchia iparosodó/városiasodó/polgárosodó világának pozitív élménye, amely sokak számára magától értetődővé tette a „hungarus-tudat" reneszánszát. [6]

Ennek a korszaknak a végén teljesedett ki Prohászka Ottokár (Nyitra, 1858 – Budapest, 1927 katolikus püspök, író) életútja [7], amelynek szerves részét képezte a hungarizmus fogalmának és eszméjének következetes hangoztatása. A neves egyházfi a modern kapitalizmus nemkívánatos társadalmi jelenségeit a zsidóság tevékenységével azonosította, amely népesség asszimilációját is veszélyesnek tartotta. [8] A Tanácsköztársaság után a szociáldemokrácia és a szakszervezetek elutasítása szintén antiszemita érvrendszer alapján működött nála, amely kritikát azonban következetesen visszautasította. Bár a későbbi holokausztért személyes felelősség nem terheli, többen hivatkoznak nézeteire a zsidósággal szembeni fellépés igazolásaként. Az általa képviselt politikai katolicizmus a kor demokratikus szemlélete alapján, a parlamentarizmus keretei között értelmezhető. [9] [10]

POLITIKAI KATOLICIZMUS = IDEOLÓGIAI JOBB + GAZDASÁGI BAL

Szálasi Ferenc fellépése az 1930-as évek elején államelméleti értekezésekből bontakozott ki. Konnacionalizmusként megnevezett téziseiben a kárpát-medencei népek békés, a magyarság vezetése alatt megvalósuló együttélését propagálta a Pax Hungarica keretei között. Már kortársainak zöme is utópisztikusnak tartotta ezen nézeteit a fiatal nemzetállamok világában. Lejáratásának másik fontos elemét képezte, hogy a messianisztikus gondolatokat hangoztató politikust elmebajosnak bélyegezték, és vele kapcsolatban több orvos pszichopatológai szakvéleményét (miszerint skizofrén, paranoid pszichopata) is publikálták.

"Mi tehát a hungarizmus?
A legmagasabb fokú magyarság!
A hungarizmus célja a magyar birodalmi gondolat megvalósítása!" [11 p. 7]

1. ábra: Szálasi Ferenc (forrás: Internet)

A hungarizmus, az önmagát a konzervativizmussal szemben megfogalmazó nézet nem nevezhető szélsőjobboldalinak, mivel egyes kérdésekben baloldali válaszokat fogalmaz meg. [9] A hungarizmus követőinek gondolkodása inkonzisztens, az ideológiai jobboldal (a vallás, a tekintély, a nacionalizmus elfogadása) mellé gazdasági téren baloldali szemléletet képvisel. A gazdaságban meghatározó állami szerepvállalás gondolata, annak szabályozása, felügyelete például egyenesen Marxtól származik. A marxizmussal szemben viszont elutasítja az osztályharcot és a nemzeti közösséget hivatásrendek alapján működtetné. [11]

„A Hungarizmus elveti a nemzeti társadalmak természetellenes rétegződését és az állandó osztályharcot jelentő, osztályokba való sorolását: felső osztály, középosztály, alsóosztály. Ehelyett társadalmi szemléletében a hivatásuknál kialakult természeti csoportokat tartja a nemzeti társadalom összetevőinek. Ezek: a nemzetfenntartó paraszt, a nemzetépítő munkás, a nemzetvezető értelmiség, a nemzet halhatatlanságát biztosító nők, a nemzet jövőjét biztosító gyermek és a nemzetvédő katona." [11 p. 12]

A marxizmussal szemben a kereszténység társadalomszervező szerepét még az újhungaristák (pl. Kántor Béla) is hangsúlyozták az 1990-es években: [12]

„A szociális kérdés egy alapjában kapitalista szervezetű rendszerben is megoldható lenne, ha az államot és a társadalmat közösségi szellem, keresztény társadalmi erkölcs és nemzeti felelősségérzet töltené el."

A parlamentarizmus, mint dekadencia elutasításra talál. A politológia segítségével az alábbi képlettel írható le a közvélemény számára szélsőjobboldalként értelmezett hungarizmus:

HUNGARIZMUS (NEMZETISZOCIALIZMUS)/„SZÉLSŐJOBBOLDAL” =
IDEOLÓGIAI JOBB + GAZDASÁGI BAL + PARLAMENT-ELLENESSÉG [9]

Hogy ez az ideológia mennyire értelmezhetetlen volt a kor konzervatív elitjének, azt jól bizonyítja Szálasi számonkérő monológja évekkel később, amit hatalomra kerülését követően mondott el az országgyűlési képviselőknek: [11 p. 5]

"Zöld kommunisták voltunk és vagyunk mi, akik legfanatikusabb ellenségei vagyunk a bolsevizmusnak. Vallásellenesek voltunk és vagyunk mi, akik mindenkor hívő tagjai vagyunk egyházainknak. Német bérencek voltunk és vagyunk mi, akik egy pillanatig meg nem tántorodva a németekkel szemben is a Magyar Birodalom megvalósításáért küzdöttünk."

Szálasi legjelentősebb nemzetiszocialista szerveződései a Nemzet Akaratának Pártja (NAP), Magyar Nemzeti Szocialista Párt, Nyilaskeresztes Párt – Hungarista Mozgalom voltak. Pártműködés szempontjából megfigyelhető az összes nemzetiszocialista erőnél, így a hazai erőknél is egyfajta küldetéstudat, nagyfokú ideológiai- és pártfegyelem (amely segített a börtönéveket, üldöztetéseket elviselni). Szűk körű elitként értelmezték magukat, amelybe bekerülni érdem volt. Egyszerre csak egy nézet érvényesülhetett a párton belül, elhajlásra nem volt lehetőség. Ha valaki mégis megpróbálta, az vált az elsőszámú ellenséggé, aki korábban „nyilván", mint kém működött a mozgalomban, ezért rövidesen eltávolították. [13] A hungaristák totalitárius hatalmat akarnak létrehozni, amelynek minden nemzethű egyén a tagja, ahol az elbírálás, ítélkezés jogát maguknak tartják fent. Rendszerellenes jellegüket mutatja, hogy még napjainkban is megkérdőjelezik az egész rendszerváltást [14], sőt kiválasztott történelmi esemény – Szálasi kivégzése – óta a törvényes hatalom megszűnéséről beszélnek, miként például az 56-os Magyarok Világtanácsa kezelésében megjelent – *1956 – A forradalom igaz története*. 1999. című kiadvány bevezetőjében Szalay Róbert megfogalmazta, vagy a Pannon Front számaiban olvasható [15].

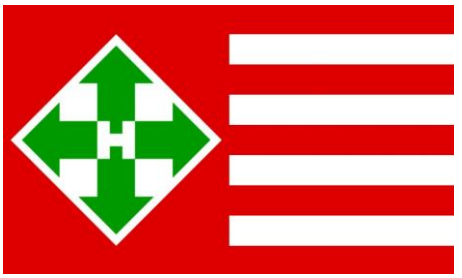
AZ ELSŐ HUNGARISTA HATALOMÁTVÉTELI KÍSÉRLET (1940)

A Horthy-korszak második felére, 1935 után az addigi kommunista veszély mellett egyre inkább kézzelfogható fenyegetést jelentett a hatalom számára a nemzetiszocialista szervezetek térnyerése. Sombor-Schweinitzer József (rendőr-főtanácsos, főkapitány-helyettes, a budapesti rendőr-főkapitányság politikai rendészeti osztályának vezetője) fontosnak tartotta a rendőrségi ellenőrzés kiterjesztését, így titkos együttműködői hálózatot alakított ki a nemzetiszocialista erők táborában is [15]. A társadalom-biztonság szempontjából kockázatosnak értékelték az erőre kapó irányzatot. A Keresztes-Fischer Ferenc belügyminiszter (1931-35 között a Károlyi- és Gömbös-kormányban, majd 1938-44 között az Imrédy-, Teleki-, Bárdossy- és Kállay-kormányban) által 1938-ban kiadott 3400-as rendelet eltiltotta a köztisztviselőket és az állami üzemek alkalmazottait a kommunista és nemzetiszocialista pártoktól. Ezt azonban a hungaristák szervezet-szabályzati szinten igyekeztek kijátszani. Így került 1939. január végén Szálasi a szegedi Csillagbörtönbe, ahol 9323-as számú politikai fogolyként a mártírrá válás útjára lépett. Keresztes-Fischer feloszlatta a Magyar Nemzeti Szocialista Párt - Hungarista Mozgalmat, vezetőit eljárás alá vonta. Főbb lapjaikat, az Összetartást és Magyarságot betiltották. [12]

A hungaristákkal szembeni drasztikus fellépést a Dohány utcai zsinagógánál végrehajtott terrorcselekménnyel indokolták. Történt ugyanis, hogy 1939. február 03-án [17] két kézigránátot hajítottak a zsinagóga előtt várakozó tömegbe. A kutatók (pl. Kádár Gábor, Vági Zoltán, Vámos György) egymásnak ellentmondó adatokat közölnek még ma is a sé-

rültek számáról és a sérülések súlyosságáról. A szakértők 13-23 főt, alapvetően könnyű sérültet említenek, illetve egy idős szívbeteg személyt, aki a szélsőségesek által elkövetett esemény hatására elhunyt. Lényegesen eltérő álláspontot képvisel Karsai László, aki szerint *„több mint valószínű, hogy a politikai rendőrség által megszervezett akcióról volt szó, amellyel a választások előtt le akarták járatni a nyilasokat, és ürügyet szereztek pártjuk betiltására, sajtójuk elnémítására.”* [17]

A pártszervezői feladatokat akkor már a bebörtönzött Szálasinál tehetségesebb országgyűlési képviselő, Hubay Kálmán vette át, aki sikeresen újjáépítette a pártot Nyilaskeresztes Párt – Hungarista Mozgalom (3. számú ábra) néven, de emellett a kormányt is hatékonyabban – és a potenciális bázis jelentő közvélemény számára is érthetően – támadta: *"Ma Magyarországon nem az igazságnak van hatalma, hanem a hatalomnak van igazsága!"* [18]



2. ábra: Nyilaskeresztes Párt – Hungarista Mozgalom jelképe (forrás: Internet)

A tehetséges Hubay (Hubay Kálmán tulajdonképpen nem hungarista, hanem fajvédő politikus volt. 1938-ban csatlakozott Szálasihoz, akit 1939. január végén bebörtönöztek. Hubay szervezte újjá másfél hónap alatt a pártot Nyilaskeresztes Párt – Hungarista Mozgalom néven, amely korábban nem látott sikereket ért el a választásokon. 1942-ben Szálasi és közte ellentét támadt, ezért ki kellett lépnie a pártból. 1946-ban a Népbíróság ítélete alapján kivégezték.) által szárnyalt a párt.

3. ábra: Hubay Kálmán (forrás: Internet)

Az 1939-es választásokon a nemzetiszocialista akciópártok és pártonkívüli jelöltjeik összesen csaknem 900 000 listás és egyéni választókerületi szavazatot szerezve a legjelentősebb ellenzéki erőként jutottak a törvényhozásba. (Az azt megelőző, 1935-ös választásokon alig 50 000 szavazatot kaptak összesen a hazai nemzetiszocialista szervezetek és jelöltjeik.) Csak a nyilasoknak 31 képviselőjük ülhetett be a padsorokba. [19]

Mindezen események elgondolkodtatták a kormányzatot – és a rendvédelmet – az egyre inkább egységesülő hazai „szélsőjobboldallal" szembeni további intézkedések kapcsán. A teljes ellehetetlenítést hatékonyan szolgálta, hogy 1940-ben a hungaristák puccsot kíséreltek meg. Erről szól Sombor-Schweinitzer József, a politika-rendészeti osztály vezetőjének jelentése, amelyet elöljárójához, Éliássy Sándor budapesti rendőrfőkapitányhoz terjesztett fel.

„Méltóságos Főkapitány Úr,
Mély tisztelettel jelentem, hogy folyó hó 24-én Kiss Jenő mérnök, műszaki főtisztviselő /.../ a Fegyvergyárban ebédszünet alkalmával a gépteremben ellenőrző útján véletlenül kihallgatta két munkás beszélgetését, akik a kormányzó úr őfőméltósága elleni merényletről tárgyaltak...." [20 p. 225]

Az esemény felgöngyölítését segítette a kedvező környezet, így például, hogy a Danubia Rt-t a Horthy családdal szoros rokonságban álló ifj. Károlyi Gyula gróf vezette. A kormányzati politika iránt egyértelműen elkötelezett közegben sikerült azonosítani az „összeesküvőket", illetve megfigyelhető a többi (megszólított) „munkavállaló" lojalitása. Elgondolkodtató azonban az is, hogy az eljárásban névvel és adatokkal szereplő tanúk lakcímein a megadott személyek nem találhatóak fel a korabeli lakcímnyilvántartás szerint.

A tervezett hatalomátvétel az alábbi forgatókönyvek szerint zajlott volna le:

„Az egyik munkás Bosnyák Imre lakatossegéd volt, a másiknak azonban a személyazonosságát megállapítani nem tudta, mert úgy voltak elhelyezkedve, hogy a köztük levő egyik gép eltakarta őket a szemei elől. /.../ Bosnyák Imre azonban még aznap délután, gondolván, hogy mindent hallott, felkereste őt irodahelységében és részletesen közölte vele a kormányzó úr személye ellen elkövetendő merénylet tervet. Elmondotta, hogy a Nyilaskeresztes Párt a jövőben át fogja venni a hatalmat, /.../ olyan módon, hogy a kormányzó úr őfőméltóságát egy vidéki útja során elfogják, és erőszakkal kényszerítik, hogy a főhatalom gyakorlásáról Szálasi Ferenc javára lemondjon. A lemondási nyilatkozat már előre meg lesz szövegezve, azzal az előre kiszemelt helyen – hová a kormányzó urat elfogatása után szállítják – várakozni fognak, és ott kényszerítik annak aláírására. A merénylet végrehajtását úgy tervezték, hogy a kormányzó úr egyik kenderesi, vagy gödöllői útja alkalmával az arra kiszemelt emberek felfegyverkezve el fognak helyezkedni egy alkalmas helyen, és amikor őfőméltósága gépkocsija odaér, azt mesterséges akadállyal feltartóztatják, és őt fogságba ejtik. Elhatározták, hogy ha a kormányzó úr kíséretében levők a legkisebb ellenállást fejtenék ki, azokat legyilkolják.

Egy másik terv szerint őfőméltóságát a Királyi Várban lévő lakosztályában fogják el, oly módon, hogy embereiket katonai ruhába öltöztetve őrváltás ürügye alatt csempésznék a kormányzó úr lakosztályába, és ott ejtenék fogságba. Amikor Bosnyák mindezeket közölte, megfenyegette, hogy a hallottakat tartsa titokban, mert annak elárulása esetén úgy őt, mind családját ki fogják irtani." [20 p. 225]

A tanúkihallgatások szerint a nyilas politikusok és aktivisták nehezen viselték meghurcoltatásukat és Szálasi 1941 nyaráig tervezett börtönbüntetését. [21] Esténként kocsmai, italgőzös beszélgetéseik során igazságuk kivívásán gondolkodtak. A mérsékelt intellektusú Bosnyák Imre vélhetően az egyik ilyen alkalmat követően, még túlfűtött állapotban dekonspirálta a „puccskísérletet". Személye, mozgalmi aktivitása folytán már ismert lehetett a rendőri és az üzemrendészeti szervek előtt, így vélhetően megfelelő pozíciókkal vették körül. Közlékenységével, kifecsegő hencegésével „szállította is" a kiemelt értékű információt a tervezett nyilas hatalomátvételi kísérletről, amelynek tényleges előkészítettsége a mai napig nem ismert. Hála a sikeres felderítésnek, a gyors és hatékony intézkedéseknek, a hatóság idejében felszámolta az összeesküvést…

1944. október 16 – 1945. március 29. között megvalósult a hungarista hatalom az akkorra már hadszíntérré változó Magyarországon. [22] A történészek által egyre árnyaltabban vizsgált időszak kapcsán kiemelendő, hogy míg korábban, a Sztójay kormány regnálása alatt mintegy 370 ezer zsidót deportáltak Magyarországról, addig Szálasi nem járult hozzá a zsidóság külföldi munkatáborokba szállításához [23], elsősorban azért, mert nélkülözhetetlen munkaerőként tekintett rájuk. Szintén sokak köszönhetik annak az életüket, hogy ebben az időszakban megszervezték a pesti gettót és annak őrzését [24], illetve a semleges államok menleveleit is elfogadták a magyar hatóságok a zsidómentő akciók során. Tény azonban az is, hogy ezen hónapok alatt mintegy ötvenezer zsidó honfitársunk vált a halálmanetek, Dunába lövetések, rablások és egyéb antiszemita erőszakcselekmények áldozatává. [25]

ÁTMENETI IDŐSZAK

A második világháborút követően a magyar társadalom önként és a hivatalos propaganda hatására idegenkedve tekintett vissza az elmúlt évtizedekre. A „Horthy-fasizmus" és a „nyilas bábkormány" elutasítása általános elfogadást nyert. A diktatórikus eszmék hasonlóságát és átjárhatóságát tükrözi azonban, hogy mindezzel párhuzamosan a „kisnyilasok" felvételt (és „bűnbocsánatot") nyertek a Magyar Dolgozók Pártjába.

A kádári Magyarországon is folytatódott a hungarizmus elutasítása. A nemzetiszocialista reneszánszt akadályozta, hogy a hivatalos politika több hullámban is fontosnak tartotta a hungarizmussal szembeni propagandahadjáratot. Az 1956-os eseményeket igyekeztek nyugati felforgató és reakciós erők, valamint a hungarizmus képviselőinek ellenforradalmi fellépéseként beállítani. A hungarista emigráció valóságtól elrugaszkodott propagandája munícióként szolgálta ezt a törekvést. Az 1967-as zuglói nyilasper pedig azt üzente a lakosságnak, hogy ezek a bűnök nem évülnek el, elkövetőiket bármikor utolérheti az igazságszolgáltatás. (Több mint két évtizeddel a második világháború lezártát követően rendezték a zuglói nyilaspert, amelynek végén a 19 megvádolt egykori pártszolgálatosból hármat halálra ítéltek.) [26]

A szocialista propaganda és az emelkedő életszínvonal idővel legitimálta a Kádár-rendszert, a mérsékelt számú ellenzéki erő sem a nemzetiszocialista oldalon szerveződött. A nyilas hagyományok ápolása így néhány veterán köré koncentrálódott, illetve alig pár főnyi érdeklődő követő képezte a magyarországi támogatói bázist.

A hungarista emigráció mindemellett működött, és élénken érdeklődött a hazai események iránt. A mozgalom vezetését 1946-tól, Szálasi kivégzését követően Henney Árpád

látta el 1980-as haláláig. Ekkor Tatár Imre (másképpen: Tarjányi-Tatár Imre) állt a mozgalom élére. Személyének elfogadottsága nem volt egyöntetű, így ketté is szakadt a Hungarista Mozgalom. Követői Juhászi Ferenc vezetésével működtették tovább az Út és Cél című kiadványt, illetve a rendszerváltást követően támogatták Magyarországon Győrkös Istvánt, aki – elmondása szerint – 1993-ban megkapta Tatártól a mozgalom vezetői feladatait. A másik, önmagát hivatalosnak nevező vonal Kántor Béla kiadásában jelentette meg mindezzel párhuzamosan a saját Út és Cél című lapját, illetve támogatta az 1993-ban hazaérkező és aktivizálódó Szabó Albertet.

A Hungarista Mozgalom további, immár a rendszerváltáshoz kapcsolódó sajátossága, hogy a – parlamentarizmus elutasításán túl a – jelenlegi jogrendszert nem tekintik önmagukra kötelező érvényűnek, ugyanis (szerintük) nem érvényesül a népfelség elve, illetve véleményük szerint a rendszerváltást követő Alkotmány, majd a hatályos Alaptörvény illegitim. Álláspontjuk alapja, hogy az 1989. évi XVII. törvény 7. § [27] értelmében az Alkotmány [28] elfogadásáról népszavazás útján kellett volna dönteni. Ennek hiánya következtében aktuálisan az Alaptörvényt és annak alkalmazását magukra nézve nem fogadják el kötelező érvényűnek. [29]

Mielőtt azt gondolnánk, hogy a második világháború óta túl sok idő telt el már ekkorra, és semmi folytonosság nem mutatható ki a korabeli eseményekkel, érdemes – az 1940-es puccskísérlet során már látókörbe került – Bosnyák Imre tevékenységére pillantani. Bosnyák a Mártírok Igazságtevő Bizottsága nevében kezdeményezte a Rákoskeresztúri Újköztemető 298. parcellája (főként itt temették el a II. világháború után a Népbíróság – többékevésbé jogszerű – ítéletei után kivégzetteket) rendbehozatalát, [30] majd nemzeti emlékhellyé nyilvánítva azt. Álláspontja szerint itt nyugszik ugyanis Szálasi Ferenc Lukács Ferenc név alatt feltüntetve. A széthúzás újabb példáját jeleníti meg, hogy a hazai hungarista tábor kisebb része a Weinhardt János nevéhez köthető sírt szokta koszorúzni. Bosnyákról tudni érdemes, hogy a Független Kisgazdapárt (FKGP) VII. kerületi alapszervezetének infrastruktúráját felhasználva ő biztosított először előadótermet az 1993-ban hazatérő Szabó Albertnek. Bosnyák temetésén az FKGP felsővezetése is képviseltette magát. [31]

RENDSZERVÁLTÁS – GYŐRKÖS ISTVÁN – ÚJKORI HUNGARIZMUS [32]

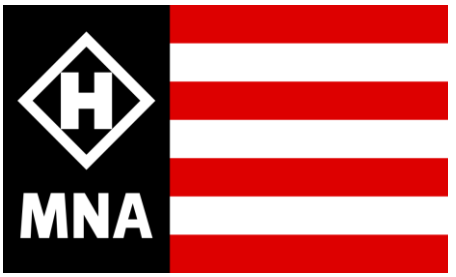
Győrkös István, a rendszerváltozás időszakától a magyarországi extrém jobboldal meghatározó alakja. Volt ő államellenes bűncselekmény központi figurája, a hungarista mozgalom társ-, majd egyszemélyi vezetője, bigott keresztény ideológus, a szkinhedek vezére [32], majd követőinek atyja. Jelenleg hivatalos személy sérelmére elkövetett, több ember életét veszélyeztető emberölés bűntettével, illetve lőfegyver engedély nélküli tartásával elkövetett lőfegyverrel visszaélés bűntettével gyanúsítja az ügyészség. [33]

Győrkös István, elmondása szerint [34] már a hatvanas évek elején is összeütközésbe került a törvénnyel, amikor is politikai okok miatt többéves szabadságvesztésre ítélték. Itt ismerkedett meg – bebörtönzött nyilasok révén – a hungarizmussal. [31] Későbbi politikai aktivitására vonatkozóan nem rendelkezünk ismeretekkel, azonban figyelmet érdemel, hogy az 1980-as években, lakókörnyezetében teret nyert a nemzetiszocialista propaganda. [35] Mivel önmagát is politikai fogolynak tekintette, az évtized végén minden igyekezetével egy fogolyszövetségbe próbált bekerülni, amely teret adott volna az addigra már nyíltan felvállalt nemzetiszocialista gondolatai megvalósításához. A rendszerváltás lehető-

ségeit kihasználva a „Nyugaton” élő nyilas emigránsokkal kapcsolatba lépve, az ígért támogatás lehetőségeire építve, szűk családi körből politikai szervezet megalakítását kezdeményezte. Már ekkor jellemezte a konspirációkészség, így fedőszervezetek létrehozását sem hanyagolta el. Első politikai produktumként 1989-ben megalakította gyermekeivel (ifj. Győrkös István, Győrkös Csaba és Győrkös Kolos), valamint szűk követői körével a Magyar Nemzetiszocialista Akciócsoportok nevű szervezetet. A működéshez jelentős pénzügyi segítséget kapott emigráns hungarista és neonáci körökből. [32]

4. ábra: Győrkös István (forrás: Internet)

A hungarizmust is több szervezet és irányzat képviselte Magyarországon a rendszerváltást követően. Győrkös István önmagát a Hungarista Mozgalom nyilas emigráció által felruházott kizárólagos hazai vezetőjének hirdette, begyűjtve így az anyagi támogatások zömét. Kiteljesedő szervezetépítésében jelentős állomást jelentett, hogy a Gottfried Küssel letartóztatásával végződő, osztrák nemzetiszocialista puccskísérlethez kapcsolódóan a magyar hatóságok eljárás alá vonták. A büntetőeljárás és az arra reflektáló médianyilvánosság lehetőségeit kihasználva 1992-től Magyar Nemzeti Arcvonal néven működtette szervezetét, amelynek – és családjának – központja a militáns aktivisták kiképzéseinek is helyet biztosító bőnyi birtok lett… [36]



5. ábra: a Magyar Nemzeti Arcvonal jelképe (forrás: Internet)

A napjainkig tartó, időről-időre kiteljesedő, nemzetbiztonsági súlyú fenyegetést a következő számban vizsgáljuk tovább, hogy az 1990-es évekből megismerjünk két hungarista hatalomátvételi kísérletet, majd a közelmúltból (2016) pedig egy rendőrgyilkosság körülményeit. [37]

FELHASZNÁLT IRODALOM

[1] I. Resperger, „Biztonsági kihívások, kockázatok és fenyegetések 2030-ig," in *Nemzetbiztonsági alapismeretek*, I. Kobolka, szerk. Budapest, 2013.

[2] Z. Gy. Bács, „A radikalizáció és a terrorizmus kapcsolata, egyes formái, gondolatok a megelőzés lehetséges perspektíváiról," *Nemzetbiztonsági Szemle*, no. 1, pp. 5–26, 2017.

[3] A. Kasznár, „Bioterrorizmus," *Terror & Elhárítás*, no. 2, pp. 4–36, 2012; valamint B. Laufer és G. Takács, „A HUMINT vége?," *Arc és álarc*, no. 1–2, pp. 175–194, 2018.

[4] M. Szinai és L. Szűcs, szerk., *Horthy Miklós titkos iratai*. Budapest: Kossuth Könyvkiadó, 1962.

[5] F. Szálasi, *Hungarizmus*. Sydney: Hungarista Mozgalom kiadása, 1994.

[6] R. Paksa, *A magyar szélsőjobboldal története*. Budapest: Jaffa Kiadó, 2012.

[7] O. Prohászka, *A diadalmas világnézet*. Budapest: Szent István Társulat, 1927.

[8] F. Brisits, szerk., *Prohászka breviárium*. Budapest: Szociális Misszió Társulat, 1927.

[9] A. Körösényi, *Pártok és pártrendszerek*. Budapest: Századvég Kiadó, 1993.

[10] J. Gyurgyák, szerk., *Mi a politika?* Budapest: Osiris Kiadó, 1996.

[11] Á. Henney, *Mi a hungarizmus?* Salzburg: A szerző kiadása, 1957.

[12] B. Kántor, *Kik vagyunk és mit akarunk?* Merredin: n.p., 1992.

[13] E. Hoffer, *A fanatizmus természetrajza*. Budapest: Bagolyvár Kiadó, 1999.

[14] A. Vécsey (Zs. Horváth), *A radikális jobboldal és a szélsőjobb története Magyarországon*. Kaposvár: Vagabund Kiadó, 2014.

[15] *1956 – A forradalom igaz története*. Budapest: 56-os Magyarok Világtanácsa, 1999.

[16] „Rendőrségi célkeresztben a szélsőjobb – Dr. Schweinitzer József feljegyzése (1932–1943)," elérhető: http://www.gondolatkiado.hu/…, hozzáférés: 2026. jan. 20.

[17] „Tényleg nem halt meg senki az 1939-es Dohány utcai merényletben?," *Múlt-kor*, elérhető: https://mult-kor.hu/…, hozzáférés: 2026. jan. 20.

[18] „Nyilas mozgalmak történeti dokumentumai," elérhető: http://www.pannonfront.hu/29/9323.htm, hozzáférés: 2026. jan. 20.

[19] G. Juhász, *Uralkodó eszmék Magyarországon 1939–1944*. Budapest: Kossuth Könyvkiadó, 1983.

[20] M. Szinai és L. Szűcs, szerk., *Horthy Miklós titkos iratai*. Budapest: Kossuth Könyvkiadó, 1962.

[21] E. Karsai és L. Karsai, *A Szálasi-per*. Debrecen: Reform Kiadó, 1988.

[22] „Szálasi Ferenc születése (1897. január 6.)," *Rubicon*, elérhető: http://www.rubicon.hu/…, hozzáférés: 2026. jan. 20.

[23] R. Paksa, *Szálasi Ferenc és a hungarizmus*. Budapest: Jaffa Kiadó, 2013.

[24] T. Zinner és P. Róna, *Szálasiék bilincsben*, vols. I–II. Budapest: Lapkiadó Vállalat, 1986.

[25] „Kiadták Szálasi Ferenc naplóját," *Index*, elérhető: https://index.hu/…, hozzáférés: 2026. jan. 20.

[26] „Szálasi-perrel kapcsolatos jogi elemzés," *Jogi Fórum*, elérhető: http://www.jogiforum.hu/…, hozzáférés: 2026. jan. 20.

[30] „Nyilas mozgalmak az 1940-es években," *Népszabadság* (archív), elérhető: http://nol.hu/…, hozzáférés: 2026. jan. 20.

[31] M. Andorfer, „Neonáci csoportosulás Magyarországon," *Belügyi Szemle*, vol. 41, no. 1, pp. 80–88, 1993.
[32] Zs. A. Boross, „Győrkös István mint a rendvédelem folyamatos célszemélye," *Belügyi Szemle*, no. 6, pp. 108–118, 2018.
[34] G. M. Nagy, „ÁVH-s férfit is ölt Győrkös István?," *Magyar Narancs Online*, elérhető: http://m.magyarnarancs.hu/…, hozzáférés: 2026. jan. 20.
[35] I. Grecsó, „Antiszociális fiatalok körében végzett ifjúságvédelmi munka Győr-Sopron megyében," *Belügyi Szemle*, no. 11, pp. 45–48, 1988.
[36] G. M. Nagy, „Apa elment ölni – Portré Győrkös István MNA-vezérről," *Magyar Narancs Online*, 2016, elérhető: http://magyarnarancs.hu/…, hozzáférés: 2026. jan. 20.
[37] *NBH Évkönyv 2000–2008*. Budapest: Nemzetbiztonsági Hivatal, 2001–2009.

JOGSZABÁLYOK

[27] 1989. évi XVII. törvény a népszavazásról és népi kezdeményezésről
[28] 1949. évi XX. törvény a Magyar Népköztársaság alkotmányáról
[29] Magyország Alaptörvénye (2011. április 25.)
[33] 2012. évi C. törvény a Büntető törvénykönyvről (Btk.)

DOI: https://doi.org/10.12700/btsz.2026.8.1.53

APPLYING LAYERED PHYSICAL SECURITY FOR THE PROTECTION OF CRITICAL ORGANIZATIONS

TÖBBRÉTEGŰ FIZIKAI VÉDELEM ALKALMAZÁSA A KRITIKUS SZERVEZETEK VÉDELMÉBEN

NAGY Gergely[1]

Abstract

Recent developments in the fields of security and security policy have once again drawn attention to the decisive role of physical protection for critical infrastructures and institutions essential to the functioning of society. The European and Hungarian regulatory environment, as well as legislation adopted in the course of legal harmonisation and certification requirements imposed on certain organisations, prescribe concrete physical and environmental protection measures. The study presents an easily adaptable, multilayered framework based on the principles of defence in depth. Through the structured logic of interconnected security zones, it provides transparency regarding areas of responsibility and the designation of necessary controls. The model applies a risk-proportionate approach, defining protective measures on the basis of relevant threats, exposures, and critical dependencies, thereby supporting business continuity. The proposed framework serves both as a practical planning guideline for strengthening physical security and as a compliance framework for meeting applicable legal and standards-based requirements.

Keywords

layered defense, defense in depth, hybrid warfare, industrial security

Absztrakt

Az elmúlt időszak biztonsági és biztonságpolitikai fejleményei ismét ráirányították a figyelmet a kritikus infrastruktúrák és a társadalom működése szempontjából jelentős intézmények fizikai védelmének meghatározó szerepére. Az európai és hazai szabályozási környezet, valamint a jogharmonizáció során megalkotott előírások és tanúsítványi követelmények konkrét fizikai és környezeti védelmi intézkedéseket is megfogalmaznak. A tanulmány egy könnyen adaptálható, többrétegű védelemre épülő keretrendszert mutat be a mélységi védelem elveinek alkalmazásával, amely biztonsági zónák egymásra épülő logikáján keresztül teszi átláthatóvá a felelősségi területeket és a szükséges kontrollok kijelölését. A modell kockázatarányos megközelítést érvényesít: a védelmi intézkedéseket a releváns fenyegetettségek, kitettségek és kritikus függőségek ismeretében határozza meg, támogatva az üzletmenet-folytonosság fenntartását. A bemutatott modell egyszerre szolgál gyakorlati tervezési alapelvként a fizikai biztonság megerősítéséhez, valamint megfelelési keretként a vonatkozó jogszabályi és szabványi elvárások teljesítéséhez.

Kulcsszavak

többrétegű védelem, mélységi védelem, hibrid hadviselés, létesítmény biztonság

[1] gergely.nagy777@gmail.com | ORCID: 0009-0004-2590-2120 | information security expert |információbiztonsági szakértő, We-Know Zrt.

BEVEZETÉS

A 2025-ös év egyik meghatározó biztonsági és biztonságpolitikai trendje a fizikai biztonság felértékelődése volt. A globális digitalizáció folyamata továbbra sem tört meg, és ezzel párhuzamosan a kiberbiztonság jelentősége is tovább növekedett, számos olyan esemény történt Magyarországon, valamint közvetlen és tágabb környezetünkben, amelyek ismét ráirányították a figyelmet a fizikai térben megvalósuló védelem megkerülhetetlen szerepére. A kritikus infrastruktúrák, pénzintézetek, közintézmények és katonai létesítmények őrzés-védelme továbbra is kulcsfontosságú, nem kiváltható biztonsági tényező.

Az elmúlt év során több, nagy visszhangot kiváltó esemény is rávilágított a társadalom működése szempontjából fontos intézmények fizikai védelmének sérülékenységeire. Az év végén történt az elmúlt évtizedek egyik legnagyobb bankrablása, valamint a Louvre ékszerrablása, Magyarországon pedig több alkalommal is felfedező kedvű fiatalok jutottak be kritikus infrastruktúra-létesítményekbe. Ezek az esetek, bár részben haszonszerzésből vagy kalandvágyból elkövetett cselekmények sok esetben súlyos rendszerszintű hiányosságokra mutatnak rá.

A fenti incidenseknél lényegesen komolyabb kihívást jelent Oroszország fokozódó hibrid hadviselési tevékenysége, melynek keretében 2022 óta szisztematikus, nem hagyományos hadviselési kampányt folytat Európa ellen, amelynek központi eleme a kritikus infrastruktúrák elleni szabotázs, vandalizmus és kémkedés. A cél elsősorban nem az azonnali fizikai rombolás vagy tömeges emberáldozatok okozása, hanem az európai társadalmak destabilizálása, az Ukrajna támogatásával összefüggő politikai és társadalmi költségek növelése, valamint a NATO és az Európai Unió kollektív reagálóképességének gyengítése.

Európa kritikus infrastruktúrája különösen sérülékeny a hosszú évtizedeken át halogatott beruházások, az elöregedett rendszerek, valamint az egymásra utalt hálózatok miatt. Oroszország ezt a helyzetet tudatosan használja ki, célpontjai között szerepel az energiaellátás, a közlekedés, a kommunikáció, a vízellátás, az egészségügy, valamint a katonai és logisztikai infrastruktúra. [1, p. 2]

A biztonsági fenyegetések mellett az európai és magyarországi vállalatoknak, valamint közigazgatási szerveknek egyre összetettebb jogszabályi megfelelési kötelezettségeknek is eleget kell tenniük. A NIS2 és a CER irányelvek[7] [8], valamint az ezekhez kapcsolódó hazai jogharmonizáció során megalkotott jogszabályok[2] [3] és végrehajtási rendeletek [4] [5] már konkrét fizikai védelmi intézkedések bevezetését is előírják a több mint 3000 érintett hazai szervezet számára. A vonatkozó hazai jogszabály a 2-es ellenálló képességi szintbe tartozó szervezetek számára konkrétan előírja „a kritikus infrastruktúrák területén a biztonság több rétegű kialakítását, amely késlelteti a legnagyobb védelmet igénylő területek elérését.”[4 2.2]

Ezzel párhuzamosan egyre több nagyvállalat követeli meg beszállítóitól olyan információbiztonsági tanúsítványok (pl.: ISO/IEC 27001, TISAX) megszerzését, amelyek nemcsak logikai, hanem fizikai biztonsági kontrollokat is előírnak, ideértve a fizikai hozzáférés korlátozását, a létesítmények védelmét (behatolás, tűz, betekintésvédelem stb.), valamint az eszközök és adatok fizikai biztonságának fenntartását.

A tanulmány célja, hogy egy könnyen adaptálható keretrendszert és gyakorlati segítséget nyújtson az érintett szervezetek számára: egyrészt a jogszabályi és beszállítói megfelelési követelmények teljesítésében, másrészt saját fizikai és szervezeti rezilienciájuk mérhető és fenntartható növelésében.

MÉLYSÉGI VÉDELEM

A mélységi védelem (Defense in Depth) koncepciója a katonai stratégiai tervezésből ered, ahol célja olyan akadályok komplex rendszerének kialakítása volt, amelyek lassítják és feltartóztatják a támadó felet céljai elérésében, miközben lehetőséget biztosítanak tevékenysége folyamatos nyomon követésére, valamint a megfelelő válaszlépések kidolgozására és végrehajtására a támadás elhárítása érdekében.

A koncepciót viszonylag régóta alkalmazzák a nukleárisipar területén is, ahol a balesetek hatásainak elszigetelése érdekében három egymástól független, egymást követő védelmi gát kerül kialakításra, ami alacsony szintre csökkenti annak valószínűségét, hogy egy baleset a létesítményen kívül is hatást gyakoroljon. Az alapelv szerint, minden biztonsági berendezést eleve sérülékenynek kell tekinteni, ezért azt egy további védelmi eszközzel kell védeni. [9, p. 9]

A kiberbiztonsági megközelítésben a mélységi védelem olyan megelőző és észlelő intézkedések összességét jelenti, amelyek akadályozzák a támadó előrehaladását, miközben lehetővé teszik a behatolás időben történő felismerését és a reagálást, a biztonsági incidens következményeinek csökkentése érdekében.

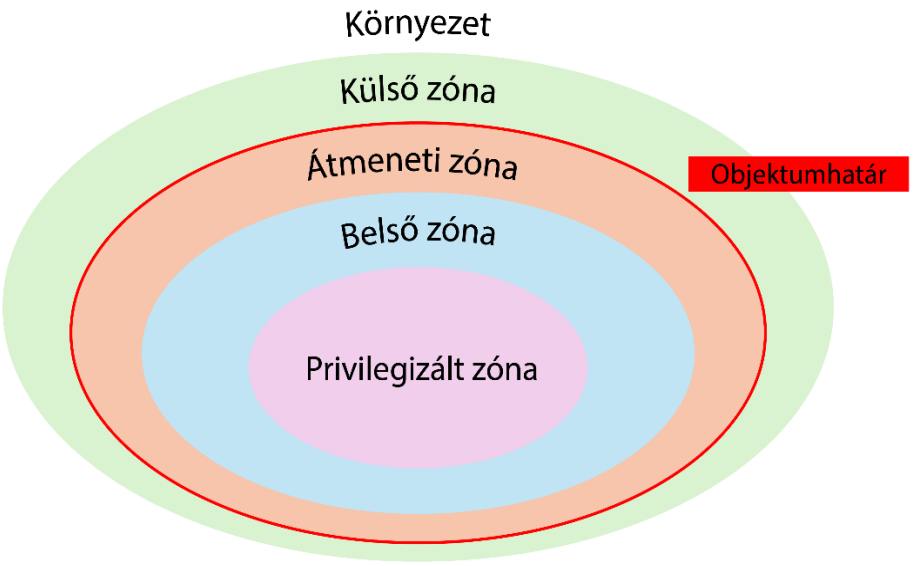
A mélységi védelem nem egy az egyben történő megfeleltetésen alapul, vagyis egy-egy konkrét kockázatra nem egyetlen megoldással, válaszlépéssel válaszol. Ezzel szemben holisztikus megközelítést alkalmaz, amely a szervezet valamennyi eszközének védelmét célozza, figyelembe véve azok kapcsolatait és egymásrautaltságát. A rendelkezésre álló erőforrások felhasználásával olyan, egymásra épülő megfigyelési és védelmi rétegek kerülnek kialakításra, amelyek a szervezet tényleges kitettségéhez és üzleti kockázataihoz igazodnak, ezáltal hatékony és kockázatarányos védelmet biztosítva. [10, p. 2]

A védelmi intézkedések alkalmazása tehát nem – lehet – öncélú, hanem szorosan kell kapcsolódnia a szervezet alapvető működési céljaihoz. Elsődleges rendeltetése a szervezet üzletmenet-folytonosságának fenntartása, valamint a kritikus folyamatok és erőforrások védelme. Ennek megfelelően a többrétegű védelmi intézkedések kiválasztása és kialakítása során a kockázatarányosság elvét kell érvényesíteni és a bevezetett kontrolloknak kizárólag olyan mértékben szabad korlátozniuk a szervezet mindennapi működését, amennyire a fenyegetések kezeléséhez feltétlenül szükséges.

A túlzottan szigorú vagy nem megfelelően illesztett védelmi intézkedések önmagukban is kockázatot jelenthetnek, mivel felesleges többletköltséget jelentenek, akadályozhatják az üzleti folyamatokat és hosszútávon a szabályok megkerülésére ösztönözhetik a felhasználókat. Ez adott esetben azt is jelentheti, hogy egy belsőbb védelmi zónában „enyhébb" védelmi intézkedések is elfogadhatóak. A mélységi védelem sikeres alkalmazása csak akkor valósulhat meg, ha a kontrollok kiegyensúlyozott, a működéshez illeszkedő rendszerként kerülnek kialakításra.

TÖBBRÉTEGŰ VÉDELMI MODELL

A mellékelt védelmi modell nem új szemléletet vezet be, hanem a jelenleg hatályos hazai jogszabályi környezet, valamint a vonatkozó nemzetközi szabványok és bevált jógyakorlatok rendszerbe foglalt alkalmazására épül. Emellett a szervezetek meglévő üzletmenet, működési-folyamati és infrastrukturális sajátosságaihoz illeszthető.



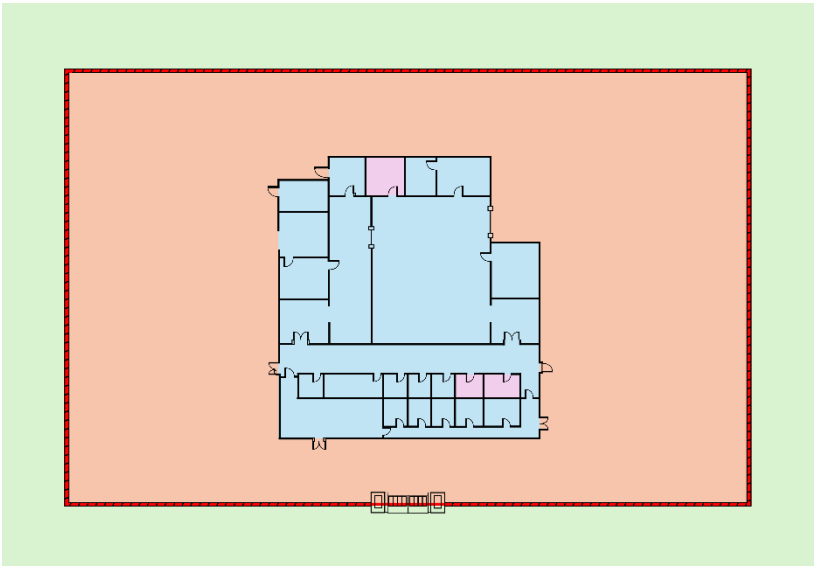
1. ábra – Védelmi zónák rétegrendje. Forrás: saját szerkesztés.

A modell célja a felelősségi területek, illetve az egyes területeken alkalmazandó védelmi intézkedések egyértelmű kijelölésének és kiválasztásának megkönnyítése. A modell strukturált keretet biztosít a fizikai biztonsági intézkedések tervezéséhez és értékeléséhez, elősegítve a következetes és kockázatarányos védelem kialakítását.

Fontos hangsúlyozni, hogy egy szervezet a gyakorlatban nem kizárólag egy-egy zónával rendelkezhet: a működés jellegétől, méretétől és kockázati kitettségétől függően az egyes zónákból több is kijelölhető, akár párhuzamosan, akár egymástól elkülönülően. Ugyanakkor a zónák egymásra épülő rétegrendjének – az ábrán meghatározott logika szerinti – megtartása a modell működőképességének alapfeltétele.

A zónák sorrendje nem felcserélhető, minden belsőbb védelmi szint csak az azt megelőző rétegek működése mellett képes megfelelően ellátni funkcióját. Ez a felépítés biztosítja, hogy az egyes védelmi intézkedések ne önálló, elszigetelt elemekként jelenjenek meg, hanem a mélységi védelem alapelvének megfelelően, egymást erősítő, koherens rendszerként támogassák a szervezet biztonságát. Amennyiben nem megoldható, hogy az adott zónát az alacsonyabb védelmi szintű zóna fizikailag is teljesen körbevegye, úgy a rétegrendet legalább a megközelítési útvonal tekintetében kell alkalmazni.

Egyes kritikus rendszerelemek esetében indokolt lehet a védelmi modell nem kizárólag síkbeli, hanem térbeli értelmezése is. Elsősorban a pilóta nélküli légieszközök, drónok elterjedése miatt, lehetőség szerint a fizikai biztonsági rétegek a fizikai tér teljes spektrumában értelmezendők. Ennek megfelelően a modell alaplogikája nemcsak a horizontális elrendezésben, hanem adott esetben a megközelítési irányok teljes halmazára kiterjedően is alkalmazható lehet.



2. ábra – Minta kialakítás: ipari létesítmény alaprajza, a zónák jelölése az 1. ábrán alkalmazottal megegyezik. A felső privilégizált zóna esetében csak a megközelítési útvonalak, az alsó két privilégizált zóna esetében teljes spektrumban alklmazott védelmi rétegekkel. Forrás: saját szerkesztés.

VÉDELMI ZÓNÁK

Környezet

A környezet a szervezet működésének tágabb fizikai és nem fizikai, így különösen jogi, gazdasági, társadalmi és biztonságpolitikai elemeit és összefüggéseit foglalja magába. Ebbe a dimenzióba tartoznak mindazon külső tényezők, amelyek a szervezet működésére hatással lehetnek, ugyanakkor többnyire közvetlen befolyásolási körén kívül esnek, vagy csak rendkívül korlátozott mértékben befolyásolhatók.

A szervezettel kapcsolatos kockázatok jelentős része ebben a külső térben gyökerezik: a geopolitikai folyamatok, a jogszabályi környezet változásai, a gazdasági helyzet, a társadalmi feszültségek, valamint az általános biztonsági környezet mind olyan tényezők, amelyek közvetlenül vagy közvetve hatással vannak a szervezet fenyegetettségi szintjére.

A környezethez kapcsolódó kontrollintézkedések célja nem a közvetlen fizikai védelem, hanem a szervezet működését érintő külső kockázatok korai felismerése, értelmezése és kezelhetővé tétele. A külső környezet változásainak értelmezése nélkül nem alakítható ki reális kép a fenyegetettségekről és nem határozhatók meg megalapozottan a szervezet fizikai biztonsági intézkedései. A külső környezeti tényezők vizsgálata így a mélységi védelem kiindulópontja, amely meghatározza a további zónákban alkalmazandó védelmi szinteket és kontrollokat.

Elsődleges védelmi intézkedésként a szervezet részéről egy átfogó, dokumentált és folyamatosan működtetett kockázatmenedzsment-keretrendszer kialakítása és fenntartása szükséges és sok esetben jogszabályi kötelezettség is. [3, 6. § (1)] A szervezetek mindennapi működésük során folyamatosan kockázatokat kezelnek üzleti-működési céljaik elérése érdekében, ideértve többek között a kiberbiztonsági, az ellátási láncok megszakadásából,

vagy a munkavállalók biztonságát érintő kockázatokat. Ennek érdekében olyan folyamatokat kell kialakítaniuk, amelyek lehetővé teszik a működésükkel összefüggő kockázatok értékelését és a kezelésükre vonatkozó döntések meghozatalát a szervezeti prioritások, valamint a belső és külső korlátok figyelembevételével. A kockázatmenedzsment tehát nem lehet egyszeri tevékenység, hanem a mindennapi működésbe ágyazott, folyamatos és iteratív folyamat kell, hogy legyen.[12, p. 44] A kockázatelemzés szerves része a minőség-, környezeti- és információbiztonsági irányítási rendszereknek is, melyek kialakítása egyes szervezetek esetében szintén jogszabályi kötelezettség. [4, 2.2]

A zónához kapcsolódó védelmi intézkedések tehát jellemzően adminisztratív jellegű kontrollok, amelyek a szervezet stratégiai szintű felkészültségét és döntéstámogatását szolgálják. Ide tartozik mindenekelőtt a rendszeres és dokumentált kockázatelemzés, az ellenálló képességi tervek és mátrixok.

Kulcsfontosságú a kritikus függőségek azonosítása, különös tekintettel azokra a külső erőforrásokra és szolgáltatásokra (pl.: közműellátásra, adatkapcsolatokra), beszállítókra amelyek kiesése vagy sérülése aránytalan hatással lehet a szervezet működésére és biztonságára. A környezethez kapcsolódó kontrollintézkedések keretében a szervezet köteles biztosítani a hatóságokkal történő együttműködés és információcsere kialakítását és fenntartását. Célravezető lehet továbbá a nyílt forrású információk (OSINT) monitorozása a szervezetet érintő eseményekről.

Külső zóna

A külső zóna a szervezet közvetlen fizikai környezetét jelenti, amely az objektumhatáron kívül elhelyezkedő területeket foglalja magába, és közvetlen kapcsolatban áll a tágabb környezettel. Ez a zóna képezi a szervezet és a külvilág közötti első érintkezési felületet, ahol a fenyegetések legkorábban megjelenhetnek, ugyanakkor a szervezet befolyása ezen a területen jellemzően továbbra is korlátozott.

Ebbe a zónába tartozhatnak többek között: a közterületek, parkolók és várakozóhelyek, megközelítési útvonalak, a bejáratokhoz, kapukhoz vezető utak, az objektum környezetében található nyílt területek, szomszédos épületek, létesítmények.

Sajátossága, hogy nem kizárólag a szervezet által használt vagy ellenőrzött területeket foglalja magába, mégis jelentős hatással van az objektum biztonságára. A környezeti adottságok, a forgalom jellege, a közvilágítás, a beláthatóság, valamint a szomszédos funkciók mind befolyásolják a későbbi zónákban alkalmazandó védelmi intézkedések kialakítását.

A külső zóna esetében a szervezet elsősorban nem korlátozó, hanem megfigyelő, értékelő és megelőző jellegű tevékenységeket végezhet. A cél nem a teljes kontroll, hanem a fenyegetések korai felismerése, valamint a belsőbb védelmi rétegek megalapozása.

A zónában tipikusan az alábbi tevékenységek végezhetők és szükségesek: a környezeti és biztonsági tényezők folyamatos figyelemmel kísérése (forgalom, események, rendészeti helyzet), amennyiben lehetséges a terület védelmi szempontok szerinti optimalizálása (pl.: kerítés vonalában lévő növénytakaró ritkítása)[4, 2.1], megfigyelési és „elrettentési” eszközök alkalmazása (pl.: közvilágítás, látható kamerák, figyelmeztető jelzések), a megközelítési útvonalak és bejáratok láthatóságának biztosítása, a szomszédos létesítményekből vagy területekről eredő kockázatok azonosítása.

A külső zóna és korlátozottabb mértékig a környezeti zóna esetében a szervezet legnagyobb ráhatása a biztonságra a tervezési szakaszban érvényesül. A beruházási, illetve kivitelezési döntések meghozatala előtt, különösen zöldmezős beruházások esetén kiemelt jelentőségű a létesítmény telepítési helyének megválasztása. [5, 12.49.]

Ebben a fázisban szükséges elvégezni az első, magas szintű kockázatelemzést, amely feltárja a területre jellemző természeti, infrastrukturális, környezeti és biztonsági kockázatokat, és amelynek eredményei alapján kiválasztható az üzletmenet és a biztonság szempontjából leginkább megfelelő helyszín. A nem megfelelő telepítési döntések hosszú távon olyan kockázatokat konzerválhatnak, amik később kizárólag jelentős költségek vagy kompromisszumok árán, bizonyos esetekben pedig még így sem kezelhetők.

Redundáns telephelyek kialakítása esetén a külső zónához kapcsolódó kockázatelemzésnek regionális biztonsági-biztonságpolitikai és akár geológiai szempontokra is ki kell terjednie (pl.: földrengési zónák, tektonikus lemezek elhelyezkedése, időjárási mintázatok).[5, 12.43.]

A külső zónában végzett tevékenységek eredményei közvetlen bemenetet jelentenek a kockázatmenedzsment és a mélységi védelem további szintjei számára, meghatározva az objektumhatáron és azon belül alkalmazandó védelmi intézkedések jellegét és mértékét.

Kiemelt kockázati tényezőt jelentenek az objektum működéséhez szükséges közműellátottsághoz kapcsolódó kritikus függőségek és azok belépési pontjainak védelme [4, 2.2] és esetleges redundanciák kialakításának lehetősége.[4, 2.2] Az energiaellátás, a víz- és csatornahálózat, a gázszolgáltatás, valamint a távközlési és adatátviteli infrastruktúra jellemzően az objektumhatáron kívülről érkezik, így azok sérülékenysége, elérhetősége és védelmi szintje a szervezet közvetlen ellenőrzésén kívül esik. E függőségek megszakadása, történjen akár szándékos beavatkozás, akár műszaki hiba vagy természeti esemény következtében, jelentős működési zavarokat és kaszkádhatásokat idézhet elő, amelyek a belső és privilegizált zónák biztonságát és működését is közvetlenül érintik.

Objektumhatár

Az objektumhatár a szervezet által védett terület fizikai és jogi elválasztási vonala, amely kijelöli a külső, jellemzően nem ellenőrzött környezet és az objektum belső, már szervezeti felelősség alá tartozó területek közötti határt. Az objektumhatár a mélységi védelem egyik kulcseleme, mivel többnyire itt történik meg a nyílt környezetből az ellenőrzött térbe való belépés első szintű szabályozása.

Megjelenési formája a létesítmény jellegétől és kockázati besorolásától függően eltérő lehet. Ide tartozhatnak többek között: a kerítések, falak, kapuk és sorompók, természetes akadályokkal (pl.: vízfelület, terepadottságok) megerősített határvonalak. Abban az esetben amikor a fizikai elválasztás korlátozott mértékben valósítható meg jelölések, táblák és egyéb figyelemfelhívó elemek elhelyezése, egyéb építészeti-tájépítészeti megoldások vagy egyes esetekben akár útfelfestések is hatásosak lehetnek. [11, p. 182]

A zóna elsődleges funkciója nem feltétlenül a behatolás teljes megakadályozása, hanem a fenyegetések észlelésének, az elrettentésnek és a behatolási kísérletek késleltetésének biztosítása. A megfelelően kialakított objektumhatár időt nyer a szervezet számára a reagálásra, és lehetőséget teremt a belső védelmi rétegek aktiválására.

Az alkalmazott védelmi intézkedések kiválasztása során is a kockázatarányosság elvét kell érvényesíteni, figyelembe véve az objektum funkcióját, a fenyegetettségi környezetet és a működési sajátosságokat és jogszabályi előírásokat. [4, 1. mellékelt]

Ennek megfelelően az objektumhatáron tipikusan az alábbi eszközök és megoldások jelennek meg: mechanikai védelmi elemek (kerítések, kapuk, zárak), elektronikus jelző- és érzékelőrendszerek (pl.: kerítésvédelem, mozgásérzékelés), kamerás megfigyelőrendszerek, beléptetési pontok és forgalomszabályozó megoldások, őrzés-védelmi és járőrtevékenységek.

Az objektumhatár nem önálló védelmi elem, hanem a mélységi védelem logikai rendszerébe illeszkedő átmeneti pont a külső zóna és az átmeneti zóna között. Hatékony működése feltételezi a külső zónában végzett megfigyelési és kockázatelemzési tevékenységek eredményeinek eredményes felhasználását, valamint a belsőbb zónákban alkalmazott kontrollokkal való összehangolt működést.

Megfelelő kialakítása és üzemeltetése biztosítja, hogy a belsőbb zónákon belül alkalmazott védelmi intézkedések ne legyenek indokolatlanul túlterhelve, miközben hozzájárul a szervezet fizikai biztonságának, üzletmenet-folytonosságának és rezilienciájának fenntartásához.

Átmeneti zóna

Az átmeneti zóna az objektumhatáron belül elhelyezkedő, de még nem teljes mértékben védett terület, amely átmenetet képez a külső, jellemzően nyilvános vagy korlátozottan ellenőrizhető környezet és a szervezet belső, védett működési területei között. Funkcióját tekintve ez a zóna szolgálja a forgalom szétválasztását, az előzetes ellenőrzést, valamint a belsőbb védelmi rétegek tehermentesítését.

Sajátossága, hogy itt különböző jogosultsági szintű személyek tartózkodhatnak egyidejűleg. Ide tartozhatnak például: látogatók és ügyfelek, beszállítók és alvállalkozók, áruszállítást végző személyek, olyan munkavállalók, akiknek nincs jogosultságuk a belső vagy privilegizált zónákba történő belépésre.

Tipikus átmeneti zónák a recepciók, előterek, várók, egyes tárgyalók, rakodóterületek, árufogadó helyek, közintézmények nyilvánosan hozzáférhető belső és látogatóterei.

A zónában alkalmazott védelmi intézkedéseknek is kiegyensúlyozott módon kell biztosítaniuk a biztonságot és a működés folyamatosságát. Ezért jellemzően csak korlátozott ellenőrzési intézkedések alkalmazhatók, a belépés még nem feltétlenül egyéni jogosultsághoz kötött és a hangsúly a megfigyelésen és elkülönítésen van. A túlzottan szigorú kontrollok itt is akadályozhatják az üzletmenetet (pl.: be- és kiszállítást) vagy a szolgáltatások igénybevételét, míg a nem megfelelő védelem közvetlen kockázatot jelenthet a belsőbb zónákra nézve.

Indokolt lehet a látogatók és külső személyek regisztrációja, előzetes azonosítása, forgalomirányítás és mozgási útvonalak kijelölése, vizuális megfigyelés (pl.: kamerarendszerek, személyzet jelenléte), belépési jogosultságok előkészítése a belső zónák irányába, fizikai elválasztás biztosítása a belsőbb területektől (pl.: ajtók, beléptetőpontok), áruszállítás és logisztikai folyamatok ellenőrzött lebonyolítása.

Az átmeneti zóna hatékony működése kulcsszerepet játszik abban, hogy az illetéktelen személyek ne juthassanak tovább a belső védelmi rétegekbe, miközben a szervezet alaptevékenysége zavartalanul folytatható marad.

Az itt alkalmazott intézkedések célja nem a teljes kizárás, hanem a kockázatok elkülönítése, csökkentése és kezelhető szintre hozása, mielőtt azok a belső vagy privilegizált zónákat érintenék.

Belső zóna

A belső zóna az objektum azon területeit foglalja magában, ahol a szervezet alaptevékenysége ténylegesen megvalósul. Ezek a terek nem nyilvánosak, és kizárólag a megfelelő jogosultsággal rendelkező személyek számára hozzáférhetőek. A belső zóna elválasztása az átmeneti zónától a mélységi védelem egyik meghatározó eleme, mivel a zónában üzletmenetkritikus folyamatok is zajlanak.

A zónába tipikusan az alábbi területek tartoznak: irodák, gyártási és termelési területek, raktárak, laboratóriumok, műhelyek, belső kiszolgáló és adminisztratív helyiségek, tárgyalók és olyan zárt terek, ahol üzleti, technológiai vagy személyes adatok kezelése történik.

Az itt alkalmazott védelmi intézkedések célja már nem csupán az elrettentés vagy az észlelés, hanem a jogosulatlan hozzáférés tényleges, fizikai megakadályozása, valamint a szervezet működésének és erőforrásainak védelme. Ennek megfelelően a belépés ebbe a zónába szabályozott és dokumentált, jellemzően egyéni jogosultságokhoz kötött kell hogy legyen. A zónában található munkaterületek további jogosultság alapú elkülönítése is indokolt lehet.[13, p. 6]

A védelem kialakítását ezért jogosultságon alapuló hozzáférés („need to access” elv), a munkakörhöz és feladatokhoz igazított hozzáférési szintek, a fizikai és szervezeti kontrollok összehangolt alkalmazása kell hogy meghatározza.

A mélységi védelem rendszerében a belső zóna a védelmi intézkedések súlypontját jelenti. Míg a külső és átmeneti zónák célja a fenyegetések kiszűrése és csökkentése, addig a belső zóna biztosítja, hogy az objektumba jutott személyek és eszközök csak a szükséges mértékben és ellenőrzött körülmények között férhessenek hozzá a szervezet erőforrásaihoz, valamint előkészíti a legmagasabb védelmi szintet képviselő privilegizált zóna elkülönítését.

Privilegizált zóna

A privilegizált zóna a szervezet objektumán belül kialakított legmagasabb védelmi szintű terület, amely azokat a helyiségeket és funkcionális egységeket foglalja magába, ahol a szervezet működése szempontjából kiemelten érzékeny erőforrások, információk vagy személyek találhatók. A zóna védelme alapvetően meghatározza a szervezet ellenálló képességét, mivel az itt bekövetkező biztonsági incidensek aránytalanul nagy hatással lehetnek az üzletmenetre, a jogszabályi megfelelésre és reputációra.

A zónába tartozhatnak többek között a felsővezetői irodák és tárgyalók, szerverszobák, adatközponti helyiségek, biztonsági szobák, kritikus irattárak, ipari és kritikus infrastruktúra esetén vezérlőtermek, irányítóközpontok.

Az ebben a zónában alkalmazott védelmi intézkedések célja nem csupán a jogosulatlan hozzáférés megakadályozása, hanem a belső fenyegetések minimalizálása, valamint az egyes események gyors és pontos visszakövethetőségének biztosítása. Ennek megfelelően a belépés kizárólag szigorúan szabályozott, személyre szabott és dokumentált jogosultságok alapján történhet, valamint a legkisebb jogosultság elvének (least privilege)[4, 2.1] is érvényesülnie kell.

A zónában alkalmazott intézkedések jellemzően: többtényezős fizikai azonosítás (pl.: belépőkártya + kód), belépések és jelenlét részletes naplózása, folyamatos vagy eseményvezérelt kamerás megfigyelés, kísérési kötelezettség külső vagy ideiglenes jogosultságú személyek esetén, négyszem-elv alkalmazása, rendszeres jogosultság-felülvizsgálat és audit, környezeti paraméterek (pl.: hőmérsékelt, páratartalom) folyamatos monitorozása valamint a rendkívüli eseményekre vonatkozó speciális eljárások (pl.: vészhelyzeti belépés). Ezen intézkedések célja nem kizárólag a külső támadások kivédése, hanem a belső visszaélések, emberi és műszaki hibák és szándékos károkozás kockázatának csökkentése is.

Minta kialakítás

Zóna	Elhelyezkedés	Tipikus szereplők	Fő cél	Egy-egy a zónára jellemző védelmi intézkedés
Környezet	Objektumhatáron kívül, tágabb környezet	Lakosság, közlekedők, külső szereplők	Fenyegetések azonosítása, kontextus megértése	A kritikus szervezet kockázatértékelése: „felméri és dokumentálja a kritikus szervezet és a kritikus infrastruktúra fenyegetettségét, fenyegetést jelentő kockázatait, amelyek rendkívüli eseményhez vezethetnek, meghatározza az azonosított fenyegetések káros hatásait és azok mértékét, a fenyegetések káros hatásainak és azok bekövetkezésének valószínűségét, és a kitettség mértékét” [4, 15. § (1)]
Külső zóna	Objektumhatáron kívül, közvetlen környezet	Belépő és külső személyek	Korai észlelés, elrettentés	Létesítmény elhelyezkedése: „Figyelembe veszi a fizikai és környezeti veszélyeket az EIR-nek helyet adó létesítmény megtervezésekor. A meglévő létesítményeknél figyelembe veszi a szervezeti kockázatmenedzsment stratégiában szereplő fizikai és környezeti veszélyeket.” [5, 12.49.]
Objektumhatár	Objektumhatáron	Belépő személyek	Elválasztás, késleltetés, ellenőrzés	„a létesítmény belépési pontjain biztosítja a személyek és járművek biztonsági (átvilágítás, átvizsgálás, tiltott tárgyak kutatása) ellenőrzését” [4, 2.2. -9]

Zóna	Elhelyezkedés	Tipikus szereplők	Fő cél	Egy-egy a zónára jellemző védelmi intézkedés
Átmeneti zóna	Objektumhatáron belül	Látogatók, beszállítók, korlátozott jogosultságú dolgozók	Szűrés, forgalomszabályozás	Belátás- és rálátásvédelem: minden olyan területen biztosítani kell, ahol járműveket vagy formatervezés szempontjából releváns alkatrészeket/komponenseket dolgoznak fel vagy tárolnak. Ez magában foglalja az épületek vonatkozó üvegfelületeit, valamint azokat a védelmi intézkedéseket, amelyek megakadályozzák a belátást nyitott ajtókon, kapukon vagy ablakokon keresztül. [13 p. 5]
Belső zóna	Objektum belseje	Munkavállalók	Jogosulatlan hozzáférés megakadályozása	A fizikai hozzáférések felügyelete: „Ellenőrzi a fizikai hozzáféréseket az elektronikus információs rendszereket tartalmazó létesítményekben, hogy észlelje a fizikai biztonsági eseményeket és reagáljon rájuk.” [5, 12.17.]
Privilegizált zóna	Objektum legvédettebb részei (vezetői irodák, szerverszobák)	Korlátozott számú (privilégizált) jogosult	Kritikus erőforrások védelme	Környezeti védelmi intézkedések: „Meghatározott biztonságos szinten tartja a hőmérsékletet, a páratartalmat, a légnyomást és a sugárzást az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (például: adatközpont, szerver szoba, központi gépterem).” [5, 12.37.]

1. táblázat. Megjegyzés: a környezet nem védelmi zóna szűk értelemben, de a kockázatmenedzsment-alapját képezi. A felsorolt egy-egy védelmi intézkedés példa jellegű és a tanulmányban említett jogszabályokból és szabványokból került kiválasztásra.

ÖSSZEFOGLALÁS

A bemutatott többrétegű modell a mélységi védelem elveire építve olyan strukturált, kockázatalapú megközelítést kínál, amely egyszerre támogatja a szervezetek zárt, teljes körű, folytonos és a kockázatokkal arányos védelemének kialakítását, üzletmenet-folytonosságának fenntartását és jogszabályi megfelelését. A modell nem új követelményeket vezet be, hanem a jelenleg hatályos hazai és európai szabályozási környezet – különösen a NIS2 és a CER irányelvek és a jogharmonizáció során megalkotott hazai jogszabályok – által megfogalmazott elvárásokat ülteti át a fizikai térben értelmezhető, gyakorlati struktúrába.

A zónák egymásra épülő kialakítása lehetővé teszi a kockázatarányos védelem megvalósítását: a szervezet nem egységesen, hanem a tényleges fenyegetettségek alapján alkalmaz eltérő szintű intézkedéseket. Ez összhangban áll a nemzetközi szabványok, így az ISO/IEC 27001, a TISAX, valamint a NIST-alapú kockázatmenedzsment-keretrendszerek alapelveivel is, amelyek a kockázatok azonosítását, értékelését és arányos kezelését helyezik előtérbe.

A modell alkalmazása egyúttal hozzájárul a szervezeti reziliencia növeléséhez, mivel a fizikai, szervezeti és humán kontrollok egységes rendszerben jelennek meg, csökkentve az egyedi hibákból vagy incidensekből fakadó kaszkádhatások kialakulásának esélyét. A mélységi, zónás szemlélet így nem pusztán megfelelési eszköz, hanem egy hosszútávon fenntartható, ellenálló és átlátható fizikai biztonsági architektúra alapja.

IRODALOMJEGYZÉK

[1] Charlie Edwards, Senior Adviser, Strategy and National Security; Nate Seidenstein, Research Assistant (2025 augusztus) The International Institute for Strategic Studies, The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure Forrás: https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

[2] 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről és

[3] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

[4] 474/2024. (XII. 31.) Korm. rendelet Kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról

[5] 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

[6] 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

[7] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

[8] Az Európai Parlament és a Tanács (EU) 2022/2557irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (CER irányelv)

[9] Premier ministre; Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil La défense en profondeur appliquée aux systèmes d'information, La défense en profondeur appliquée aux systèmes d'information - Mémento Forrás: https://messervices.cyber.gouv.fr/documents-guides/mementodep-v1-1.pdf

[10] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team September 2016 Forrás: https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[11] National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology Joint Task Force NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations Forrás: https://doi.org/10.6028/NIST.SP.800-53r5

[12] Stouffer K, Pease M, Tang CY, Zimmerman T, Pillitteri V, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M (2023) Title. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-82r3. Forrás: https://doi.org/10.6028/NIST.SP.800-82r3

[13] Verband der Automobilindustrie Minimum requirements for prototype protection in the German automotive industry Version: 3.0 Date: November 07, 2018 Forrás: https://www.vda.de/dam/jcr:855b28fe-fc1b-4819-bd49-f282f2ff754b/20181107_VDA_Minimum_Requirements_for_Prototype_Protection_Version3.pdf?mode=view

DOI: https://doi.org/10.12700/btsz.2026.8.1.67

CHALLENGES OF DEVELOPING ORGANIZATIONAL AND SAFETY CULTURE IN THE HUNGARIAN PRIVATE SECURITY SECTOR

A SZERVEZETI ÉS BIZTONSÁGI KULTÚRA FEJLESZTÉSÉNEK KIHÍVÁSAI A MAGYAR MAGÁNBIZTONSÁGI SZEKTORBAN[1]

KOLLÁR Csaba[2]

Abstract

The study analyzes the interrelation between organizational and safety culture in the private security sector, focusing on the possibilities for improving security awareness. It highlights how structural dependencies, informal employment, limited employee recognition, and the absence of strategic planning influence organizational behavior, philosophy, and identity. Building on Schein's iceberg model of organizational culture, as well as the concepts of Robbins and Juhász–Vasvári, the paper emphasizes the importance of managerial commitment, learning-driven safety environments, and ethical corporate behavior. It proposes conceptual and practical measures—such as targeted training and internal auditing—to strengthen safety culture and awareness within private security companies, contributing to more professional and sustainable sectoral development.

Keywords

safety culture, organizational culture, security awareness, private security, organizational philosophy, risk management

Absztrakt

A tanulmány a magánbiztonsági szektor szervezeti és biztonsági kultúrájának összefüggéseit vizsgálja, különös tekintettel a biztonságtudatosság fejlesztésének lehetőségeire. A szerző rámutat arra, hogy a szektor sajátosságait – mint a hierarchikus függelmi viszonyokat, a feketefoglalkoztatást, az alacsony munkaerő-megbecsülést és a stratégiai gondolkodás hiányát – miként befolyásolják a szervezeti viselkedés, filozófia és identitás elemei. Az elemzés a Schein-féle szervezeti kultúra jéghegy-modelljére, valamint Robbins és Juhász–Vasvári biztonsági kultúra-elméleteire épül. A tanulmány felhívja a figyelmet a vezetői példamutatás, a tanulásvezérelt biztonsági környezet és az etikus szervezeti működés fontosságára, továbbá javaslatot tesz a biztonsági kultúra és a biztonságtudatosság fejlesztését elősegítő oktatási és ellenőrzési mechanizmusokra a magánbiztonsági vállalkozások működésében.

Kulcsszavak

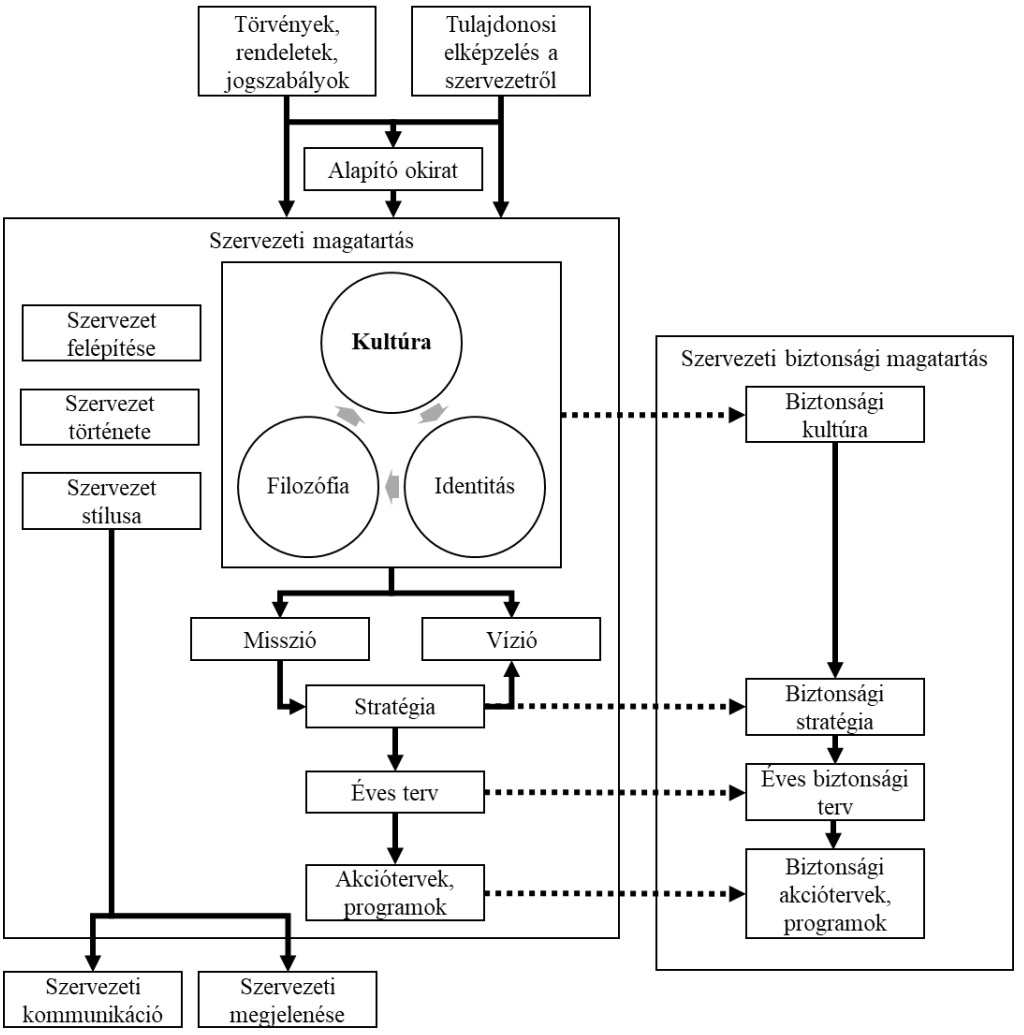
biztonsági kultúra, szervezeti kultúra, biztonságtudatosság, magánbiztonság, szervezeti filozófia, kockázatmenedzsment

[1] A tanulmány alapja a szerző „A magyarországi magánbiztonsági szektor elemzése, fejlődésének lehetséges irányai" (témavezető: Prof. Em. Dr. Berek Lajos) című doktori értekezése.

[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 alábbiakban az 1. ábra magyarázatát adom meg a magánbiztonsági szektor vállalkozásainak fókuszában. A megfelelő anyagi háttérrel és kellő vállalkozói kedvvel, vagy rosszabb esetben kényszerből vállalkozásba kezdő (leendő) tulajdonosnak rendelkeznie kell(ene) valamilyen elképzelésének arról, hogy a magánbiztonság területén milyen jellegű tevékenységet, kik számára, s hozzávetőlegesen milyen árakon kíván szolgáltatni. Egy, az induláskor néhány fős vállalkozás nem tudja a magánbiztonsági szektor teljes szolgáltatási palettáját kínálni, s az sem biztos, hogy egy komoly összeggel induló vállalkozás akkor jár el helyesen, ha már induláskor a teljes palettát kívánja szolgáltatni. Bár a rendszerint egyéni vállalkozásként, esetleg betéti társaságként induló kényszervállalkozókat nem jellemzi az említett tudatosság, de még esetükben is érdemes lenne egy külsős tanácsadó, vagy a Kamara segítségét igénybe venni.



1. ábra: A biztonság és a biztonsági kultúra megjelenése a szervezetben ([5], [6], [7], [8] alapján saját szerkesztés)

Ennek díja később kamatostul megtérülhet. Az elképzelések és a magánbiztonsági szektorra vonatkozó törvények, rendeletek, jogszabályok együttesen adják azt a hátteret, ami alapján az egyéni vállalkozás bejelentéssel, a társas vállalkozás ügyvéd által ellenjegyzett társasági szerződéssel (bt.), alapító okirattal (kft.), alapszabállyal (rt.) és cégbírósági bejegyzéssel jön létre. Az alapító okirat, illetve annak cégbírósági ellenjegyzése adja meg a jogalapot a vállalkozás működéséhez.

Az alapító okiratban meg kell adni a cég tevékenységét, ami esetünkben általában a következő főtevékenységeket jelenti [9]:

- 8001 Személybiztonsági tevékenység (korábban: 8010 Személybiztonsági tevékenység, illetve 8030 Nyomozás): Ebbe a szakágazatba tartozik: nyomozói szolgáltatások magán-, kereskedelmi, biztosítási és jogi területen, őrző-, járőr- vagy biztonsági szolgálat, készpénzbeszedési és -befizetési szolgáltatásokhoz nyújtott támogató szolgáltatások, biztonságos iratmegsemmisítés és adatmegsemmisítés, páncélautós szolgáltatás. Ebbe a szakágazatba tartozik még: őrző- és biztonsági szolgáltatások, pl. üzletek, baleseti központok számára, poggyász- és utasellenőrzés repülőtereken, vasútállomásokon és más hasonló helyeken, rendezvények, koncertek, vásárok és kiállítások biztonsági személyzetének tevékenysége. Nem ebbe a szakágazatba tartozik: biztonsági tanácsadás és szaktanácsadás (8009), távfelügyeleti tevékenység (8009), portaszolgálat, recepció (8110, 8210), közrend- és közbiztonsági tevékenység (8424), biztonság, beleértve a kiberbiztonsági képzést is (8559).
- 8009 M.n.s. biztonsági tevékenység (korábban: 8020 Biztonsági rendszer szolgáltatás) Ebbe a szakágazatba tartozik a következő szolgáltatások közül egy vagy több szolgáltatás nyújtása: biztonsági rendszerek szolgáltatása biztonsági szolgáltató központok vagy riasztásfogadó központok (ARC) részeként, távfelügyeleti és videómegfigyelő rendszerek szolgáltatása, elektronikus biztonsági rendszerek telepítése, javítása és karbantartása abban az esetben, ha a későbbi felügyeleti és távfelügyeleti szolgáltatásokkal összefüggésben nyújtják. Ebbe a szakágazatba tartozik még: biztonsági tanácsadás, segélyhívó és szolgáltató központban vagy riasztásfogadó központban (ARC) végzett tevékenységek, elektronikus biztonsági rendszerek, pl. betörésjelzők, videómegfigyelő rendszerek, tűzjelzők felügyelete és távfelügyelete, mechanikus vagy elektronikus zárszerkezetek, széfek és páncélszekrények felügyelete és távfelügyelete, elektronikus biztonsági rendszerek, pl. betörés- vagy lopásjelzők, videómegfigyelő rendszerek, tűzjelzők telepítése és karbantartása, amennyiben a későbbi megfigyelő és távfelügyeleti szolgáltatásokkal összefüggésben nyújtják azokat, mechanikus vagy elektronikus zárszerkezetek, elektronikus biztonsági rendszerek, széfek és páncélszekrények telepítése, javítása és átalakítása, amennyiben a későbbi felügyeleti és távfelügyeleti szolgáltatásokkal összefüggésben történik. Nem ebbe a szakágazatba tartozik: biztonsági rendszerek, így pl. betörésvédelmi, megfigyelőrendszerek, tűzjelző rendszerek telepítése, későbbi felügyeleti és távfelügyeleti szolgáltatások nélkül (4321), elektromos biztonsági riasztórendszer, mechanikus vagy elektronikus zárszerkezet, széf, biztonsági páncélszekrény kiskereskedelme, későbbi felügyeleti, telepítési vagy karbantartási szolgáltatás nélkül (4752), kiberbiztonsági tanácsadás (6220), közrendvédelmi, közbiztonsági tevékenység, pl. rendőri tevékenység (8424), kulcsmásolási szolgáltatás (9529).

A SZERVEZETI MAGATARTÁS

A szervezeti magatartás a vállalat egységes, érvényes magatartását jelenti, következményeivel és kihívásaival együtt [7]. Sándor [10] Birkigt és Stadler alapján a szervezeti magatartással kapcsolatban úgy vélekedik, hogy magában foglalja valamennyi külső és belső célcsoport iránti magatartását minden dolgozó részéről. A szervezeti magatartás a vállalat egészének magatartását, viselkedését jelenti a közvélemény felé, melyet a cég tulajdonosai, menedzsmentje és az összes alkalmazottja közvetít. A szervezeti magatartás részei a kultúra-identitás-filozófia hármasa, a szervezet felépítése, története, stílusa, missziója, víziója, stratégiája, tervei, akciói, kommunikációja és megjelenése. A szervezetek biztonsági magatartására a szervezeti magatartás része. A szervezeti magatartásban ismertetésre kerülő fogalmak – ahogy az az ábrán látható – jobb esetben a biztonság fókuszában megfeleltethetők a biztonsági magatartás egy-egy fogalmával is. A szervezetek biztonsági magatartása egyfelől azt jelenti, hogy a szervezet valamennyi alkalmazottja olyan magatartást tanúsít, ami révén megelőzhetők a munkahelyi balesetek, sérülések és az adat- és információbiztonsággal kapcsolatos visszaélések, másfelől pedig azt, hogy a szervezet menedzsmentje mindent megtesz annak érdekében, hogy biztonságos munkakörnyezetet teremtsen, felmérje a biztonsági és egészségi kockázati tényezőket, intézkedéseket hozzon ezek mérséklésére, vagy elkerülésére, szabályozza a munkavégzéssel és adat-, illetve információbiztonsággal kapcsolatos tevékenységeket (és ezek betartását időközönként le is ellenőrzi). Kérdés, hogy a szervezeti kultúra-filozófia-identitás hármasában milyen értékeket fogalmaz meg a magánbiztonsági vállalkozás.

A SZERVEZETI KULTÚRA

A szakirodalmi feldolgozás alapján a magánbiztonsági vállalkozások szervezeti kultúrájával is foglalkozó írások között Szabó doktori disszertációját [4], illetve Szabó [11] tanulmányát ismertem meg, valamint témahasonlóság okán a rendőrség és a honvédség szervezeti kultúrájával foglalkozó műveket is elemeztem, nevezetesen: Pirger [12] doktori disszertációját, Laczó [13] diplomamunkáját, Kovács [14], Krizbai [15] és Elekes [16] és Horváth [17] tanulmányát. Említett szerzők írásaiban közösek az átlaghoz képest hangsúlyosabban megjelenő függelmi viszonyok, az alá- és fölérendeltség kérdése, a szolgálati, illetve őrzés-védelmi szabályzat betartása, a vezető személyes biztonságtudatossági példamutatása. A szervezeti kultúráról alkotott képet árnyalja, hogy Elekes [16 p. 32] egyet ért Horváthtal [17] abban, hogy „A rendőrség működésében, mint alapvetően segítő, szolgáltató, de részben militarista szervezetben, a »hatalomkultúra«, a »szerepkultúra« és a »feladat-kultúra« elemei vegyesen jelennek meg (Handy-féle felosztás szerint), (vagyis) … a szervezeten belül ugyanolyan jelenségek is megtapasztalhatók, mint más szervezeteknél". Meglátásom szerint a nem rendőri, honvédségi, (magán)biztonsági szervezeteknél/egységeknél az általános szervezeti kultúra, s az abból levezethető biztonsági kultúra a menedzsment modern értelmezése szerint elsősorban nem a hatalomkultúrában keresendő, ugyanakkor a veszélyes üzemeknél, illetve a szigorú törvényi, rendeleti, vagy vállalati szabályzatok miatt megjelenhetnek a szervezeti kultúrában hatalomkultúra-elemek is (pl.: a biztonsági szabályok be nem tartása miatti komoly felelősségre vonás). A szervezeti kultúrával foglalkozó tanulmányok gyakran idézik Schein [18] jéghegy modelljét, ahol a vízfelszín

feletti rész (a szervezeti kultúra megjelenése) a mindenki által látható, írásos formában jelenlevő, vagy 'hétköznapi' megfigyeléssel is jól kivehető szervezeti jellemzőket (pl.: hiedelmek, szokások, értékek, normák) foglalja magába. A biztonsági kultúra vonatkozásában ez a magánbiztonsági szektor vállalkozásainak belső biztonsági és információbiztonsági szabályzatait (pl.: őrszolgálati szabályzat, pénz- és értékszállítási szabályzat, titok- és adatvédelmi szabályzat, eseménykezelési szabályzat, munka-, tűz, és balesetvédelmi szabályzat), biztonságpolitikáját, a biztonsággal és biztonságtudatossággal kapcsolatos eljárásokat, képzéseket, továbbképzéseket, ellenőrzéseket jelenti. A jéghegy modellben a vízfelszín alatti, nem látható részek (szervezeti kultúra mélystruktúrája) határozzák meg a szervezet valódi kultúráját, azt, hogy a szervezet hogyan gondolkodik és cselekszik, milyen valódi értékrendeket vallanak magukénak a beosztottak, illetve a vezetők, mi motiválja tevékenységüket. A kultúra, s így a biztonsági kultúra mélystruktúrája az, aminek megismerése révén dolgozhatók ki olyan oktatási és képzési programok, amelyek hozzá tudnak járulni a munkavállalók biztonságtudatosságának a fejlesztéséhez. Amikor egy megfelelő végzettséggel rendelkező munkavállaló jelentkezik egy magánbiztonsági vállalkozás álláshirdetésére, akkor önéletrajzából, a felvételi beszélgetésen elhangzottakból, esetleg a kitöltetett alkalmassági tesztekből következtetni lehet a leendő munkatárs biztonsági kultúrájára is. Sikeres felvétele esetén természetesen ő is alakítani tudja – igaz, rendszerint kisebb mértékben – új munkahelye biztonsági kultúráját, s hozzá tud járulni annak fejlődéséhez, de a hatás markánsabban jelenik meg vele szemben: az ott dolgozó beosztottak és vezetők biztonsági attitűdje erősebb irányába. Ha az egyén biztonsági kultúrája és a magánbiztonsági szervezet biztonsági kultúrája és elvárásai között komolyabb különbség van, akkor az az egyén számára kognitív biztonsági disszonanciaként jelentkezhet, pl.: egészségre veszélyes anyagok őrzése során a vállalat és maguk a dolgozók sem foglalkoznak a biztonsági őrök személyes biztonságával, miközben az új kolléga speciális védőfelszerelés hiányában nem akar őrző-védő tevékenységet végezni az objektum területén. A szervezeti kultúrát, s így a szervezeti biztonsági kultúrát sem lehet gyorsan alakítani, megváltoztatni. Ugyan eredményesebbnek tűnhet a már meglevő kultúrán belül nagyobb biztonsági teljesítményt elérni, semmint megváltoztatni a mélyen gyökerező értékeket, szokásokat, gyakorlatokat és hiedelmeket (ahogy erről az Országos Atomenergia Hivatal [19] kiadványának készítői vélekednek), ugyanakkor véleményem szerint a biztonságtechnikában és domotikában megjelenő új berendezések, valamint – különösen az alvállalkozóként tevékenykedő magánbiztonsági vállalkozások esetében előforduló – más adottságokkal és szigorúbb biztonsági protokollokkal rendelkező objektumok őrzése megkívánja, hogy a munkavállalók nagyon rövid időn belül alkalmazkodjanak az új követelményekhez. Hivatkozott [19] mű a biztonsági kultúra öt jellemzőjét nevezi meg, úgymint:

1. **A biztonság egyértelműen felismert**: biztonsággal kapcsolatos eljárásrendek hozzáférhetősége, biztonsági jelzések megléte és használata.
2. **A biztonságért való felelősségre vonhatóság egyértelmű**: minden munkavállaló számára egyértelműek a biztonsággal kapcsolatban hozott szervezeti előírások.
3. **A biztonság tanulás-vezérelt**: a szervezeti kultúra aktívan támogatja a munkavállalókat, hogy a biztonsággal kapcsolatos ismereteiket fejlesszék, illetve a szervezeti tanulás 'eredménytermékei' a biztonsági kultúra és a biztonságtudatosság területén is hasznosulnak.

4. **A biztonság minden tevékenységben integrált**: a biztonság levezethető a kultúrából egészen a napi rutin valamennyi tevékenységéhez.
5. **A vezetőség elkötelezettsége a biztonság felé egyértelmű**: a személyes vezetői példa fontossága.

Robbins [20] (hivatkozza Pirger [12]) a szervezeti kultúra építőkövei között tizenegy értéket nevezett meg, melyek saját értelmezésben a magánbiztonsági szektor vállalkozásainak esetében a következők:

1. **Munkakörrel vagy a szervezettel való azonosulás**: ezzel kapcsolatban az általam elemzett szakirodalom nem képvisel egységes álláspontot. Egyfelől Szabó [11 p. 292] kiemeli, hogy az őrzésbiztonsági területen számos a rend- és a honvédelemben dolgozó szakember vesz részt, „szemléletmódjuk, tapasztalatuk formálta, és ennél fogva meghatározta a szakterület alapjait az eljárásokban, a gondolkodásmódban, szokások kialakításában, és a kialakult vezetési stílusban is". Ez jó. Másfelől Christián és Rottler [2 p. 166], illetve Fábián [1 p. 30] egyaránt utal a foglalkoztatási anomáliákra, a feketefoglalkoztatásra. Ez rossz, mivel az a személy, aki papírok, munkaszerződés nélkül dolgozik, nem képes és nem is tud azonosulni a munkaszervezettel.
2. **Egyén- vagy csoportközpontúság** (individualizmus-kollektivizmus): az általam elemzett szakmai szereplőket tömörítő Facebook csoportokban folyó beszélgetés alapján a szektor munkavállalóira inkább az individualista, semmint a kollektivista viselkedés jellemző. Természetesen a munkahelyi barátságok kialakulását kutatásaim során én is tapasztaltam, ahogy a volt katonák/rendőrök esetében a bajtárs (surranótárs) kifejezéssel is találkoztam, de összességében ez csak szűk, néhány fős közösségekre volt jellemző, a magánbiztonsági szektor egészének munkavállalóira nem. Ezt az állításomat annak ellenére is fenntartom, hogy a közös sors (agresszív vezető, bizonytalan jövő, hasonlóan rossz munkakörülmények, alacsony bérek) elvben össze tudná kovácsolni a különböző mentalitású embereket, de ez ebben a szektorban nem történt meg.
3. **Humán-orientáció**: a magánbiztonsági szektor vezetőinek, különösen a nagyobb vállalatok felsővezetőinek többsége nem veszi fontolóra a szervezeti feladatok megoldásának hatását és következményeit a munkavállalókra. Az említett feketefoglalkoztatás, az adó- és egyéb járulékfizetési kötelezettségek elkerülése, a munkaerőhiány miatti szinte állandó átszervezések és a szolgálat lejártakor bejelentett túlórakötelezettség (második szolgálat felvétele a kötelező pihenőidő kiadása nélkül) igazolják ezt.
4. **Belső függés/függetlenség**: a már említett forrás [11] alapján kijelenthető, hogy a szektor munkavállalóinak és kisebb szervezeti egységeinek koordinált cselekvése alapkövetelmény (kellene, hogy legyen). A nagyobb sport- és kulturális és egy tömegrendezvények megkövetelik ugyanis azt, hogy a különböző kisebb egységek gyorsan tudjanak reagálni egy nem várt eseményre, s e reagálás a többi kisebb egységgel a parancsnoki/vezetői utasításoknak megfelelően összehangolt legyen.
5. **Erős/gyenge kontroll**: a magánbiztonsági szektor munkavállalóinak viselkedését a vállalkozások előírásokkal, szabályzatokkal, közvetlen felügyelettel rendszeresen ellenőrzik – ami a hagyományos őrző-védő tevékenységeket illeti. Ugyanakkor az

adat- és információbiztonság területén komoly hiányosságok, felszínesség tapasztalható.

6. **Kockázatvállalás/kockázatkerülés**: ahogy arra a magánbiztonsági szektor makrokörnyezetének elemzésénél utaltam, a klasszikus területek/témák vonatkozásában rendelkezésre állnak azok a tankönyvek, melyek a munkavállalók törvényes és jogszerű magatartásához és munkavégzéséhez szükséges ismereteket tartalmazzák. A magabiztos, határozott fellépés alapvető elvárás, akárcsak a problémák fizikai erőszakba fordulásának elkerülése is. A munkatársaktól tehát elvárás az ésszerű kockázat vállalása, ugyanakkor egy demotivált munkavállaló – hacsak egyébként nem kockázatvállaló típus – erre nem képes.
7. **Teljesítményorientáció**: sajnos a magánbiztonsági szektor vonatkozásában nem, vagy csak elenyésző mértékben van jelen a jutalmazás. A feladat sikeres elvégzése után maximum szóbeli köszönetet kapnak az őrzés-védés területén tevékenykedő munkavállalók, de a gyakoribb az, hogy még azt sem. A szektor vezetőinek többsége sajnos magától értetődőnek veszi, hogy a minibál környékén foglalkoztatott munkavállaló a feladatát elvégzi, ezért a fizetését (jobb esetben) megkapja, s nem tartja fontosnak az ezen felüli teljesítményelismerést.
8. **Konfliktustűrés/konfliktuskerülés**: a magánbiztonsági szektor karakteresebb, elsősorban honvédségi és rendőrségi múlttal rendelkező, de már leszerelt munkavállalói annak ellenére, hogy a feladatokat elvégzik, gyakran fogalmaznak meg kritikát elöljáróikkal kapcsolatban, különösen akkor, ha azok nem rendelkeznek kellően megalapozott ismeretekkel az őrzés-védelem területén. A csak sorkatonai múlttal, vagy azzal sem rendelkező munkavállalók kritikáinak narratívái inkább a munkakörülményekre, a vezető stílusára vonatkoznak. Tehát: az első esetben a kritika inkább objektív tényeken, az utóbbinál inkább szubjektív érzéseken alapul.
9. **Cél- (eredmény-) - eszköz- (folyamat-) orientáció**: nehéz egyértelműen meghatározni, hogy a vezetés a végső eredményre, vagy inkább az eredményhez vezető folyamokra, technikákra koncentrál-e. Meglátásom szerint a célorientáltság inkább jellemzi a magánbiztonsági szektort, erre utalhatnak olyan narratív foszlányok, mint 'meg kell csinálni', 'el kell végezni', s e tevékenységek során a folyamat lépéseit (jobb esetben) eljárásrendek követik.
10. **Nyílt rendszer (külső) – zárt rendszer (belső) orientáltság**: a magánbiztonsági szektor vállalkozásai alapvetően nem reagálnak a külső környezet változásaira, nem előidézői, inkább passzív elszenvedői azoknak. A szektor helyzete miatt a vállalkozások többsége inkább saját belső működésére, a meglevő szerződések szerinti munkák elvégzésére, s a járandóság időben történő, megbízó általi kifizetésére koncentrál.
11. **Rövid, vagy hosszú távú időorientáció**: a korábban említett jó politikai kapcsolatokkal rendelkező, néhány nagy magánbiztonsági vállalatától eltekintve a szektor vállalkozásainak jelentős része a szervezet egyértelműen rövid időhorizonton tervezi a jövőjét.

Juhász és Vasvári [21 p. 55] saját kutatási eredményei alapján arra a következtetésre jut, hogy „(fejlett) biztonsági kultúráról akkor beszélhetünk, ha a szervezeti hierarchia minden szintjén a munkavállalók folyamatosan törekednek a veszélyforrások feltárására, tuda-

tosítására és a kockázatok csökkentésére. A szervezeti biztonsági kultúra minősége, fejlettségi szintje, hatással van a biztonságtudatos magatartásból fakadó döntésekre, amely visszahat a biztonsági kultúrára. A kockázatok kezelésével kapcsolatos döntések során, a biztonsági kultúrába beépülő rendszerek elemei (pl.: szabályozási keretrendszer, törvények stb.) hatékony működtetése nagyban függ a kockázatok és bizonytalanságok kezeléséhez kapcsolódó attitűdöktől, magatartásformáktól".

A SZERVEZETI FILOZÓFIA

A szervezeti filozófia az a kiértékelt és egyértelműen megfogalmazott gondolatiság, amely a szervezet valamennyi tevékenységét, aktivitását, cselekvését áthatja [7], olyan értékeket tudatosít, melyek zsinórmértékként szolgálhatnak a vállalat valamennyi belső és bizonyos esetekben külső érintettjei számára. A szervezeti filozófiában megjelenik, hogy a szervezet mit gondol magáról, a kollektíváról, a szolgáltatásairól/termékeiről, hogyan látja magát munkaadóként, piaci szereplőként, a társadalom hasznos szervezeteként. Alapvetően három szervezeti filozófiát tudunk megkülönböztetni aszerint, hogy inkább a politikai töltet, a szervezeti cselekvés vezérelvei, vagy inkább a szervezet társadalmi szerepét, felelősségét kiemelő fókusz van-e túlsúlyban. A magánbiztonsági szektor vállalkozásait inkább a politikai töltetű filozófia jellemzi, mivel elsősorban a szervezethez kapcsolódó érdekcsoportok elvárásainak való megfelelést helyezik a középpontba, egyben rangsorolva is azokat. Az ilyen filozófia inkább a szervezet külső érintettjeihez szól, munkavállalóihoz nem, vagy csak alig. A szervezeti filozófia hangsúlyának eltolása a szervezet társadalmi szerepére és felelősségére nem csak a szektor vállalkozásainak kedvezőbb közmegítélését eredményezné, hanem elősegítené a munkavállalók jobb közérzetét is. A szervezeti filozófiából levezethető szervezeti biztonsági filozófia a leírtak alapján arra koncentrál, hogy ha munkavédelmi vagy adóhivatali ellenőrzést kap a magánbiztonsági vállalkozás, akkor a büntetést elkerüljék, vagy legalább annak mértéke még elviselhető legyen. Emiatt a szabályos és szabványos egyéni munkavédelmi felszerelések gyakran egy másod-harmadosztályú fekete színű katonai gyakorlónadrágban, vagy a cég logójával szitázott pólóban jelennek meg. Az egész napos állásban is a láb kényelmét biztosító cipő, vagy a hidegebb időben is komfortot biztosító kabát, vagy ülőmunka esetén egy kényelmesebb szék, az egésznapos monitorfigyelés érdekében védőszemüveg, vagy váltótárs alkalmazásával a szem pihenési idejének biztosítása, a COVID alatt biztosított szájmaszk és kézfertőtlenítő, a biztonságirendszer szerelőknek az acélbetétes, 1000V-ig szigetelt talpú munkavédelmi bakancs – hogy csak a fontosabb alapvető elvárásokat említsem – rendszerint nem állnak rendelkezésre, nem valósulnak meg.

MISSZIÓ, VÍZIÓ, STRATÉGIA

A szervezeti kultúra-filozófia-identitás hármasa adja az alapot a misszió-vízió-stratégia hármasához. Értelmezésemben a misszió az út kezdetét, a vízió az út végét, a stratégia pedig magát az utat jelenti. A misszió a filozófiához hasonlóan választ ad a 'miért vagyunk', mi a 'küldetésünk' kérdésre, de hozzá képest ezt konkrétabban teszi. A misszió követhető a szervezet bármely munkatársa, bármely alrendszere számára. Amikor a misszió a magánbiztonsági szektor vállalkozásainál gyakran a tulajdonos 'még nagyobb házában' és 'még

újabb autójában' realizálódik, akkor a munkavállalók az egyébként esetleg szépen megfogalmazott missziót sem érzik a magukénak. Bár tankönyv szerint [7] a misszió világosan fogalmaz a cél, a stratégia, a magatartási normák és a vállalati értékek vonatkozásában, ezek a gyakorlatban annyira nem interpretálódnak a szektor munkavállalóinak a fejében. Ha esetleg a vezető számára világos is a vízió megvalósításához szükséges stratégia, arról általában nem beszél az őrző-védő tevékenységet, vagy vagyonvédelmi rendszert szerelő beosztottainak. Itt természetesen nem a vállalati titok kiszivárgásról van szó, hanem arról, hogy megosztja azokat az elképzeléseit a munkavállalókkal – azon kívül, hogy az adott feladatot el kell végezni – hogy azt közösen tudják megvalósítani. Ez a bizalmi hiány a szektor kezdete óta jelen van. Emiatt a vízió, vagyis a válasz arra, hogy hogyan és milyennek képzeljük el magunkat a jövőben sem születik meg. A magánbiztonsági szektor kisebb vállalkozásai rendszerint stratégiai tervvel nem rendelkeznek, így az abból levezethető biztonsági stratégiával sem. A nagyobb cégeknél a biztonsági stratégia nagyon gyakran a saját biztonsági portfóliójuknak a bővítésével, vagy valamelyik szolgáltatásuk fejlesztésével tekinthető azonosnak. A stratégia és így a biztonsági stratégia hiánya, vagy annak rosszul – inkább marketing fókuszú – értelmezése miatt a szektorban csak kis hányadban fordulnak elő a biztonsági stratégiából logikusan levezethető éves biztonsági tervek, illetve ezeken belül rövidebb időtartamú biztonsági akciók, illetve programok. Itt megint utalnék a korábban tett azon véleményemre, hogy a politikai töltetű filozófia miatt a magánbiztonsági szektor munkavállalóinak biztonságtudatosságát és biztonsági kultúráját hivatott biztonsági akciók és programok a felügyeleti szerveknek, esetleg a megbízó speciális elvárásainak való megfelelésben merülnek ki. Szabó [3 p. 178] a magánbiztonsági szakma felügyeletével kapcsolatban úgy fogalmaz, hogy a jogalkotó a magánbiztonsági szektor felügyeleti és hatósági ellenőrzési rendszerét, valamint a szakmai tevékenység korlátozásának vagy megszüntetésének a hatósági jogkörét a rendőrség hatáskörébe utalta", illetve javaslatot tett a szektor szakmai ellenőrzési modelljére, illetve belső ellenőrzési struktúrájára is. Véleményem szerint a törvényi előírásokon túlmutató ellenőrzések – ha azokat megfelelően felkészült szakemberek, tanácsadók, szakértők végzik – képesek lehetnek hozzájárulni a szektoron és munkavállalóinak biztonsági kultúrájának és biztonságtudatosságának a fejlesztéséhez. Azoknak a vállalatoknak, amelyek kritikus infrastruktúrát működtetnek a magánbiztonsági szektorhoz hasonlóan megannyi, a biztonsággal kapcsolatos törvénynek, rendeletnek, szabálynak kell megfelelniük [22], de a többségüknél (pl.: [19]) a magánbiztonsági szektor szereplőivel ellentétben – különösen, ha saját biztonsági osztályuk van – nagy hangsúlyt helyeznek arra, hogy a törvényi szabályozók mellett a biztonsági filozófiát megalkossák, abból 3-5 évre szóló biztonsági stratégiát fogalmazzanak meg, melyet az éves biztonsági tervben, illetve annak részeként a biztonsági akciótervekben és programokban realizálnak.

Azok a vállalatok, amelyeknél a szervezeti filozófiában a biztonság hangsúlyos szerepet kap, magától értetődik, hogy vezetői és munkavállalói elkötelezettek a biztonság irányába. A biztonságtudatossággal és biztonsági kultúrával kapcsolatos tréningeket, képzéseket és oktatásokat nem kötelezően letudható feladatként abszolválják, hanem a kreatív pedagógia eszköztárát is felhasználva arra törekszenek, hogy a biztonsággal kapcsolatos képességeket fejlesszék, majd ezek átültetésével a gyakorlatba az ismeretek készség szintű elsajátítása is megvalósuljon.

ÖSSZEFOGLALÁS

A cikk a magyarországi magánbiztonsági szektor szervezeti (biztonsági) kultúráját és a biztonságtudatosság fejlesztésének lehetőségeit vizsgálta, a szektor sajátosságait és ellentmondásait bemutatva.

A tanulmány a szervezeti kultúra–identitás–filozófia hármasából vezeti le a biztonsági kultúra tartalmát, Schein jéghegy-modelljére támaszkodva különíti el a látható (szabályzatok, eljárásrendek, képzések) és a mélyben húzódó (értékek, attitűdök, hiedelmek) elemeket. Részletesen tárgyalja Robbins kultúra-dimenzióit a magánbiztonsági szektorban (humánorientáció hiánya, gyenge teljesítményelismerés, rövid távú időhorizont, individualista attitűdök), valamint bemutatja, hogy a fejletlen biztonsági kultúra miként korlátozza a biztonságtudatos döntéshozatalt.

Rámutattam, hogy a politikai töltetű szervezeti filozófia, a megbízói érdekcsoportoknak való megfelelés elsődlegessége és a formális-mimetikus megfelelési kényszer (pl. ellenőrzésekre „felkészített" dokumentáció) akadályozza a valódi, értékalapú biztonsági kultúra kialakulását. Példákon keresztül mutattam be a munkavállalói biztonság háttérbe szorulását (védőfelszerelések, munkakörülmények, információbiztonsági gyakorlatok), és a kognitív biztonsági disszonancia jelenségét, amikor az egyéni és a szervezeti biztonsági normák élesen ütköznek.

A cikk ugyanakkor pozitív mintákat is felvillant: kritikus infrastruktúrát üzemeltető szervezetek és saját biztonsági osztállyal rendelkező vállalatok példáján keresztül bemutatja, hogyan építhető fel biztonsági filozófia, stratégia, majd éves és akciószintű biztonsági tervezés, amely valós tanulásvezérelt biztonsági környezetet eredményez. A tanulmány javaslatot tesz arra, hogy a magánbiztonsági szektorban a törvényi minimumon túlmutató, szakmailag megalapozott belső ellenőrzések, tudatosan felépített képzési programok és a vezetői példamutatás miként járulhatnak hozzá a biztonsági kultúra és a biztonságtudatosság érdemi fejlesztéséhez.

FELHASZNÁLT IRODALOM

[1 p. 30] FÁBIÁN P.: A magánbiztonsági szektor aktuális kihívásai a globális veszélyek relációjában. Budapest: Óbudai Egyetem, 2021.

[2 p. 166] CHRISTIÁN L. – ROTTLER V.: Magánbiztonsági helyzetértékelés 2019-2020. Glossa Iuridica VIII. évfolyam, 1-2. szám, 2021.

[3 p. 178] SZABÓ Cs.: A magánbiztonsági szektor szakmai felügyeletének és ellenőrzési modelljének vizsgálata a rendőrség hatósági ellenőrzésének vonatkozásában. Magyar Rendészet 2018/4. pp. 173-187.

[4] SZABÓ A.: Különböző rendeltetésű szervezetek objektumainak őrzésbiztonsági feladatait ellátó személy- és vagyonőrök gyakorlati képzési-fejlesztési lehetőségeinek vizsgálata és elemzése. (doktori disszertáció). Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2022.

[5] KOLLÁR Cs.: Tegyen ajánlást a GATE egységes arculatának megvalósítására. Gödöllő: Gödöllői Agrártudományi Egyetem Mezőgazdasági Gépészmérnöki Kar, 1999.

[6] KOLLÁR Cs.: PR és sajtókapcsolatok (2. kiadás). Budapest: PREMA Consulting, 2011.

[7] KOLLÁR Cs.: Arculattervezés (2. kiadás). Budapest: PREMA Consulting, 2011.

[8] KOLLÁR Cs.: Marketing kicsiknek és nagyoknak. Budapest: PREMA, Consulting, 2006.
[9] https://www.teaorszamok.hu (megtekintés: 2026.01.20.)
[10] SÁNDOR I.: Marketingkommunikáció. Budapest: Közgazdasági és Jogi Könyvkiadó, 1987.
[11] SZABÓ A.: Az élőerős objektumőrzés és a tekintélyelvű vezetési stílus kapcsolata. Hadmérnök XII. Évfolyam 3. szám – 2017. szeptember.
[12] PIRGER T.: A rendvédelmi szervek szervezetikultúra-vizsgálata. (doktori disszertáció). Sopron: Nyugat-magyarországi Egyetem, 2015.
[13] LACZÓ Gy.: A Zala megyei rendőr-főkapitányság szervezeti kultúrájának jellemzői, hatékonyabbá tétele. Diplomamunka. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2018.
[14] KOVÁCS G.: A rendészeti szervek szervezeti kultúrájának összetevői és sajátosságai, a téma feldolgozása a Rendőrtiszti Főiskola vezetéselméleti oktatásában. Pécsi Határőr Tudományos Közlemények, X. Kötet. Pécs: Magyar Hadtudományi Társaság Pécsi Szakosztály, 2009.
[15] KRIZBAI J.: A szervezeti kultúra fejlesztésének kérdései a honvédségben. HADTUDOMÁNY 2019/3.
[16] ELEKES E. A szervezeti kultúra és a szervezetfejlesztés kapcsolata. Magyar Rendészet 2014/4. pp. 25–40.
[17] HORVÁTH J.: Gondolatok a rendőrség szervezeti kultúrájáról. In: Quo vadis rendvédelem? A rendészet kultúrája – kulturált rendészet. Konferenciakiadvány. Pécsi Határőr Tudományos Közlemények. XI. kötet., 2010. pp. 21–31.
[18] SCHEIN, E. H. (1985).: The Corporate Culture Survival Guide. San Francisco: Jossey-Bass.
[19] FICHTINGER Gy.: A biztonsági kultúra felmérése és az eredmények hasznosítása nukleáris létesítményeknél. Budapest: Országos Atomenergia Hivatal, 2015.
[20] ROBBINS S. P. (1993): Organizational behavior. New Jersey: Prentice-Hall International, 816 p.
[21] JUHÁSZ M. – VASVÁRI F.: A biztonságtudatos vezetői attitűd vizsgálata. VEZETÉSTUDOMÁNY/BUDAPEST MANAGEMENT REVIEW LII. Évf. 2022. 1. szám.
[22] BOGNÁR B. – BONNYAI T. (szerk.): Kritikus infrastruktúrák védelme. Budapest: Dialog Campus Kiadó, 2019.

DOI: https://doi.org/10.12700/btsz.2026.8.1.79

ARTIFICIAL INTELLIGENCE CAPABILITY TESTING

MESTERSÉGES INTELLIGENCIA KÉPESSÉGVIZSGÁLATA

BURAI István György[1]

Abstract

The development of artificial intelligence (AI) is playing an increasingly important role in supporting engineering workflows, but its applicability in deterministic industrial environments remains questionable. This study examines the assistant capabilities of generative artificial intelligence in the field of CNC technology using a structured, task-oriented methodology. The research analyzes the applicability of AI in technical drawing, production planning, and CNC programming preparation through simple and complex tasks derived from real engineering workflows. Based on the results, AI provides effective support for low-risk, preparatory tasks, but consistency and accuracy decrease as complexity increases. The study confirms the role of artificial intelligence as an engineering assistant, while highlighting the limitations of its autonomous application.

Keywords

artificial intelligence, generative AI, engineering assistant, CNC technology, capability assessment, safety-critical systems

Absztrakt

A mesterséges intelligencia (MI) fejlődése egyre nagyobb szerepet kap a mérnöki munkafolyamatok támogatásában, ugyanakkor alkalmazhatósága a determinisztikus ipari környezetekben továbbra is kérdéses. Jelen tanulmány a generatív mesterséges intelligencia asszisztensi képességeit vizsgálja a CNC-technológia területén, strukturált, feladatvezérelt módszertan alkalmazásával. A kutatás valós mérnöki munkafolyamatokból származtatott egyszerű és összetett feladatokon keresztül elemzi az MI alkalmazhatóságát a műszaki rajzkészítés, a gyártástervezés és a CNC-programozás előkészítése során. Az eredmények alapján az MI hatékony támogatást nyújt alacsony kockázatú, előkészítő jellegű feladatok esetén, azonban a komplexitás növekedésével csökken a következetesség és a pontosság. A vizsgálat megerősíti a mesterséges intelligencia mérnöki asszisztensként betöltött szerepét, miközben rávilágít az autonóm alkalmazásának korlátaira.

Kulcsszavak

mesterséges intelligencia, generatív MI, mérnöki asszisztens, CNC-technológia, képességvizsgálat, biztonságkritikus rendszerek

[1] burai.istvan@bgk.uni-obuda.hu | ORCID: 0009-0007-8988-6301 | PhD Student, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | PhD Hallgató, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A mesterséges intelligencia (MI) az elmúlt években a műszaki és mérnöki területek egyik legdinamikusabban fejlődő technológiájává vált. A számítási kapacitás növekedése, a nagyméretű adathalmazok elérhetősége, valamint a fejlett tanulási algoritmusok megjelenése lehetővé tette olyan rendszerek kialakulását, amelyek képesek összetett mintázatok felismerésére, tartalom előállítására és döntéstámogatásra. Különösen a generatív mesterséges intelligenciák terjedése irányította rá a figyelmet arra, hogy ezek az eszközök nem csupán elemző vagy optimalizáló funkciókat láthatnak el, hanem aktív asszisztensként is megjelenhetnek a mérnöki munkafolyamatokban.

A gyártástechnológia területén a számítógépes vezérlésű (CNC) rendszerek kulcsszerepet játszanak. A CNC-technológia használata nagyfokú pontosságot, ismétlődő gyártási képességet és megbízható működést igényel, miközben a tervezési és programozási lépések összetett mérnöki döntések láncolatán alapulnak. A műszaki rajzok elkészítése, a gyártási folyamatok megtervezése és a G-kódok megírása előre meghatározott, szigorúan szabályozott környezetben történik, ahol a hibák nemcsak pénzügyi veszteségekhez vezethetnek, hanem akár gépek sérülését vagy a termelés biztonságának kockázatát is okozhatják. Emiatt a CNC-alapú rendszerek különösen érzékenyek az automatizált vagy részben automatizált döntéstámogató megoldások alkalmazására.

Az ipari digitalizációval párhuzamosan egyre több kutatás foglalkozik a mesterséges intelligencia gyártástechnológiai alkalmazhatóságával, ugyanakkor ezek jelentős része speciálisan fejlesztett, ipari célú MI megoldásokra koncentrál. Ezzel szemben viszonylag kevés empirikus vizsgálat értékeli objektív módon az általánosan elérhető, generatív mesterséges intelligenciák képességeit konkrét mérnöki feladatokon. Különösen hiányos azoknak a tanulmányoknak a száma, amelyek strukturált feladatrendszerben, mérhető kritériumok alapján elemzik az MI asszisztensi szerepét a CNC-technológia területén. Ez a kutatási rés indokolja az általános célú MI eszközök gyakorlati képességeinek részletesebb vizsgálatát.

Jelen tanulmány célja a generatív mesterséges intelligenciák asszisztensi képességeinek vizsgálata a CNC-technológia kontextusában. A kutatás egyszerű és összetett műszaki feladatokon keresztül elemzi, hogy az MI rendszerek milyen mértékben képesek támogatni a mérnöki munkát a műszaki rajzkészítés, a gyártástervezés és a G-kód generálás területén. A vizsgálat során nem az autonóm gyártásvezérlés megvalósíthatósága áll a középpontban, hanem az ember–MI együttműködés hatékonysága, valamint az alkalmazhatóság és a korlátok feltárása. A tanulmány hozzájárulása abban rejlik, hogy gyakorlati példákon és összehasonlítható értékelési szempontokon keresztül nyújt képet az MI jelenlegi állapotáról, mint mérnöki asszisztensről, és alapot teremt további kutatások számára az ipari és oktatási alkalmazások területén.

MESTERSÉGES INTELLIGENCIA MINT MÉRNÖKI ASSZISZTENS

A mesterséges intelligencia alkalmazása a mérnöki gyakorlatban hagyományosan jól körülhatárolt, specifikus feladatokra korlátozódott, mint például optimalizációs problémák megoldása, képfeldolgozás vagy prediktív karbantartás. Az utóbbi években azonban a generatív mesterséges intelligenciák megjelenése új szerepkört jelölt ki az MI számára,

amely túlmutat az automatizált számításokon, és az emberi mérnöki munkát támogató asszisztensi funkciók felé mozdult el [1], [2].

A mérnöki asszisztens fogalma ebben az összefüggésben nem autonóm döntéshozó rendszert jelent, hanem olyan intelligens eszközt, amely képes értelmezni a felhasználó által megadott problémát, releváns információkat összegyűjteni, alternatív megoldásokat javasolni, valamint a tervezési és dokumentációs folyamatokat gyorsítani. A beszélgetésalapú, nagy nyelvi modelleken (Large Language Model, LLM) alapuló rendszerek különösen alkalmasnak tűnnek erre a szerepre, mivel természetes nyelven képesek kommunikálni, összetett utasításokat feldolgozni, valamint strukturált szöveget és kódot generálni [3].

A generatív mesterséges intelligenciák működésének alapját statisztikai tanulási módszerek és nagyméretű neurális hálózatok adják, amelyek nem explicit szabályrendszerek alapján dolgoznak, hanem valószínűségi mintázatok felismerésével állítanak elő válaszokat [4]. Ennek következtében az ilyen rendszerek erőssége az információk gyors összegzése, a jól strukturált válaszok előállítása és az ismert minták mentén történő tartalomgenerálás. Ugyanakkor ez a működési elv magában hordozza a pontatlanság, a kontextus félreértelmezése és a determinisztikus rendszerekkel való ütközés kockázatát, ami a mérnöki alkalmazások esetében különös jelentőséggel bír [5].

A mérnöki asszisztensi szerep értelmezésekor fontos különbséget tenni a támogató és a helyettesítő funkciók között. Míg egyes ipari MI megoldások célja az emberi döntések kiváltása, addig az általános célú generatív MI eszközök jelenlegi fejlettségi szintjükön elsősorban a mérnöki munka kiegészítésére alkalmasak. Ezek a rendszerek hatékonyan segíthetik az információkeresést, a dokumentáció elkészítését, az alternatív megoldások felvázolását és az ismétlődő, alacsony hozzáadott értékű feladatok elvégzését, miközben a végső döntések és felelősség továbbra is az emberi szakértőt terhelik [6].

A CNC-technológia területén a mestersége intelligencia, mint mérnöki asszisztens alkalmazása különösen összetett kérdés. A CNC-programozás és gyártástervezés determinisztikus jellege, valamint a gépek működéséből fakadó szűk hibahatárok megkövetelik a nagyfokú pontosságot és következetességet. Ebben a környezetben az MI asszisztensi szerepe, elsősorban a tervezési folyamat támogatásában, a dokumentáció előkészítésében, valamint az emberi mérnök munkájának gyorsításában és ellenőrzésében értelmezhető [7]. Az MI által generált megoldások közvetlen, ellenőrzés nélküli alkalmazása ugyanakkor jelentős kockázatot hordoz, ami indokolttá teszi az ilyen rendszerek képességeinek és korlátainak módszeres vizsgálatát.

Összességében megállapítható, hogy a generatív mesterséges intelligencia jelenlegi állapotában elsősorban mérnöki asszisztensként értelmezhető, amely az emberi szakértelmet támogatja, de nem helyettesíti. Ennek a szerepnek a pontos meghatározása, valamint az alkalmazhatóság határainak feltárása elengedhetetlen ahhoz, hogy az MI-t biztonságosan és hatékonyan lehessen integrálni a CNC-technológiához kapcsolódó mérnöki munkafolyamatokba. A következő fejezet ennek megfelelően a CNC-technológia sajátosságait és az MI alkalmazásának konkrét kontextusát mutatja be.

A CNC-TECHNOLÓGIA ÉS AZ ASSZISZTENSI FELADATKÖR

A CNC-technológia sajátosságai alapvetően meghatározzák, hogy a mesterséges intelligencia milyen szerepkörben és milyen korlátok között alkalmazható mérnöki asszisztensként. A számítógépes számjegyvezérlésű megmunkálás olyan determinisztikus

rendszer, ahol a tervezési döntések, a technológiai paraméterek és a programozási utasítások közvetlen hatással vannak a gyártás minőségére, biztonságára és gazdaságosságára. Ennek következtében az MI alkalmazása ebben a környezetben nem általános automatizálási kérdésként, hanem szigorúan strukturált mérnöki problémaként értelmezendő.

A CNC-megmunkálás folyamata több egymásra épülő lépésből áll, amelyek mindegyike eltérő jellegű szakmai kompetenciákat igényel. A folyamat jellemzően a műszaki rajz elkészítésével kezdődik, amely a geometriai és méretbeli információk pontos rögzítését szolgálja. Ezt követi a gyártási terv megalkotása, amely meghatározza a megmunkálási sorrendet, a szerszámokat, a technológiai paramétereket és a befogási módokat. A folyamat záró lépése a CNC-program G-kód formájában történő elkészítése, amely közvetlenül vezérli a gép mozgását és működését [8], [9].

Ezek a lépések eltérő mértékben alkalmasak mesterséges intelligencia általi támogatásra. A műszaki rajzkészítés esetében az MI elsősorban a geometriai formák értelmezésében, egyszerű alkatrészek ábrázolásában és dokumentációs feladatokban jelenhet meg asszisztensként. A rajzok azonban szigorú szabványokhoz kötöttek, ezért az MI által generált ábrák csak korlátozottan alkalmazhatók közvetlenül, és minden esetben szakértői ellenőrzést igényelnek [10].

A gyártási terv készítése már összetettebb mérnöki döntéseket foglal magában. Itt az MI asszisztensi szerepe elsősorban a lehetséges technológiai lépések összegzésében, alternatív megoldások javaslatában és az információk rendszerezésében értelmezhető. A szerszámválasztás, a megmunkálási sorrend és a technológiai paraméterek meghatározása ugyanakkor erősen függ az adott géptől, anyagtól és gyártási környezettől, ami korlátozza az általános célú MI eszközök pontosságát és megbízhatóságát [11].

A CNC-programozás, különösen a G-kód generálása a folyamat legkritikusabb pontja. A G-kód szintaktikailag kötött, determinisztikus nyelv, ahol egyetlen hibás parancs is a megmunkálás sikertelenségéhez vezethet. Bár a generatív mesterséges intelligenciák képesek formailag helyes kódrészletek előállítására, ezek helyessége és alkalmazhatósága csak a konkrét gépvezérlés, a technológiai környezet és a biztonsági előírások ismeretében ítélhető meg. Ebben az értelemben az MI legfeljebb kiindulási alapot vagy ellenőrző eszközt jelenthet, de nem tekinthető önálló programozónak [12].

A CNC-technológiában értelmezett asszisztensi feladatkör tehát több szintre bontható. Az alacsonyabb kockázatú, dokumentációs és előkészítő feladatok esetében az MI hatékony támogatást nyújthat, míg a magas kockázatú, közvetlen gépvezérlést érintő döntések továbbra is emberi felügyeletet igényelnek. Ez a rétegzett megközelítés összhangban áll az ipari automatizálás jelenlegi gyakorlatával, ahol a mesterséges intelligencia fokozatosan, ellenőrzött módon kerül integrálásra a meglévő rendszerekbe [13].

A fejezetben bemutatott megfontolások alapján a következő lépés egy olyan strukturált feladatrendszer kialakítása, amely alkalmas a mesterséges intelligencia asszisztensi képességeinek objektív vizsgálatára a CNC-technológia kontextusában. Ennek keretében külön vizsgálhatók az egyszerű, jól körülhatárolható feladatok, valamint az összetettebb, több lépésből álló mérnöki problémák, amelyek reális képet adnak az MI jelenlegi alkalmazhatóságáról.

FELADATOK MEGHATÁROZÁSA A MESTERSÉGES INTELLIGENCIA ASSZISZTENS SZÁMÁRA

A mesterséges intelligencia mérnöki asszisztensként történő alkalmazhatóságának objektív vizsgálatához olyan feladatrendszer kialakítása szükséges, amely tükrözi a valós mérnöki gyakorlatot, ugyanakkor lehetőséget biztosít az egyes részfeladatok elkülönített értékelésére. A jelen kutatás során alkalmazott módszertan alapelve, hogy nem az egyes mesterséges intelligencia rendszerekhez kerülnek feladatok kiválasztásra, hanem fordítva: a tipikus CNC-technológiai feladatok határozzák meg, hogy milyen MI alapú megoldások alkalmazhatók azok támogatására.

A feladatrendszer kialakításakor elsődleges szempont volt a fokozatosság elve. Ennek megfelelően a vizsgálat egyszerű, jól körülhatárolható részfeladatokkal indul, majd fokozatosan halad az összetettebb, több lépésből álló mérnöki problémák felé. Ez a megközelítés lehetővé teszi annak elemzését, hogy a mesterséges intelligencia milyen mértékben képes kezelni az egyes feladattípusokat, valamint hol jelentkeznek a komplexitás növekedéséből fakadó korlátok.

Az egyszerű feladatok olyan alapvető mérnöki tevékenységeket reprezentálnak, amelyek a CNC-megmunkálás előkészítő szakaszában rendszeresen előfordulnak. Ide tartozik az egyszerű geometriai formák műszaki rajzának elkészítése, az alapvető méret- és jelölésrendszerek alkalmazása, valamint az ezekhez kapcsolódó dokumentáció előállítása. Ezek a feladatok viszonylag alacsony kockázatúak, ugyanakkor jól alkalmasak az MI értelmezési, struktúraalkotási és szabálykövetési képességeinek vizsgálatára.

A vizsgálat következő szintjén megjelennek a részben összetett feladatok, amelyek már több mérnöki szempont együttes kezelését igénylik. Ebbe a kategóriába tartozik például a menetes alkatrészek ábrázolása, a technológiai sorrend megtervezése, valamint a gyártási lépések logikai összekapcsolása. Ezek a feladatok nemcsak a geometriai pontosságot, hanem a műszaki konvenciók és szabványok helyes értelmezését is megkövetelik, így alkalmasak az MI kontextuskezelési és következtetési képességeinek elemzésére.

Az összetett feladatok a teljes CNC-előkészítési folyamatot modellezik, ahol a mesterséges intelligenciának egy kezdeti bemenet, például egy kézi skicc vagy részleges műszaki leírás, amely alapján kell több egymásra épülő lépést végrehajtania. Ezek a lépések magukban foglalják a műszaki rajz pontosítását, a gyártási terv kidolgozását, valamint a CNC-program logikai felépítésének előkészítését. Az ilyen feladatok különösen alkalmasak annak vizsgálatára, hogy az MI képes-e következetesen kezelni a több lépésből álló mérnöki problémákat, illetve mennyire tartható fenn a megoldások minősége a feladat komplexitásának növekedésével.

A feladatok értékelése során nem kizárólag a végeredmény helyessége került figyelembe vételre, hanem a megoldáshoz vezető folyamat is. Vizsgálatra került, hogy az mesterséges intelligencia modell milyen mértékben érti meg a feladat lényegét, mennyire következetesen alkalmazza a korábban megadott információkat, valamint hány iterációra van szükség a használható eredmény eléréséhez. Ez a megközelítés összhangban áll azzal a gyakorlati szemlélettel, amely szerint a mesterséges intelligencia asszisztensként való alkalmazhatóságát nem csupán az elméleti képességek, hanem a tényleges használhatóság és a felhasználói interakció hatékonysága határozza meg.

A fejezetben bemutatott feladatstruktúra alapot teremt a következő fejezetekben ismertetett képességvizsgálatokhoz. A módszertan lehetővé teszi az egyszerű és összetett

feladatok eredményeinek összehasonlítható értékelését, valamint hozzájárul annak megértéséhez, hogy a mesterséges intelligencia jelenlegi fejlettségi szintjén milyen szerepet tölthet be a CNC-technológiához kapcsolódó mérnöki munkafolyamatok támogatásában.

A KÉPESSÉGVIZSGÁLAT MÓDSZERTANA

A mesterséges intelligencia mérnöki asszisztensként való alkalmazhatóságának vizsgálata csak akkor tekinthető objektívnek, ha az egységes szempontrendszer alapján, reprodukálható módon történik. Ennek érdekében a jelen kutatás nem az egyes MI rendszerek összehasonlítására fókuszál, hanem arra, hogy az adott mérnöki feladatok milyen mértékben oldhatók meg mesterséges intelligencia támogatásával. A módszertan középpontjában ezért a feladatok jellege, az elvárt szakmai kimenetek, valamint az ezekhez rendelt értékelési kritériumok állnak.

A képességvizsgálat során a CNC-technológiához kapcsolódó tipikus mérnöki tevékenységek kerültek modellezésre. A feladatok kiválasztása a valós ipari és oktatási gyakorlatot tükrözi, és lefedi a tervezési folyamat főbb lépéseit a műszaki rajzkészítéstől a gyártástervezésen át a CNC-programozás előkészítéséig. A vizsgálat alapelve, hogy a mesterséges intelligencia asszisztensként történő alkalmazhatóságát nem kizárólag a végeredmény minősége, hanem a megoldáshoz vezető folyamat alapján kell megítélni.

Az értékelés három fő dimenzió mentén történt. Az első dimenzió a **feladatértelmezés helyessége**, amely azt vizsgálja, hogy az MI mennyire pontosan érti meg a műszaki problémát és a megadott feltételeket. A második dimenzió a **szakmai megfelelőség**, amely magában foglalja a műszaki szabványok, konvenciók és technológiai elvek helyes alkalmazását. A harmadik dimenzió a **használhatóság**, amely a gyakorlati alkalmazhatóságot, az iterációk számát és a szükséges emberi beavatkozás mértékét értékeli.

A módszertan strukturált bemutatását az 1. táblázat szemlélteti, amely a vizsgált feladatokat, az azokkal szemben támasztott elvárásokat, valamint az értékelési kritériumokat foglalja össze.

Feladattípus	Elvárt kimenet	Értékelési kritériumok
Egyszerű geometriai alkatrész műszaki rajza	Méretarányos, szabványos jelöléseket tartalmazó műszaki rajz	Feladatértelmezés pontossága; méret- és jelöléshelyesség; szabványkövetés
Menetes alkatrész ábrázolása	Helyes menetjelölés, letörések és arányok alkalmazása	Konvenciók helyes alkalmazása; geometriai következetesség; hibák javíthatósága
Gyártási terv készítése	Logikus megmunkálási sorrend, megfelelő szerszámválasztás	Technológiai logika; alternatívák kezelése; szakmai indokoltság
CNC-program logikai felépítése	Szintaktikailag helyes, értelmezhető G-kódstruktúra	Determinisztikusság; kockázatos elemek felismerése; ellenőrzési igény

Feladattípus	Elvárt kimenet	Értékelési kritériumok
Összetett, több lépésből álló feladat	Rajz–terv–program összhangja	Következetesség több lépésen át; információmegtartás; iterációk száma

1. Táblázat: Feladat–elvárás–értékelési kritérium hármas a képességvizsgálat során, saját szerkesztés

A táblázatban szereplő feladatok növekvő komplexitást képviselnek, ami lehetővé teszi annak vizsgálatát, hogy a mesterséges intelligencia asszisztensi teljesítménye miként változik a feladat összetettségének növekedésével. Az egyszerű feladatok elsősorban az MI értelmezési és struktúraalkotási képességeit tesztelik, míg az összetett feladatok a következetességet, a kontextuskezelést és a mérnöki logika hosszabb távú fenntartását vizsgálják.

A módszertan fontos eleme, hogy az értékelés nem bináris (helyes–helytelen) módon történik. Ehelyett a részleges megfelelés, a javíthatóság és az emberi beavatkozás szükségessége is értékelési szempontként jelenik meg. Ez a megközelítés összhangban van a mesterséges intelligencia asszisztensként történő alkalmazásának gyakorlati szemléletével, ahol a cél nem az emberi szakértelem kiváltása, hanem annak hatékony támogatása.

A fejezetben bemutatott módszertan biztosítja az alapot a következő fejezetekben részletezett képességvizsgálatok eredményeinek bemutatásához és értelmezéséhez. Az egységes értékelési keretrendszer lehetővé teszi az egyszerű és összetett tesztek összehasonlítását, valamint hozzájárul a mesterséges intelligencia jelenlegi alkalmazhatóságának objektív megítéléséhez a CNC-technológia területén.

EGYSZERŰ FELADATOK EREDMÉNYEINEK BEMUTATÁSA ÉS ÉRTÉKELÉSE

Az egyszerű feladatok célja az volt, hogy feltárják a mesterséges intelligencia alapvető asszisztensi képességeit olyan mérnöki problémák esetén, amelyek jól körülhatárolhatók, alacsony kockázatúak, és a CNC-technológia előkészítő szakaszában rendszeresen előfordulnak. Ezek a feladatok lehetőséget biztosítottak az MI értelmezési, struktúraalkotási és szabálykövetési képességeinek vizsgálatára anélkül, hogy a komplexitás elfedné az alapvető működési sajátosságokat.

Az értékelés minden esetben az „A képességvizsgálat módszertana” fejezetben bemutatott módszertani keretrendszer szerint történt, különös tekintettel a feladatértelmezés pontosságára, a szakmai megfelelőségre és a gyakorlati használhatóságra.

Műszaki rajzkészítési feladatok értékelése

Az egyszerű műszaki rajzkészítési feladatok során az MI modellnek alapvető geometriai elemeket tartalmazó alkatrészek rajzát kellett elkészítenie meghatározott méretek alapján. A feladat célja nem az esztétikai minőség, hanem a műszaki szabványoknak megfelelő ábrázolás vizsgálata volt.

A tapasztalatok alapján megállapítható, hogy az MI általában helyesen értelmezte a geometriai alapformákat és azok méretbeli viszonyait. Az alkatrészek arányai jellemzően megfelelőek voltak, és a rajzok tartalmazták a szükséges méretjelöléseket. Ugyanakkor több esetben megfigyelhető volt, hogy a vonalvastagságok, nézetválasztások és jelölési konvenciók nem feleltek meg teljes mértékben a műszaki rajzolás szabványainak.

Az értékelés során különösen fontos szempont volt az iterációk száma. A rajzok minősége jellemzően javult a pontosító utasítások hatására, ami arra utal, hogy az MI alkalmas lehet interaktív asszisztensi szerepre. Ugyanakkor az is megállapítható, hogy önállóan, első lépésben ritkán eredményezett teljes mértékben elfogadható műszaki rajzot. Ez megerősíti azt a következtetést, hogy a rajzkészítés területén az MI inkább támogató, semmint helyettesítő szerepet tölthet be.

Menetes alkatrészek ábrázolásának értékelése

A menetes alkatrészek ábrázolása már a rajzkészítésen belül is összetettebb feladatnak tekinthető, mivel speciális jelöléseket, szabványos ábrázolási módokat és geometriai részleteket igényel. A feladat célja annak vizsgálata volt, hogy az MI mennyire képes kezelni ezeket a konvenciókat, illetve mennyire következetes a korábban megadott geometriai információk alkalmazásában.

A vizsgálat során az MI általában felismerte a menet létezésének szükségességét, és alkalmazta az alapvető menetjelöléseket. Ugyanakkor gyakran előfordult, hogy a menet hossza, a letörések kialakítása vagy a jelölések pontos formája nem felelt meg maradéktalanul a szabványos elvárásoknak. Ezek a hibák különösen akkor jelentkeztek, amikor a feladat több paraméter együttes figyelembevételét igényelte. Pozitívumként értékelhető, hogy a hibák többsége pontosító utasításokkal korrigálható volt, ami ismételten az asszisztensi jelleg erősödését mutatja. Ugyanakkor az is egyértelművé vált, hogy a menetes elemek ábrázolása olyan szintű szabványismeretet és következetességet igényel, amelyet az MI jelenlegi formájában csak korlátozottan képes önállóan biztosítani.

Gyártási terv készítésének értékelése

A gyártási terv készítése az egyszerű feladatok közül a leginkább koncepcionális jellegű volt, mivel itt nem konkrét geometriai ábrázolásról, hanem a megmunkálási folyamat logikai felépítéséről van szó. A feladat során a mesterséges intelligenciának meg kellett határoznia a megmunkálási lépések sorrendjét, valamint javaslatot kellett tennie a szükséges műveletekre és eszközökre.

Az eredmények azt mutatták, hogy az MI ezen a területen viszonylag jól teljesített. A javasolt gyártási sorrendek többnyire logikusak voltak, és megfeleltek az általános technológiai elveknek. Az MI képes volt felismerni az alapvető megmunkálási műveleteket, valamint azokat egymáshoz megfelelő sorrendben kapcsolni.

Ugyanakkor a gyártási tervek gyakran maradtak általános szinten, és nem minden esetben vették figyelembe a konkrét géptípus, szerszámkészlet vagy anyag sajátosságait. Ez arra utal, hogy az MI erőssége ebben a feladatkörben elsősorban az információk strukturálásában és összefoglalásában rejlik, míg a részletek kidolgozása továbbra is emberi szakértelmet igényel.

Az egyszerű feladatok összegző értékelése

Az egyszerű feladatok eredményei alapján megállapítható, hogy a mesterséges intelligencia alkalmas alapvető mérnöki asszisztensi feladatok támogatására, különösen a dokumentációs és előkészítő tevékenységek területén. A feladatértelmezés általában megfelelő volt, és a hibák jelentős része iteratív módon javíthatónak bizonyult.

Ugyanakkor az is egyértelművé vált, hogy a pontosság és a szabványkövetés szintje önálló alkalmazás esetén nem minden esetben felel meg a CNC-technológia szigorú

követelményeinek. Ez megerősíti azt a következtetést, hogy az MI jelenlegi fejlettségi szintjén elsősorban támogató szerepkörben alkalmazható, ahol az emberi mérnök szakmai kontrollja elengedhetetlen.

ÖSSZETETT FELADATOK EREDMÉNYEINEK BEMUTATÁSA ÉS ÉRTÉKELÉSE

Az összetett feladatok célja annak vizsgálata volt, hogy a mesterséges intelligencia mennyire képes több egymásra épülő mérnöki lépést következetesen kezelni, valamint hogy a feladat komplexitásának növekedése milyen hatással van az asszisztensi teljesítményre. Ezek a feladatok már nem izolált részproblémákat reprezentáltak, hanem a CNC-technológia előkészítési folyamatának jelentős részét modellezték a kezdeti koncepciótól a gyártás előkészítéséig.

Az értékelés során kiemelt szempont volt az információmegtartás, a korábbi lépések következetes alkalmazása, valamint az iterációk során mutatott stabilitás. A fejezet alfejezetei külön tárgyalják az MI önálló problémamegoldási képességeit, valamint az emberi mérnöki megoldással való összevetést.

Összetett feladat megoldása kézi skiccből kiindulva

Az első összetett feladat során a mesterséges intelligencia egy kézi skiccből indult ki, amely a megmunkálandó alkatrész alapvető geometriai jellemzőit tartalmazta. A feladat célja az volt, hogy az MI a vizuális vagy szövegesen leírt bemenet alapján műszaki rajzot készítsen, majd erre építve gyártási tervet és a CNC-program logikai struktúráját határozza meg.

A tapasztalatok azt mutatták, hogy az MI kezdeti lépésként általában felismerte az alkatrész fő geometriai elemeit, és képes volt egy értelmezhető műszaki rajz vázlatos elkészítésére. Ugyanakkor már ebben a fázisban megjelentek pontatlanságok, különösen a méretarányok, a részletek pontos elhelyezése és a szabványos jelölések alkalmazása terén. Ezek a hibák a későbbi lépésekben tovább öröklődtek, ami jól szemlélteti az összetett feladatok egyik alapvető kockázatát: a korai fázisban elkövetett pontatlanságok kumulatív hatását.

A gyártási terv készítése során az MI jellemzően logikus, de általános jellegű megoldásokat adott. A megmunkálási sorrend többnyire megfelelt az általános technológiai elveknek, ugyanakkor a konkrét részletek, például a befogási stratégiák vagy a szerszámválasztás finomságai gyakran hiányoztak vagy csak részben voltak megalapozottak. Ez arra utal, hogy az MI képes a magas szintű folyamatlogika követésére, de a részletekben rejlő mérnöki döntések meghozatalában korlátozott.

Következetesség és kontextusmegtartás több lépésen keresztül

Az összetett feladatok egyik legfontosabb vizsgálati szempontja a kontextusmegtartás volt. Ez azt jelenti, hogy az MI mennyire képes a korábban megadott információkat, döntéseket és paramétereket a későbbi lépések során helyesen alkalmazni.

A vizsgálat során megfigyelhető volt, hogy az MI rövidebb interakciós láncok esetén viszonylag jól megőrizte a kontextust, azonban a lépések számának növekedésével egyre gyakrabban jelentkeztek inkonzisztenciák. Ezek például eltérő méretadatok

megjelenésében, korábban rögzített geometriai elemek figyelmen kívül hagyásában vagy a gyártási terv és a programlogika közötti eltérésekben nyilvánultak meg.

Ez a jelenség különösen kritikus a CNC-technológia szempontjából, mivel a gyártási folyamat minden lépése szorosan egymásra épül. A kontextusvesztés nemcsak pontatlanságot eredményezhet, hanem olyan logikai hibákat is, amelyek a gyártás során közvetlen kockázatot jelentenek. A tapasztalatok alapján az MI asszisztensként történő alkalmazása ebben a feladattípusban csak folyamatos emberi ellenőrzés mellett tekinthető biztonságosnak.

Összevetés az emberi mérnöki megoldással

Az összetett feladatok értékelésének fontos eleme volt az MI által adott megoldások összevetése egy emberi mérnök által készített referencia-megoldással. Az emberi megoldás jellemzően lassabban készült el, ugyanakkor nagyobb következetességet és pontosságot mutatott a teljes folyamat során.

Az emberi mérnöki megoldás egyik legnagyobb előnye a globális áttekintés képessége volt. A mérnök már a kezdeti lépések során figyelembe vette a későbbi gyártási szempontokat, így a műszaki rajz, a gyártási terv és a CNC-program egymással összhangban készült el. Ezzel szemben az MI megoldásai inkább lokális optimalizációt mutattak, azaz az adott lépést próbálták a lehető legjobban megoldani, gyakran a későbbi következmények figyelmen kívül hagyásával.

Ugyanakkor az MI jelentős előnyt mutatott az információk gyors összegzésében és a kezdeti koncepciók felvázolásában. Ez arra utal, hogy az MI hatékony eszköz lehet a mérnöki gondolkodás támogatásában, különösen a tervezési folyamat korai szakaszában, míg a végső döntések és a kritikus részletek kidolgozása továbbra is emberi kompetenciát igényel.

Az összetett feladatok tanulságai

Az összetett feladatok eredményei alapján egyértelművé vált, hogy a mesterséges intelligencia asszisztensi teljesítménye a feladat komplexitásának növekedésével jelentősen csökken. Míg az egyszerű feladatok esetében az MI hatékony támogatást nyújtott, addig az összetett, több lépésből álló problémák során a következetesség és a pontosság fenntartása már komoly kihívást jelentett.

Ezek az eredmények alátámasztják azt a megközelítést, miszerint az MI jelenlegi fejlettségi szintjén nem alkalmas autonóm mérnöki feladatellátásra a CNC-technológia területén. Ugyanakkor asszisztensként, megfelelően strukturált feladatkörnyezetben és emberi felügyelet mellett jelentős hozzáadott értéket képviselhet.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK ÉS JÖVŐBELI KUTATÁSI IRÁNYOK

A tanulmány célja a mesterséges intelligencia asszisztensi képességeinek vizsgálata volt a CNC-technológia kontextusában, strukturált feladatrendszer és egységes értékelési szempontok alkalmazásával. A kutatás nem egyes mesterséges intelligencia megoldások összehasonlítására fókuszált, hanem arra, hogy tipikus mérnöki feladatok milyen mértékben támogathatók MI alapú eszközökkel. Ez a megközelítés lehetővé tette az mesterséges intelligencia alkalmazhatóságának feladatvezérelt, objektív értékelését.

Az eredmények alapján megállapítható, hogy a mesterséges intelligencia jelenlegi fejlettségi szintjén elsősorban mérnöki asszisztensként értelmezhető, amely képes

támogatni a tervezési és előkészítési folyamatokat, de nem alkalmas autonóm mérnöki döntéshozatalra a CNC-technológia területén. Az egyszerű feladatok, mint például alapvető műszaki rajzkészítés vagy gyártási terv vázlatos kidolgozása esetében az MI hatékony segítséget nyújtott, míg az összetett, több lépésből álló problémák során a következetesség, a kontextusmegtartás és a pontosság jelentős korlátokat mutatott.

A vizsgálat egyik fontos tanulsága, hogy az MI teljesítménye erősen függ a feladat strukturáltságától és az emberi iránymutatás minőségétől. Az iteratív, párbeszédalapú használat során az MI képes volt javítani a megoldások minőségét, ami megerősíti asszisztensi szerepének létjogosultságát. Ugyanakkor a CNC-technológia determinisztikus jellege miatt az MI által generált eredmények minden esetben szakértői ellenőrzést igényelnek.

Oktatási implikációk

A kutatás eredményei jelentős következtetéseket hordoznak a műszaki és mérnökképzés számára. A mesterséges intelligencia asszisztensként történő alkalmazása lehetőséget teremt arra, hogy a hallgatók a hagyományos tanulási módszereket kiegészítve interaktív támogatást kapjanak a tervezési és gyártástechnológiai feladatok megoldása során. Az MI alkalmas lehet a fogalmi összefüggések magyarázatára, a megoldási lépések strukturálására, valamint alternatív megközelítések bemutatására.

Ugyanakkor az eredmények rámutatnak arra is, hogy az MI alkalmazása az oktatásban csak tudatos keretek között lehet hatékony. Amennyiben a hallgatók kritikátlanul fogadják el az MI által generált megoldásokat, fennáll a veszélye a felszínes tudásszerzésnek és a mérnöki gondolkodás háttérbe szorulásának. Ezért az MI oktatási integrációja során kiemelt hangsúlyt kell kapnia a validálás, az ellenőrzés és a hibák felismerésének tanításának.

A CNC-technológia oktatásában az MI különösen hasznos lehet az előkészítő fázisok támogatásában, például a műszaki rajzok értelmezésében vagy a gyártási folyamatok logikai felépítésének megértésében. Az MI alkalmazása így nem a hagyományos oktatási módszerek kiváltását, hanem azok kiegészítését szolgálhatja, elősegítve a hallgatók önálló gondolkodásának és szakmai reflexiójának fejlődését.

Ipari implikációk

Az ipari alkalmazások szempontjából a kutatás eredményei megerősítik azt az álláspontot, hogy a mesterséges intelligencia jelenleg nem tekinthető önálló mérnöki szereplőnek a CNC-technológia területén. Az MI közvetlen, ellenőrzés nélküli alkalmazása a gyártásban jelentős kockázatot hordoz, különösen a CNC-programozás és a gépvezérlés területén, ahol a legkisebb hiba is komoly következményekkel járhat.

Ugyanakkor az MI asszisztensként történő alkalmazása az iparban is jelentős potenciált rejt. A tervezési és előkészítési fázisban az MI hozzájárulhat a mérnöki munka hatékonyságának növeléséhez, az információk gyors rendszerezéséhez és az alternatív megoldások feltárásához. Ez különösen értékes lehet olyan környezetben, ahol a mérnöki erőforrások korlátozottak, vagy ahol a tudásmegosztás és a dokumentáció kulcsszerepet játszik.

Az ipari integráció során kulcsfontosságú a megfelelő munkafolyamatok kialakítása, amelyek egyértelműen meghatározzák az MI szerepét és felelősségi körét. Az MI által generált eredmények validálása, a döntési pontok egyértelmű kijelölése és az emberi felügyelet biztosítása elengedhetetlen feltétele annak, hogy az MI biztonságosan és hatékonyan illeszkedjen a CNC-alapú gyártási rendszerekhez.

FELHASZNÁLT IRODALOM[2]

[1] European Parliament, "What is artificial intelligence and how is it used?" European Parliament Topics, Brussels, Belgium, Sep. 4, 2020. [Online]. Available: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

[2] European Parliament and the Council of the European Union, *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Official Journal of the European Union, L 1689, Jul. 12, 2024. [Online]. Available: https://eur-lex.europa.eu

[3] A. Vaswani *et al.*, "Attention is all you need," in *Proc. 31st Int. Conf. Neural Information Processing Systems (NeurIPS)*, Long Beach, CA, USA, 2017, pp. 5998–6008.

[4] T. B. Brown *et al.*, "Language models are few-shot learners," in *Proc. 34th Int. Conf. Neural Information Processing Systems (NeurIPS)*, Vancouver, BC, Canada, 2020, pp. 1877–1901.

[5] R. Bommasani *et al.*, "On the opportunities and risks of foundation models," Stanford Center for Research on Foundation Models (CRFM), Stanford, CA, USA, Tech. Rep., 2021. [Online]. Available: https://crfm.stanford.edu

[6] European Parliamentary Research Service, *General-Purpose Artificial Intelligence*, EPRS Briefing, European Union, Brussels, Belgium, 2023.

[7] B. D. Á. Duska, *Mesterséges intelligencia asszisztensi feladatainak vizsgálata a CNC technológia területén*, BSc/MSc szakdolgozat, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, Hungary, 2025.

[8] P. Smid, *CNC Programming Handbook*, 3rd ed. New York, NY, USA: Industrial Press, 2008.

[9]] M. Mattson, *CNC Programming: Principles and Applications*. Clifton Park, NY, USA: Delmar Cengage Learning, 2002.

[10] International Organization for Standardization, *ISO 128-1:2003—Technical drawings—General principles of presentation—Part 1: Introduction and general requirements*. Geneva, Switzerland: ISO, 2003.

[11] International Organization for Standardization, *ISO 129-1:2018—Technical product documentation (TPD)—Indication of dimensions and tolerances—Part 1: General principles*. Geneva, Switzerland: ISO, 2018.

[12] International Organization for Standardization, *ISO 2768-1:1989—General tolerances—Part 1: Tolerances for linear and angular dimensions without individual tolerance indications*. Geneva, Switzerland: ISO, 1989.

[13] M. P. Groover, *Fundamentals of Modern Manufacturing: Materials, Processes, and Systems*, 7th ed. Hoboken, NJ, USA: Wiley, 2020.

[2] példák hivatkozásokra | REFERENCES examples of references

DOI: https://doi.org/10.12700/btsz.2026.8.1.91

MACHINE E-LEARNING IN ARTIFICIAL INTELLIGENCE – COMPARATIVE STUDY

GÉPI TANULÁS A MESTERSÉGES INTELLIGENCIÁBAN – ÖSSZEHASONLÍTÓ TANULMÁNY

OLÁH Róbert[1]

Abstract

The study provides an insight into the field of machine learning (ML) by reviewing the literature of the past decades, primarily in Hungarian, and providing a detailed comparison between different theoretical approaches and applications. Based on the review of the source works, the study demonstrates that machine learning is not just a technological tool, but a multidisciplinary phenomenon that fundamentally shapes scientific and social structures. The article pays special attention to the three main methodological directions of machine learning, their practical applications, and the ethical and social challenges. The authors describe in detail the architecture of neural networks, the learning model, pathfinding on graphs, and supervised learning, where the quality of annotation affects the accuracy of algorithms. The study compares the work of several Hungarian authors along the formal frameworks, the applied methods, and the theoretical differences, highlighting the common foci of the research.

Keywords

Machine learning, Supervised learning, Unsupervised learning, Reinforcement learning, Artificial neural networks, Deep learning

Absztrakt

Ez a tanulmány a gépi tanulás (ML) területére nyújt betekintést az elmúlt évtizedek elsősorban magyar nyelvű szakirodalmak feldolgozásával, részletes összehasonlítást nyújtva a különböző elméleti megközelítések és alkalmazások között. A forrásmunkák áttekintése alapján a tanulmány bemutatja, hogy a gépi tanulás nem csupán egy technológiai eszköz, hanem egy multidiszciplináris jelenség, amely alapvetően alakítja a tudományos és társadalmi struktúrákat. A cikk különös figyelmet fordít a gépi tanulás három fő módszertani irányára, azok gyakorlati alkalmazásaira, valamint az etikai és társadalmi kihívásokra. A szerzők részletesen ismertetik a neurális hálózatok architektúráját, a tanulási modellt, a gráfokon történő útkeresést és a felügyelt tanulást, ahol az annotáció minősége befolyásolja az algoritmusok pontosságát. A tanulmány több hazai szerző munkásságát veti össze a formai keretek, az alkalmazott módszerek és az elméleti különbségek mentén, rávilágítva a kutatások közös fókuszpontjaira.

Kulcsszavak

Gépi tanulás, Felügyelt tanulás, Felügyelet nélküli tanulás, Megerősítéses tanulás, Mesterséges neurális hálózatokat, Mélytanulás

[1] olah.robert.oe@gmail.com | ORCID: 0009-0007-9134-9521 | IT teacher, Educational Center of Érd | Informatikai oktató, Érdi Tankerületi Központ

GÉPI TANULÁS KATEGÓRIÁK

Gépi tanulás kategóriák

A vizsgált forrásdokumentumok alapján a gépi tanulás (ML) nem csupán egy technológiai eszköz, hanem a mesterséges intelligencia egyik legdinamikusabb ága, amely napjainkban számos tudományterületet formál át és nyer alkalmazást. A szakirodalmi kutatás alapján megállapítható, hogy a szerzők egységesek a gépi tanulás három fő kategóriába sorolásában:

- **Felügyelt tanulás (Supervised Learning):** Címkézett adatokból (példapárokból) tanul, célja a klasszifikáció (osztályzás) vagy regresszió. A szociológiában például gyűlöletbeszéd felismerésére, a marketingben lemorzsolódás előrejelzésére, a kiberbiztonságban pedig behatolás detektálásra használják.
- **Felügyelet nélküli tanulás (Unsupervised Learning):** Rejtett mintázatokat keres címkézetlen adatokban. Tipikus alkalmazása a marketingben a fogyasztói szegmentáció (klaszterezés), illetve a hálózati anomáliák felismerése.
- **Megerősítéses tanulás (Reinforcement Learning):** Egy ágens próbálkozások és jutalmak útján tanul. Ez a módszer kritikus az **önvezető járművek** trajektóriatervezésében és a komplex játékstratégiák kidolgozásában. [1] [4]

Ágazatspecifikus alkalmazások összehasonlítása

Tekintettel hogy több tanulmányt vizsgáltunk meg, az alábbi témaösszehasonlítás jött ki eredménynek. A források technikai szempontból hasonlóságot mutatnak de a célok és az alkalmazott modellek eltérők. Közlekedés és autonóm rendszereknél a fókusz a biztonságon és a valós idejű döntéshozatalon van. A mélytanulást (CNN) képfeldolgozásra, a megerősítéses tanulást, pedig a jármű irányítására használják. Itt a hiba emberi életekbe kerülhet, szemben a marketinggel.

- **Kiberbiztonság:** A fő feladat az **anomália-detektálás** és a behatolásmegelőzés. A források hangsúlyozzák, hogy a pontosság (accuracy) helyett a **felidézés (recall)** a döntő mutató, mivel egy támadás elvétsége súlyosabb következményekkel jár, mint egy téves riasztás. Itt megjelenik a kvantumszámítógépek jövőbeli szerepe is az észlelés gyorsításában.
- **Marketing és gazdaság:** A tradicionális ML-megoldások (pl. döntési fák) népszerűbbek az **interpretálhatóság** miatt. A cél a fogyasztói élmény fokozása és a profittermelés az adatok bányászata révén.
- **Szociológia és médiaelmélet:** Itt a gépi tanulás egyfajta **„technológiai protézis”**, amely tágítja szellemi kapacitásunkat. A szociológiai alkalmazások legnagyobb kihívása a **humán annotálás (címkézés) szubjektivitása**, mivel a komplex fogalmak (pl. depresszió keretezése) interpretációja még az embereknek is nehéz.

Elméleti és filozófia háttér

A gépi tanulás egyedülálló filozófiai párhuzamokat von, amelyet a források több irányból is kifejtenek. David M. Berry a gépi tanulás elméleti hátterét Baruch Spinoza filozófiájára alapozza. Spinoza két fogalmat alkalmaz a számítási folyamatok leírására:

- **Számító művelet (Natura naturans):** Az aktív tanulási komponens, amelyben a rendszer algoritmusa folyamatosan fejlődik és adaptálódik, hasonlóan a teremtő természethez, amely a világ változásait és fejlődését irányítja.

- **Kiszámított művelet (Natura naturata):** Az elvégzett számítások eredményeként létrejött, passzív állapotban lévő modell, amely végrehajtja a szükséges feladatokat, analógiát képezve a már kialakult természet rendjével. [1] [2][3][4][5][6][7][8]

A fentiekkel szemben Gyarmati Péter más megvilágításba helyezi az MI -t az úgynevezett antropomorf modellt helyezi az előtérbe, amely alapján kimondható, hogy az MI az emberi gondolkodás és döntéshozatal egy utánzása. De különbséget tesz az emberi agy, és a gépek közötti működésnek.

Gyarmati a következőképpen gondolkodik a meglátásom alapján, az emberi agy az összefüggéseket felismeri, új célokat tűz ki, amelyeket cselekvéssel megvalósíthat. Ha viszont a számítógép alapján vizsgálódunk, tudhatjuk, hogy a gép egy parancskövető, amit beprogramoznak egy szellemi alkotáson keresztül, egy szoftverben megvalósított funkcióba ágyazzák és kódolt instrukciók alapján feladatot hajtanak végre. Ezzel szemben az emberi agy a születéskor a kinti világból fogadja be az információkat, és idővel megtanulja az anyanyelvét is.

A források rávilágítanak, hogy míg technikai alapok hasonlóak, de az alkalmazott modellek eltérőek lehetnek. Ha közlekedés biztonságot vizsgáljuk itt ebben az esetben a forráscikkek szerint, a fókusz a biztonság és a valós idejű döntéshozatalban van, a mély tanulást a CNN képfeldolgozásra, a megerősítéses tanulást pedig az adott jármű irányítására használják. A kiberbiztonság esetében van közös pont a közlekedés biztonsággal mert itt is van döntéshozatal, de a fő feladat az anomália detektálás, és behatolásmegelőzésben van. A források hangsúlyozzák hogy a felidézés a döntő mutató. [7]

A források mélyebb elméleti kérdéseket is adnak a gépi tanuláshoz, David M. Berry Baruch Spinoza terminológiáját hívja segítségül: a **számító műveletet** (aktív tanulás) a *Natura naturans*-hoz, a **kiszámított műveletet** (passzív, generált adat) pedig a *Natura naturata*-hoz hasonlítja, Gyarmati Péter ezzel szemben az **antropomorf modellt** emeli ki, rámutatva, hogy az MI az emberi gondolkodást igyekszik utánozni, de a számítógép imperatív (parancskövető) működése alapvetően eltér, az emberi agy deklaratív természetétől. Tehát az emberi agy egy deklaratív, mert összefüggéseket tár fel a célok mellett, míg a számítógép imperatív mert parancskövető, és egy beprogramozott utasításkészletet hajt végre. Az alábbi táblázat jól összefoglalja a felügyelt, felügyelet nélküli és a megerősítéses tanulás jellemzőit. [7][9]

Szempont	Felügyelt tanulás	Felügyelet nélküli tanulás	Megerősítéses tanulás
Adatok jellege	Címkézett adatok (példahalmazok)	Címkézetlen adatok	Környezeti visszacsatolás (jutalom/büntetés)
Cél	Klasszifikáció (osztályozás) vagy regresszió	Mintázatok, klaszterek keresése	Optimális stratégia megtalálása próbálkozásokkal
Alkalmazási példa	Lemorzsolódás előrejelzés marketingben	Vásárlói szegmentáció, anomália detekció	Önvezető autó trajektória tervezése

1 táblázat: Tanulási jellemzők, saját szerkesztés.

KÖZÖS KIHÍVÁSOK, TORZÍTÁS ÉS ETIKA

A gépi tanulás alkalmazásával kapcsolatos kihívások fontos szerepet játszanak a mindennapi életben [1][2]. Az algoritmusok és azok adathalmazok torzítást eredményezhetnek mivel a gépi tanulás módszerei gyakran adhatnak más eredmény kimeneteket. [3][4]

Az MI torzításra tekintve az algoritmusok képesek lehetnek arra, hogy valamilyen szempont szerint kiválogassák egy adott állásra a kívánt személyeket, akik megfelelnek a feltételeknek, és azon belül is válogathatnak. Pl. Egy toborzó algoritmus program, amely akár az életkor alapján is válogathat, ami diszkriminációs jelenséget mutathat. Ez a probléma arra hívja fel a figyelmet, hogy az algoritmust finomítani kell, és optimálisan működést biztosítani az adathalmazon, de a fenti problémára tekintve a társadalmi minták érvényesülhetnek [3]. A másik példa az önvezető autók kérdése, az etikai dilemmák egy esetleges bekövetkezett baleset után komoly vitákat válthat ki pl. ki a felelős a balesetért, ki volt a hibás. A médiaelméleti megközelítés pedig arra mutat rá, hogy az algoritmusok nem csupán technikai entitások, hanem egyben ideológiai struktúrák is, amelyek a társadalom értékeit és előítéleteit tükrözik [6]. A gépi tanulás nemcsak egy technológiai eszköz, hanem az emberi tudás kiterjesztése, amelyet alkalmazhatnak a különböző tudományágban.

KIBERBIZTONSÁG

Közlekedés és autonóm rendszerek

A közlekedési rendszerekben a mesterséges intelligenciának a fő célja a biztonságos közlekedés növelése, kiemelve, az önvezető járművek úgynevezett autonóm rendszerek tervezése és fejlesztése során. A gépi tanulás kulcsszerepet játszik a járművek trajektóriájának optimalizálásában. Az autó a tesztpályán a tanulás során képes lehet figyelembe venni a forgalmi adatokat, a környezeti tényezőket, a jármű irányításának hatékonysága céljából, de a közlekedési jelzések, és jelek felismerése kihívást jelenthetnek.

A kiberbiztonság pl. egy informatikai rendszer behatolásában szintén a gépi tanulás kerül az előtérbe az anomáliák felismerése szempontjából. A szignatúra alapú detektálás, jól működhet az ismert támadások ellen. Azonban a forrásművek alapján elmondható, hogy a gépi tanulás a mélytanulás alkalmazása erősen ágazatfüggő, és az élet minden területén eltérőek lehetnek a célok, módszerek és a megoldandó problémák. A közlekedésben és az autonóm rendszerekben az MI elsődleges feladata a biztonság növelése, ahol a képfeldolgozás, mint képi információk elemzése, valamit a megerősítéses tanulás és az MI döntése áll a fókuszban. A kiberbiztonság területén a gépi tanulás az anomáliák felismerésében nélkülözhetetlen szerepe van, az észlelési folyamatok mellett. A közeljövőben a kvantumszámítógépek segítségével gyorsítani lehet az észlelési folyamatokon, de nem utolsó sorban a párhuzamos programozás módszerének alkalmazása is segíthet a folyamatok gyorsabb feldolgozására. Ha a marketingkutatásra gondolunk az MI -t a gazdasági elemzésekben kérhetjük és alkalmazhatjuk, amely által jobban megérthetjük az üzleti folyamatokat, és annak a döntéseit. Itt előnyös, ha alkalmazzuk a döntési fákat, amelyek alkalmasak az előrejelzésekre is. A mesterséges neuronhálók és a mély tanulás egy adott struktúrára épül fel, és az úgynevezett backpropagation algoritmussal tanul. A több réteggel rendelkező mély hálózatok hatékonyak a beszéd, nyelv, és a képfeldolgozásban az RNN és LSTM modellek használata során. Összességében a gépi tanulás egy sokoldalú eszköztár, amelynek az alkalmazhatósága, az adatok és a alkalmazása területen való illeszkedést jelenti. Én úgy gondolom,

hogy a jövő kulcsa az MI modellek készítésében, és a hozzá való adathalmaz alkalmazásában van. Az alábbi mélyebb összehasonlítás öt fő dimenzió mentén mutatja be a források közötti összefüggéseket és eltéréseket.

Az elemzett források alapján a gépi tanulás nemcsak egy technikai módszertan, hanem filozófiai módszertan szempontból is vizsgálandó. Eltérően értelmezik az MI természetét míg David M. Berry Spinozára építve a gépi tanulást generatív, önmagát újratermelő folyamatként írja le, addig Gyarmati Péter hangsúlyozza, hogy az MI alapvetően imperatív, parancskövető rendszer, amely nem képes önálló célalkotásra, bár én ezt vitatom hiszem az MI öntanulásra is képes lehet. A médiaelméleti irányzat e kettő között helyezkedik el, az MI-t az emberi gondolkodást kiterjesztő technológiai protézisként értelmezve. Ha a módszerek alapján vizsgálódunk a forrásanyagok elismerik a felügyelt és felügyelet nélküli, valamint a megerősítéses tanulás szerepét, de az egyes ágazatok eltérő modellek és algoritmusokkal és eltérő adathalmazokkal dolgozhat. A közlekedésben a megerősítéses tanulás dominál, az autonóm döntéshozatala miatt, azonban a kiberbiztonságban pl. számítógépes hálózatban a hibrid és anomáliaalapú megoldások lehetnek a hatékonyak, A mérnöki tudományágban a fuzzy logika ad kapcsolódási pontot, az emberi érzékelés és a matematika között. Az adatok minősége minden területen kiemelt fontosságú. A műszaki és informatikai tudományágban többnyire mérhető adatokra támaszkodik. Az MI esetében a torzított adatok torz döntések eredménye lesz, a felelősség az emberé. A szerzők az alábbiak alapján gondolkodtak az elemzett forrásmunkájuk alapján. [2] [3][4]

- Az Mi természete gondolkodik-e a gép?

A gépi tanulás kvázi „teremtő” folyamat, amely belső mintázatokat épít fel, ezért nem pusztán mechanikus. Az MI nem gondolkodik, csak végrehajt. Az antropomorf értelmezés félrevezető, mert elfedi az emberi felelősséget.

- **Ellentét lényege:** generatív autonómia vs. eszközjelleg.

A „fekete doboz” elfogadható ár a magas prediktív teljesítményért (pl. autonóm közlekedés)

- **Társadalomtudományi források:**
  Az értelmezhetőség fontosabb, mint a maximális pontosság.
  Ellentét: hatékonyság ↔ magyarázhatóság.

Hatékonyság szerinti összevetés ((kontextusfüggően)

- **Leghatékonyabb megközelítések:**
  anomália-detektálás + autoencoder
  → ritka, de veszélyes események felismerésében kiemelkedő.
  megerősítéses tanulás
  → dinamikus, valós idejű döntésekhez ideális.
- **Közepesen hatékony, de stabil megoldások:**
  - **Marketing:** döntési fák, logisztikus regresszió
    → jó kompromisszum predikció és értelmezhetőség között.
  - **Mérnöki alkalmazások:** fuzzy logika
    → robusztus, de korlátozott adaptivitás

- A források közötti viták arra mutatnak rá hogy a gépi tanulás nem univerzálisan jó vagy rossz. A hatékonyság mindig attól függ hogy
- Milyen a vizsgált probléma mire keressük a megoldást
- Milyen MI modellt alkalmazunk vagy milyen saját modellt fejlesztünk
- Milyen adathalmazt adunk meg a modellnek
- És milyen következtetést vonunk le a modell tanításából.

FŐBB ELLENÉRVEK ÉS SZEMLÉLETBELI ÜTKÖZÉSEK

Míg a mérnöki és informatikai források alapján (Horváth Gábor, Husi Géza),a neurális hálózatokat az emberi és biológiai modellként kezelik, amely az idegsejt működését utánozza, addig Gyarmati éles kritikát fogalmaz meg ezzel szemben, ő azt mondja hogy a számítógép működése imperatív azaz parancskövető míg az emberi gondolkodás deklaratív ami azt jelenti hogy az összefüggéseket tárja fel, Gyarmati úgy véli hogy a gép üres agyal nem képes önálló célok megvalósítására, csak szoftveres tudás és ismeret feltöltéssel, így az MI soha nem lesz egyenrangú a humán intelligenciával. A marketingforrásra tekintve Pál és Iványi hangsúlyozzák hogy az üzleti döntéseknél a tradicionális döntési fák hatékonyabb lehet, mert az eredmények jól magyarázhatóak, de ezzel szemben a kiberbiztonság esetében a mély tanulás (Deep Learning) részesítik előnyben mert bonyolult mintázatokat is képes felismerni. A műszaki cikkek az adatokat egzakt mérési eredményeknek tekintik.

Németh András szerint a felügyelt tanulás alapját adó címkézésben nincs igazság, azaz ez szubjektív és interszubjektív, az algoritmus pedig átveszi az annotátorok előítéleteit. Az annotálás itt azt jelenti hogy a tanulóhalmaz létrehozása a kódolok munkáját igényli, ami egy szubjektív és interszubjektiv folyamat.[6]

HATÉKONYSÁG

A források összehasonlítása alapján megállapítható, hogy a hatékonyság attól függ, hogy milyen feladatra, és milyen területen alkalmazzuk az MI-t. Minden területen más és más algoritmus bizonyulhat hatékonynak.[1] Nem létezik univerzális módszer, de egyes problématípusra beazonosítható a gyakorlat alapján a megfelelő algoritmus alkalmazása, a gépi modellben. Ha egy önjáró autó programjának a fejlesztését végezzük akkor az útkeresés és optimalizálás feladatokban az A* kereső algoritmus adhat hatékonyabb működést a mohó algoritmussal szemben , mert nem csak a becsült távolságot vizsgálja hanem az útvonalköltségeket is, ami az optimális megoldást adhatja, és meghatározza a legrövidebb utat is hatékonyabban, elhárítja hogy az algoritmus végtelen utakon fusson.[5][6] A játékprogramok esetében a DeepMind AlphaGo Zero amely a megerősítéses tanulás hatékonyságát adja, mert ez az algoritmus bizonyítja hogy komplex döntésekben is képes az optimális stratégiák kiváltására. [10][11] A beszédfelismerésben az LSTM hálózatok bizonyultak a leghatékonyabbnak, mert képes az összefüggések megőrzésére, amely fontos szempont a beszéd értelmezésében, amely a szavakban és mondatokban rejlik a jelentés. Összességében a források azt támasztják alá, hogy a hatékonyság nem kategóriának tekinthető, hanem az adott problémát vizsgálva alkalmazzuk a megfelelő algoritmust, amelyik jól teljesít a megoldásban. A szignatúra alapú detektálás ez a legkevésbé hatékony a támadások ellen, mivel csak a már ismert mintákat ismeri fel. A torzított tanulóhalmaz esetében a források egyet-

értenek, hogy bármilyen ML modell hatástalan lehet, ha az adathalmaz torzítottak. A források több konkrét modellt is kiemelnek, amely kiemelkedő hatékonyságot mutatnak. Ilyen például a V3 hibrid modell, amely Brunner Csaba kutatása alapján. Ez a modell a leghatékonyabb a ritka és komplex támadások detektálásában, míg a többi modell elvétheti az alul prezentált osztályokat, a V3 mas modell kb 65,68% os felidézési arányt tudhat magának (recall arány) ért el, ami messze meghaladja a hatékonyság százalékát a hagyományos más modellekkel szemben. De van egy másik modell, a **(CVAE-DNN**) a szakirodalmi összehasonlítások alapján ez a modell (javított kondicionális variációs autóencoder és mély neurális hálózat kombinációja) kimagasló, **85,97%-os pontosságot (accuracy)** és **62,66%-os felidézést** mutatott az NSL-KDD adathalmazon.

Az RNN (Rekurrens Neurális hálózat a mélytanulási modellek közül az egyik leghatékonyabbnak mondható a források alapján, mert a hálózati forgalmat időbeli mintázatának felismerésére képes. A leghatékonyabb modellek (mint a fent említett V3) képesek a többségi osztályokon elért teljesítményt feláldozni azért, hogy a veszélyes támadásokat nagyobb arányban ismerjék fel, azonban van lehetőség a szintetikus mintavételre (SMOTE) és mesterséges minták generálásával segíteni az algoritmust (SVM SOTE) a támadások felismerésében. A detektálási pontosságot pedig a TPE (Tree-structured Parzen estimators) algoritmussal jelentősen lehet javítani a detektálási pontosságot. A hálózati anomáliák észlelését, a kvantumszámítógépek megjelenésével gyorsíthatóak. [3]

Az észlelési képesség javítható a hálózatban, ha a hibrid modellt alkalmazzuk, ami szignatúra alapú (ismert mintákat kereső), és az anomális alapú (nem szokványos viselkedés a hálózati forgalomban) detektálásnak kombinációjának alkalmazzuk. Ez különösen jól alkalmazható a mély autóencoder hálózatoknál, ahol a normál forgalom tanulása mellett képesek felismerni az eltérő anomáliákat is. A modellek mellett többféle mérőszámot alkalmazhatnak, amely az adott modell teljesítményét adja vissza, amelyet matematikai és statisztikai mutatószámokkal támasztanak alá. Az alábbi táblázatban összefoglaltam a teljesítmény mutatókat.

A felidézés, detektálási ráta az egyik legfontosabb mutató a hálózati behatolás esetében, ez a támadások arányát méri az összes támadáshoz képest. Ezt azért veszik prioritásként mert egy valódi támadás súlyosabb következménnyel jár, mint egy téves riasztás. A jól osztályozott esetek aránya az összes esethez képest a pontosságot mutatja. A konfúziós mátrix pedig abban adhat segítséget, hogy ezt szemlélteti, a (TO) valódi pozitív, (TB) valódi negatív, téves pozitív (FP), téves negatív (FN) döntéseknek a számát, így a modellt részlelesebb elemzés alá tudjuk vonni. A hálózati támadást kategóriaként is mérhetik mivel egyes modellek jobban teljesíthetnek a támadás felismerése során. Téves riasztás esetében. [8]

Teljesítmény mutatók

A teljesítményi mutatók kiemelten fontosak egy kiberbiztonsági rendszer esetében. A recall itt azt méri, hogy milyen arányban méri fel a támadásokat. Az adott rendszer biztonsága esetén ez az egyik kiemelt mutatószám, mivel egy támadás védelem igen komoly következménnyel járhat, ami a teljes rendszer leállását is okozhatja az adatvesztés mellett. Az Accuracy (pontosság) azaz itt az összes esetet vizsgáljuk és ahoz mérten lesz a helyes aránymutató. Azonban vigyázzunk mert normál hálózati forgalom nagyobb arányban lehet egy támadást tekintve és más eredményt kaphatunk a környezetben. A konfúziós mátrix a modellben az algoritmus lépéseit bontjuk le döntéseit bontja le kimenetekre, ami lehet

valódi pozitív (TP), valódi negatív (TN), hamis pozitív (FP) és hamis negatív (FN) esetek. Ezek segíthetnek a biztonsági kockázat elemzésében, érdemes az kimenetek értelmezhetőségét segíteni recall vagy precision alkalmazásával kombinálni. [2] [8]

Tesztelési módszertan

Mutató	Mit mér?	Miért fontos a biztonságban	Kockázatok
Recall (Felidézés)	A helyesen felismert támadások aránya az összes tényleges támadáshoz képest	Kritikus, mert egy elmulasztott támadás (FN) súlyos következményekkel járhat	Magas recall gyakran több téves riasztással jár
Accuracy (Pontosság)	Helyes besorolások aránya az összes esethez képest	Általános összehasonlításra használható	Kiegyensúlyozatlan adatoknál félrevezető
Konfúziós mátrix	TP, TN, FP, FN értékek megoszlása	Részletes képet ad a modell hibáiról	Önállóan nehéz értelmezni aggregált mutatók nélkül

2. táblázat: Teljesítmény mutatók (saját szerkesztés).

Konfúziós mátrix

A modellek hatékonysága a konfúziós mátrix segítségével jellemezhető. Mérni úgy tudunk a konfúziós mátrixal hogy lebontjuk a fentiekben leírtak alapján, azaz valódi pozitív (TP), valódi negatív (TN), Hamis pozitív (FP), Valódi negatív (FN). A valódi pozitív (TP) a modell helyesen felismerte a vizsgált eseményt. A valódi negatív esetében a modell helyesen beazonosította a negatív esetet. A hamis pozitív azt jelenti, hogy téves riasztás történt, a modell olyan esetben jelzet téves riasztást amikor normál működés volt. A hamis negatív azt jelenti, hogy a modell a valós eseményt nem vette figyelembe, amit tévesen normál működését osztályozta. A konfúziós mátrix eredményekből statisztikai mutatói kiértékelések hozhatok létre, amelyből a modell jósága meghatározható a kívánt alkalmazási területtől függően.

Tesztelési módszertan

Az adatkezelési módszerek befolyásolják a mért teljesítményi értékeket. Itt van két adat az egyik a tesztadat, a másik a tanító adathalmaz. A tanító adatokon dolgozik a modell, a teszt adatokon pedig az értékelések kimenete várható. Ez segíthet azon, hogy a modell csak az adatokon tanuljon és az ismeretlen adatokon. A KDD Cup 1999 vagy az NSL-KDD alkalmazása lehetővé teszi az eredmények hasonlóságának vizsgálatát más kutatási eredményekkel, így a hatékonyságokból levonhatóak könnyebben a következtetések. Az információszivárgást azt kerüljük el, mert vannak előfeldolgozási lépések, ami a tanító adathalmaz statisztikai adatokra kell épülniük, ellenkező esetben más eredményt kaphatunk. A osztályszintű vizsgálat során a támadástípusokat ajánlatos külön megvizsgálni, mert az összetettségben a mutatókban rejtett maradhat a támadások felismerése ami igen fontos biztonsági kockázatot is jelenthet. Az alábbi 3. táblázat bemutatja a szempontok alapján a tesztelési módszertani jellemzőket az adathalmazon. [2]

Szempont	Leírás	Jelentőség
Tanító–teszt szétválasztás	A modell csak tanító adatokon tanul	Megakadályozza a túllillesztést
Standard adatkészletek	KDD Cup 1999, NSL-KDD	Összehasonlíthatóság a kutatások között
Információszivárgás elkerülése	Normalizálás, skálázás csak tanító adatok alapján	Reális teljesítménymérés
Osztályszintű értékelés	DoS, Probe, R2L, U2R kategóriák külön vizsgálata	Ritka, de kritikus támadások felismerése

3. táblázat: Tesztelési módszertan és adathalmazok, saját szerkesztés.

Kutatásom alapján a következő eredményekre jutottam a hagyományos és a hibrid modellek szempontjából.

Hibrid modellek	
Modell	Pontosság
V1(Stacking Neurális hálózat	78,11 % pontosság és 55,84% felidézés(recall) ért el
V2 (Stacking NN + SMOTE Tomek	78,34%-os pontossággal és 59,29%-os felidézéssel zárt
V3 (Autoencoder + Stacking NN)	A pontossága alacsonyabb (74,26%), a kiberbiztonságban kritikus felidézési aránya (recall) kimagasló, 65,82% volt, különösen a ritka támadások (U2R) észlelésében

4. táblázat: Hibrid modellek összehasonlító mérések, saját szerkesztés.

Hagyományos modellek	
Modell	*Pontosság*
KNN (K-legközelebbi szomszéd	*76,51% pontosság, 48,3% felidézés*
RF (Random Forest)	*76,49% pontosság, 48,84% felidézés*
DNN (Mély Neurális Hálózat)	*80,22% pontosság, 52,77% felidézés*
SVM (Support Vector Machine)	*72,28% pontosság, 45,88% felidézés*

5 táblázat: Hagyományos modellek összehasonlító mérések, saját szerkesztés.

Az eredmények összevetésekkor a források hangsúlyozzák, hogy a recall(felidézés) mutató a legfontosabb, mert a ritka és veszélyes támadásokat felismerése kritikusabb a rendszere biztonsága szempontjából. A standarnizált adathalmazok használata szükséges mert az ad valós képet és eredményt a modellek teljesítményéről.

Gyakorlati szempontok és korlátok

A rendszerbe való behatolás esetén több tényezőt kell figyelembe venni, tekintettel az alábbiakban összefoglalt tényezők táblázatára, amelyben láthatjuk, az előnyök és hátrányokat. Az anomália alapú detektálás képes felismerni a null napi támadásokat, ami ismeretlen és a rendszer viselkedését figyelemmel kíséri ez a detektálás, azonban a nem szokványos viselkedést támadásnak veheti és így azonosíthatja be. A szignatúra alapú módszerek esetében az előre definiált támadási mintára épül, de az ismeretlen támadásokkal szemben

gyenge teljesítményű eredményt hozhatnak, azonban, ha ismert a támadási jellemzők akkor stabil működést eredményezhet. A tanítási és futási idő igen fontos tényező lehet egy rendszerben. Azok a modellek, amelyek nagyobb komplexitásúak számottevő a számítási és erőforrásigényük, ami korlátozottságot jelenthet, de a tanítási időt is tekintve a gyors reagálás fontos. A humán autentikáció során lehetőségünk van arra, hogy a modellbe beépítsük a szakértői tudást, ami által lehetőségünk van a modell pontosságának a működésére.

Tényező	Előny	Hátrány
Anomália-alapú detektálás	Új (null-napi) t támadások felismerése	Magas téves riasztási ráta
Szignatúra-alapú módszerek	alacsony FP arány	Ismeretlen támadásokkal szemben gyenge
Tanítási / futási idő	Gyors reagálás kritikus rendszereknél	Komplex modellek erőforrás-igényesek
Humán annotáció	Szakértői tudás beépítése	Szubjektivitás, címkézési hibák

6. táblázat: Gyakorlati szempontok és korlátok, saját szerkesztés.

Algoritmusok hatékonysága

A kiberbiztonságban számtalan algoritmus létezhet, amelyet az alábbi táblázat példaképpen mutat. Az egyes alkalmazási területek eltérő probléma szerkezetek és hatékonysággal rendelkezhetnek, így nem igazán létezik univerzális algoritmus, meg kell nézni milyen területre szeretnénk az alkalmazást. A megfelelő módszer kiválasztása mindig az adott feladat céljától, a rendelkezésre álló adathalmaztól és az elvárt teljesítménytől függ.

Terület	Preferált algoritmus	Miért ez a leghatékonyabb?
Kiberbiztonság	V3 Hibrid (AE+Stacking)	Jobban felismeri a ritka, kritikus támadásokat (Recall).
Közlekedés	DDPG (Reinforcement)	Emberi tudás nélkül is optimális trajektóriát tervez.
Keresés	(A-csillag)*	Optimális és teljes; figyelembe veszi a megtett költséget
Marketing	Tradicionális ML	Az üzleti döntésekhez szükséges interpretálhatóságot nyújtja
Mérnöki munka	Fuzzy logika	Képes kezelni a pontatlan, emberi jellegű bemeneteket.

7. táblázat: Algoritmusok hatékonysága, saját szerkesztés.

A kiberbiztonság területén a V3 hibrid modell alkalmazása indokolt lehet, mert hatékonyan ismerheti fel a ritka és kritikus támadásokat,A magas recall érték fontos lehet, mert egy elmulasztott incidens, nagyobb károkat okozhat. A közlekedési rendszerben első körben az önjáró autóra gondolhatunk, itt a DDPG típusú megerősítéses tanulási algoritmus előnye, hogy az emberi szabályrendszer nélkül is képes optimális döntéseket hozni. A keresési problémákra tekintve az (A-csillag)* látszik a leghatékonyabbnak mert az adott feladatra *o*ptimális megoldást ad, és az útvonal költségeket is figyelembe veszi, amely egy gráfos feladat esetén igen jó választásnak mondható keresés esetén. Az üzleti világban az elemzésre tekintve a hagyományos gépi tanulási módszerek kerülnek előtérbe, a jó teljesít-

ményt adva, és meg tudjuk érteni miért hozott a modell döntést az adott szituációra az algoritmus alapján. A mérnöki megközelítés szempontjából ott a fuzzy logika segítségével menedzselni tudjuk a pontatlan jellegű inputot, ahol matematikai értelemben a modellezés nehézségbe ütközhet. Ilyenkor a MATLAB programot hívhatjuk segítségül megalkotva a fuzzy szabályokat is. [4][2]

A feltöltött források összességében egyetértenek abban, hogy a mély tanulás jelenleg a legerősebb eszköz a mintafelismerés során, pl. a képi orvosi diagnosztika, mint a röntgen ahol a CT felvételek automatikus kiértékelése, nagy mennyiségű strukturálatlan adat feldolgozását igényli. A konvolúciós neurális hálózatok (CNN)képesek a formák, és összetett mintázatok felismerésére Ezek a hálózatok képesek egy CT felvételen pl daganatra utaló jelek detektálására. Ez egy felügyelt tanulási folyamat, hiszen a szakértők által címkézett adatokon tanulják meg az egészséges és kóros állapotokat. A tanulási folyamat elsődleges célja hogy a téves diagnózisok csökkentése. A mély felügyelt tanulási modellek hatékonyan támogatják az anomália és mintafelismerést, riasztást adva minden a normálistól eltérő struktúrát, rendszerviselkedésre.

Brunner Csaba munkái rámutatnak a **hibrid megoldások** jelentőségére, amelyek a mély tanulást más módszerekkel kombinálva növelik a megbízhatóságot és csökkentik a kritikus hibák esélyét. Ezzel párhuzamosan Gyarmati Péter és Németh megközelítései hangsúlyozzák a **filozófiai és etikai kontroll szükségességét**, különösen olyan területeken, ahol az algoritmikus döntések közvetlen hatással vannak emberi életekre.

Összességében a CNN alapú mély tanulás a leghatékonyabb eszköz az orvosi képfeldolgozásban. A gépi tanulás jövője úgy gondolom, hogy nem az orvos helyettesítésében, hanem az orvosi döntéshozatal felelős támogatásában rejlik. A fekete doboz jellegű mélytanulás az egyik legmeghatározóbb jelenkori irány, ez az algoritmusok átláthatóságát és értelmezhetőségét célozza meg. [3] [7]

BEHATOLÁST DETEKTÁLÓ RENDSZEREK

A behatolást detektáló rendszerek az IDS két alapvető irányzatot ad a szignatúra alapú és az anomália detektálást, melyek eltérő működésre épülnek a források alapján. A források szerint ezek nem egymással versenyeznek, hanem eltérő biztonsági igényeket szolgálnak ki. A szignatúra alapú támadás az ismert támadások felismerésére szolgál. A működése szempontjából, hogy a hálózati forgalmat összeveti, egy előre definiált támadási minta adatbázissal és azonosság esetén riaszt. Ennek előnye a magas megbízhatóság, és az alacsony téves riasztás az ismert fenyegetések szempontjából, azonban hátrány a null napi támadásokkal szemben, amihez nem áll a rendelkezésre szignatúra. Ezzel szemben az anomália alapú detektálás a rendszer normál működését modellezi és nem mintákra épít, így minden olyan viselkedést, ami eltér a normális működéstől, a modell alapján gyanúsnak minősít. Nagyobb rugalmasságot ad, mint a szignatúra alapú rendszer, mert itt képesség van az új típusú támadások felismerésére, viszont magasabb téves riasztás lehet mert a rendszer nehezen különbözteti meg, a valódi támadásokat a forgalmi mintáktól. Azonban itt az anomáliák több típusát megkülönbözteti, a környezetfüggő és egy egymással összefüggő anomáliákat. Összességében itt leírható, hogy az IDS szignatúra alapú megbízható védelmet nyújtanak, az ismert fenyegetéssel szemben, addig az anomália alapú esetében a támadások ellen erősebbnek bizonyulnak. A források alapján a legjobb, ha a két módszert kombináljuk, amely egyesíti az alacsonyhiba arányt és a szélesebb felismerés képességet.

A forrás alapján Brunner Csaba is a kettő kombinációját a hibridet javasolja a hatékony működésre tekintve. Disszertációjában négy alapvető hibrid architektúrát azonosít: a párhuzamos detektálást, a szignatúra anomália szekvenciális detektálást, az anomália szignatúra szekvenciális detektálást, valamint az összetett kevert megoldásokat.

Kutatásai alapján a V3 as modellt találta a leghatékonyabbnak. Ez a modell a stacking neurális hálózatot kombinál mély autoencoder hálózatokkal, amit normál hálózati forgalom alapján tanítanak be, amelynek függvényében a fent leírtak alapján is alkalmas az eltérő minták és anomáliák felismerésére. A teljesítményt tovább növeli az **SVM SMOTE szintetikus mintavételezés** a ritka támadások kiegyensúlyozására.

A V3-as modell különösen hatékonynak bizonyult a ritka, de súlyos fenyegetések például az U2R támadások – felismerésében, ahol **65,82%-os átlagos recall értéket** ért el. Brunner szerint ez azért is előnyös mert a kiberbiztonságban egy elmulasztott támadás nagyobb kockázatot rejthet magában, mint egy téves riasztás. [3][7]

Szerzők szerinti vélemény összehasonlítás

Nagy Attila és Husi Géza munkásságában a gépi tanulás (ML) alkalmazása több alapvető ponton is találkozik annak ellenére, hogy a kutatási területük eltérő. A neurális hálóban mindkét szerző a neurális hálót tekinti a gépi tanulás egyik legfontosabb eszközének. Tárgyalják a publikációjukban, hogy a neuronhálózat rétegekből épül fel, és az emberi agy alapján a neuronok működését szimulálja. Mindkét szerző tárgyalja a felügyelet és felügyelet nélküli tanulási módszert. Nagy Attila a hálózati anomáliák észlelésénél a felügyelet nélküli tanulást helyezi előtérbe, míg Dr. Husi Géza az ellenőrzött tanulást a hiba-visszaterjesztési (backpropagation) modell kapcsán mutatja be. Mindketten egyetértettek abban hogy a gépi intelligencia áttörése a 21. században a megjelenő BIG DATA technológia, és a nagy teljesítményű számítógépnek köszönhető. Nagy Attila megjegyzi, hogy az algoritmusok már korábban a rendelkezésre álltak, csak az erőforrások nem voltak elérhetőek. Mindkét szerző módszernek tekinti a gépi tanulást, azaz a rejtett minták és összefüggések megtalálását. Minkét szerző kimondta, hogy ha egy modell jól van betanítva akkor, általánosan elvárható, hogy a tanító halmazban nem szereplő, de új adatokra is helyes választ adjon. Az osztályzást mindketten alkalmazzák, Nagy Attila a hálózati forgalmat osztja káros és hasznos kategóriákra, Dr. Husi Géza pedig például a kézzel írott karakterek felismerését vagy ipari folyamatok állapotait osztályozza. Azonban van eltérés is, Nagy Attila a gépi tanulást a jövő kvantum- számítástechnikájával és a mély tanulással kapcsolja össze a kiberbiztonságra tekintve, addig Husi Géza a gépi tanulást a fuzzy logikával kombinált hibrid rendszerként mutatja be a mérnöki és ipari folyamatokat adott helyzetben való irányításra. Pl. Daruk irányítása. [1] [2][3][4][5][6][7][8]

Tanulási tényezők kiválasztása

Husi Géza a tanulási tényezők kiválasztását kísérleti és matematikai módszerekkel támogatja.

- Nagy Attila megközelítése:
- A felügyelet nélküli tanulás a hálózati anomáliák észleléséhez
- Kvantum neurális hálózat súlytalanítása és kvantumkeresés.

Összegzésként Husi Géza heurisztikus és automatizált keresési stratégiákat, módszerek támogatja a tanulási tényező megtalálását, míg Nagy Attila esetében a hangsúly az

automatikus mintafelismerésen van. A tudományos szintmeghatározása jelen pillanatban, a fekete doboz jellegű mélytanulástól a hibrid rendszer felé mozdul el.

A JÖVŐ TECHNOLÓGIÁI

A források szerint a klasszikus behatolás érzékelők elavulnak, mert lassú és több hibás jelzést adhat. A hatékonyság növelésének új iránya a mély tanulásban lehet (Depp Learning) mert ez lehetővé teszi a hatékonyabb null napi támadások hatékony kezelése a többrétegű neurális hálózatban. A jelenlegi álláspont szerint a hibrid mély tanuló modellek a leghatékonyabbak, mert képesek a modellek az ismert támadások beazonosítására, de az ismeretlen anomáliák felismerésére is. A kiberbiztonsági modellek hatékonysága a ritka támadások felismerésénél több technológiai és módszertannal javítható lehet. A mély autoencoder hálózatok különös hatékonyság mutatnak, ők a hálózat normál forgalmán tanulnak tapasztalnak, és ennek köszönhetően képesek lehetnek felismerni a ritka anomáliákat is. Az egymásra épülő modellek segítségével pedig pontosabb osztályzást érhetünk el egy komplexebb eseményél. A gépi tanulás jövőjét tekintve a kvantum neurális hálózatok QNN kiemelt szerepet kaphatnak, tekintettel a kvantum gép gyorsaságára, és a párhuzamos számítási feladatok elvégzésére, amely hatékonyabban teszi lehetővő az adathalmazok feldolgozását a gépi tanulási modell számára, és a komplexebb mintázatok felismerésére. A mély tanulás továbbfejlesztése új architektúrát is foglalhat magában, és neurális hálózatokkal pontosabb eredményhez juthatunk optimalizálva az algoritmust is. A megerősítéses tanulás a világban lévő ismeretek és tapasztalataim alapján elmondható, hogy a robotikában, az önvezető járművekben, és a döntéshozó feladatokban elterjedt. A hibrid rendszerek, amelyek kombinálják a rendszereket, mint a neurális hálózatokat és genetikai algoritmusokat gyorsabb és stabilabb tanulást eredményezhetnek. Az aditiv rendszereknek köszönhetően fontos hogy ne felejtsen az MI, amit korábbi időkben szerezett tudást jelent, és amit felhasználhat egy következő feladat megoldásához is, hiszen a környezet egy dinamikusan változó területű is lehet, ahol szintén tapasztalhat és tanulhat az MI. Összességében a gépi tanulás az egyik kiemelt terület számomra is, mert ezen keresztül jobban meg lehet érteni az MI algoritmusok elvi működését is. A jövőt illetően pedig a gyorsabb, és pontosabb intelligens rendszerek fejlesztési irányába halad, amely képesek lehetnek komplexebb problémák megoldására, azonban a véleményem szerint az embernek megszabott korlátok közé kell tenni az MI -t hogy ne veszítse el az ember a kontrollt az MI felett.

ÖSSZEFOGLALÓ

Jelen cikk a szerzők munkájának az összehasonlítási téziseket foglalta magában, amelyek közül kiemeltem a gépi tanulás témakörét. A cikk a gépi tanulás alkalmazásait vizsgálja, a gépi tanulás nemcsak egy eszköz, hanem egy olyan jelenség, ami formálja a tudományos és társadalmi struktúrát. A tanulmány kiemelten elemzi a gépi tanulás témakörét. A szerzők bemutatják a neurális hálózatok ismereteit, tanulási modelleket, a felügyelt és nem felügyelt tanulási módszert, ahol az annotáció minősége meghatározó az algoritmusok pontosságában. A forrásanyagok alapján megállapítható, hogy a kiberbiztonsági rendszerek hatékonysága az alkalmazott módszereken múlik, és nem annyira az algoritmuson, hanem a metrikák és a rendszer beállítások alapján. A közlekedés és behatolás észlelései

különböző rendszereket képvisel, és ez által mások lehetnek az elvárások a működésre tekintve. A recall és az osztályszintű értékelésnek kiemelt szerepe van, de a kritikus támadások felismerése fontos tényező. A konfúziós mátrix jól mutatja a modell hibáinak és tulajdonságainak jellegét. Hogy az eredmények más kutatással összehasonlítható legyen, fontos a jó adatkezelés és tanító és teszt adat elkülönítése egymástól, és az adatszivárgás elkerülése. Ezek megadhatják a mért teljesítmény valós képét. A gyakorlat alapján a hibrid megoldások alkalmazása optimálisabb. Több forrásmunkát összehasonlítva a cikk rávilágít különböző megközelítések formájára, a fókusz a gépi tanulás kutatásában és alkalmazásában van.

Szó esik a közlekedési rendszerekről is, amelynek egyik célja a biztonságos közlekedés. A gépi tanulás kulcsszerepet játszik ebben is, figyelembe véve a környezeti tényezőket. Fontosak a célok, hogy mire kívánjuk alkalmazni a gépi tanulást, és az alapján érdemes választani a megoldási módszereket. Említettem a képfeldolgozás fontosságát a gépi tanulás mellett, amelynek szintén fontos szerepe van az önjáró autók hatékony működésében. A kvantumszámítógépek fontosságát is kiemeltem, amely nagyban segíthet a gyorsabb műveletvégzésben, és a minták felismerésében a modellben az adott környezeti területen. A források technikai szempontból hasonlóságot mutatnak, és közös és ellentétes véleményen alapuló fókuszt kiemeltem a cikkben, ebből is látszik, hogy az alkalmazott modellek eltérőek lehetnek. A kiberbiztonság esetén vannak közös pontok, mert ott a döntéshozatal van kiemelve, az anomália detektálás és behatolásmegelőzés tükrében. Az MI természetét eltérően értelmezik David M Berry a gépi tanulást egy önmagát újratermelő folyamatként írja le, míg Gyarmati Péter az MI-t egy imperatív parancskövető rendszernek tekinti, amely nem képes önálló alkotásra.

Jelen cikk a szerzők munkájának összehasonlítását, filozófiai gondolkodásának a leírásának a célja, hogy ki mit gondolt és milyen módszert preferál az MI alapon a gépi tanuláson ami igen fontos kulcsszerepet játszik, egy mesterséges intelligencián alapuló program működésében. Amit gondolok, mint szerző a kutatásom során, hogy eltérő vélemények vannak az MI vel kapcsolatban, azonban az alkalmazás a választott területtől függ, amelyben a modell és az MI algoritmusa fog majd dolgozni.

FELHASZNÁLT IRODALOM

[1] D. M. Berry, „Bevezetés a gépi tanulás médiaelméletébe” Médiakutató, vol. XXV, no. 2, pp. 53–61, 2024, doi: 10.55395/MK.2024.2.4.

[2] T. Bécsi, S. Aradi, and Á. Fehér, „A gépi tanulás szerepe és hatásai a közlekedésben” Közlekedéstudományi Szemle, vol. 70, no. 1, pp. 54–65, 2020, doi: 10.24228/KTSZ.2020.1.1.

[3] C. Brunner, „Behatolásdetektálás gépi tanulás által” Ph.D. dissertation, Gazdaságinformatika Doktori Iskola, Budapesti Corvinus Egyetem, Budapest, 2020, doi: 10.14267/phd.2020026.

[4] A. Nagy, „Hálózati anomáliák detektálása gépi tanulással” *Információbiztonság*, 2022.

[5] A. Németh and K. Virágh, „Mesterséges intelligencia és haderő – A mesterséges intelligencia területei III. rész” Haditechnika, vol. 56, no. 3, pp. 2–7, 2022, doi: 10.23713/HT.56.3.01.

[6] G. Husi, „Mesterséges intelligencia alkalmazása”. Budapest: TERC Kereskedelmi és Szolgáltató Kft., 2013.

[7] P. Gyarmati, „Gondolatok a mesterséges intelligencia, a gépi tanulás kapcsán (III. rész)” Mesterséges Intelligencia, vol. 5, no. 2, pp. 25–38, 2023, doi: 10.35406/MI.2023.2.25.
[8] B. Cs. Pál and T. Iványi, „Gépi tanulás lehetőségei a marketingkutatásban” in *A (marketing) világ megkettőződése* – Egyesület a Marketing Oktatásért és Kutatásért XXX. Nemzetközi Konferenciájának Absztrakt- és Tanulmánykötete, K. Szűcs, P. Putzer, and M. Törőcsik, Eds., Pécs: Pécsi Tudományegyetem Közgazdaságtudományi Kar, 2024, pp. 112–118, doi: 10.62561/EMOK-2024-10.

DOI: https://doi.org/10.12700/btsz.2026.8.1.107

ACCIDENT INVESTIGATION METHODS, APPROACHES AND APPLICATION POSSIBILITIES IN THE FIELD OF OCCUPATIONAL SAFETY

BALESETKIVIZSGÁLÁSI MÓDSZEREK, SZEMLÉLETMÓDOK ÉS ALKALMAZÁSI LEHETŐSÉGEK A MUNKAVÉDELEM TERÜLETÉN

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

Abstract

Since the era of Ancient Egypt, we have known about workplace accidents and occupational diseases - even if they were not referred to as such at the time and received far less attention than they do today. Although a great deal of time has passed, humanity still has a long way to go in this field. In this article, we present the investigation methods most commonly used in occupational safety today. While society still has room for improvement in reducing the number of accidents, efforts are being made both to proactively prevent negative impacts from occurring and to reactively avoid their recurrence through various investigation and analysis techniques. In our discussion, we will cover both the more traditional and the more modern approaches.

Kulcsszavak

Investigation, workplace accident, methodology

Absztrakt

Egészen az ókori Egyiptom kora óta tudunk munkabalesetekről és foglalkozási megbetegedésekről, még ha akkoriban nem is nevezték így őket és messze nem kapták meg azt a figyelmet, amelyet napjainkban kapnak. Habár sok idő telt el, az emberiségnek ezen a téren még jelentős fejlődési utat kell bejárnia. Jelen cikkünkben bemutatjuk a munkavédelemben használt kivizsgálási módszereket, melyekkel manapság leginkább találkozhatunk. A balesetek számosságában van hova fejlődnie a társadalomnak, hogy jelentősen csökkentse azokat. A másik oldalról mindent megtesz annak érdekében, hogy meg tudja előzni a negatív hatások kialakulását - proaktívan - vagy az ismételt kialakulását - reaktívan - különböző vizsgálási és kivizsgálási módszerek segítségével. Cikkünkben taglalni fogjuk a már mondhatni tradicionális és újkeletű, modern metódusokat is.

Kulcsszavak

Kivizsgálás, munkabaleset, módszertan

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

Mi is a munkabaleset? A jogszabály szerint: „az a baleset, amely a munkavállalót a szervezett munkavégzés során vagy azzal összefüggésben éri, annak helyétől és időpontjától és a munkavállaló (sérült) közrehatásának mértékétől függetlenül.” [1] Hasonlóan fogalmaz a Nemzetközi Munkaügyi Szervezet (továbbiakban ILO) is: olyan esemény, amely a munkahelyen vagy munka közben történik, és amely sérülést vagy halált okoz. [2] A baleseteknek számos hatása van a munkavégzés összes résztvevőjére. Természetesen elsődleges az emberi életre és egészségre gyakorolt hatása. Az emberi test és lélek jóllétét szükséges fenntartani és megőrizni. Másodlagos hatásként a gazdasági következményeket kell megemlíteni. A munkabaleset következtében emberi erő eshet ki a termelésből, valamint a baleset súlyosságától függően akár a teljes telephelyen is leállhat a termelés, amennyiben a hatóság úgy rendelkezik. [1] Végül, de nem utolsó sorban a baleseteknek hatása lehet a munkahelyi morálra, a munkavállalók pszichéjére is. [3] Példának okáért gondoljunk arra, hogy kieshet egy műszakvezető a termelésből vagy akár arra, hogy egy halálos vagy súlyos baleset szemtanúi sokszor sokkos állapotba kerülhetnek és szoronghatnak, minek feloldásához idő és szakemberek támogatása szükséges. A munkavédelemben használt különböző kivizsgálási módszertanok vizsgálata során számos jelenleg már használatban lévő, bejáratott módszerről fogunk számot adni, illetve újkeletű, modern metódusokat is érinteni fogunk, amelyek hamarosan Magyarországon az ipar fejlődésének köszönhetően kényszerűen és szükségesen a mindennapjaink részévé fognak válni, akár egy 5 Why vagy egy Ishikawa.

Az információkat leginkább az interneten elérhető szakirodalmakból, jogszabályokból, szabványokból merítjük és személyes tapasztalatainkkal vegyítve fogjuk alátámasztani az általunk leírtakat. A kutatómunkánk célja, hogy bemutassa, mely módszerek vannak jelen a balesetkivizsgálások között, melyek kevésbé ismertek, elterjedtek. A bemutatni kívánt módszertanok listája nem teljes, természetesen sokkal több létezik a gyakorlatban. A publikáció célja továbbá, hogy későbbi kutatások során a feltárt új módszereket megtaníthassuk a mesterséges intelligenciának, hogy egy társként segítse a kivizsgálásokat. A mesterséges intelligencia használatának legfőbb előnye, hogy képes megőrizni az emberi szakértelmet a számára betanított, kommunikált tapasztalatot, illetve felhasználhatja azt az emberi viselkedésre és kognitív folyamatokra alapozva. A módszerek között több is nagy mennyiségű tudást igényel, mely elsajátítása akár évekbe is telhet. Ellenben, a mesterséges intelligencia, a betáplált adatok függvényében képes mindezt rövid időn belül elsajátítani és érzelmi befolyásoltság nélkül alkalmazni. [4]

A MUNKABALESETEK KIVIZSGÁLÁSÁNAK FEJLŐDÉSE

Kronológiai szempontból különböző szakaszokra oszthatjuk a munkabalesetek kivizsgálási módszereit. Ezeket a módszereket nem kifejezetten a szakma hozta létre, hanem más, többnyire katonai célokat szolgáló létesítményekből, technológiailag előbbre járó cégekből kezdték meg útjukat a civilszféra és ezáltal a munkavédelmi iparág felé. Számos módszert, főleg minőségbiztosítási célokra alkalmaztak először. [5]A történelem során az elsők között jelent meg a napjainkban is igencsak elterjedt Hibafa-analízis (Fault Tree Analysis - FTA). A Bell Laboratories-nél kezdték el használni, azon belül is egészen pontosan az USA légierejének készülő Minuteman rakétaprogramjában. Ezt követően a Boeing

Company fejlesztette tovább a módszertant, akik a minőségi és mennyiségi FTA értékelések érdekében egy továbbfejlesztett technikát és számítógépes alkalmazást hoztak létre. [6]

A módszertan alapvetően egy logikai diagramot takar, amely az adott baleset vagy akkoriban rendszerhiba kialakulásához vezető okokat vizsgálta. A különböző tényezők között ÉS/VAGY kapukat alkalmaz, amelyek különböző részeredményekhez vezethetnek. Legfőbb hátránya, hogy főként a műszaki okokra koncentrál, az emberi tényezőket kevésbé veszi górcső alá. Fő felhasználási területei a repülőgépipar, atomenergiai ipar és a vegyipar. [6] Nem sokkal ez előtt a módszer előtt, még a háborús évek alatt jelent meg egy másik, ma is gyakran használt eszköz, ami a „Hibaállapot- és hatáselemzés" (Failure Mode and Effects Analysis - FMEA) nevet viseli. Maga a módszert a II. világháborúban kezdte el használni az amerikai hadsereg, majd a háború lezárása után kikerült a civilszférába, ahol a NASA és az amerikai gépjárműipar (Ford, GE) kezdte el az elsők között használni. [7] A módszertan célja, hogy a rendszerben előforduló meghibásodási módokat azonosítsa, azok hatását és valószínűségét elemezze.

Az értékelést három szempont alapján végzi:

- a hiba előfordulási valószínűség,
- a hiba észlelhetősége a rendszerben,
- a hiba súlyossága. [7]

Hátránya, hogy nem mindig veszi figyelembe a teljes rendszer vagy az emberi tényezők hatásait. Leginkább a közlekedési iparban, autó és repülő gyártás, valamint egészségügyi eszközök tervezéséhez használják. [7] A harmadik módszer a mennyiségi kockázatelemzés (Quantitative Risk Assessment - QRA), melyet az 1970-es években kezdtek el használni. Ezt már dedikáltan az ipari szféra, főleg az olaj, gyógyszer és gázipar számára dolgozták ki. Statisztikai és valószínűségi számításokat tartalmaz, az adott esemény bekövetkezési valószínűségével és következményeinek súlyosságával értékeli a vizsgált folyamatot, kockázatot. Ez a módszer képezi a mai kockázatértékelések alapjának nagyrészét. Általában egy 2 dimenziós, legalább 3x3-as mátrix az alapja, ennél kisebbet nem szoktak alkalmazni, de a mátrix minél nagyobb, annál részletesebb lesz a kockázatértékelés is. Általánosságban mindenhol használják. [8] A negyedik módszer kronológiai sorrendben az Eseményfa-elemzés (Event Tree Analysis - ETA), amely az FTA módszer kiegészítőjeként jelent meg szintén az 1970-es években. Ez a módszer a baleset következményeinek vizsgálatával foglalkozik elsősorban, hátránya azonban, hogy csak megadott feltételek mentén tud vizsgálni, ismeretlen változókkal nem tud operálni. Leginkább atomiparban, repülésbiztonságban, balesetek kivizsgálásakor és vészhelyzetekben használják a gyakorlatban. [6]

Végül 1972-ben megjelent a SHEL modell, amelyet az ICAO (Nemzetközi Polgári Repülési Szervezet) dolgozott ki. 4 fő jellemzőt vizsgál: **S**oftware (eljárások, szabályok), **H**ardware (eszközök, technológia), **E**nviroment (környezet, külső hatások), **L**iveware (emberi tényezők). A későbbiekben még egy L betűvel bővült, mellyel az emberi tényezők egymásra gyakorolt hatását is tudta elemezni. Leginkább közlekedéstechnikában és egészségügyben használják. [9]

A rendszerszemlélet megjelenése, gyökerei

A rendszerelméletek megjelenése alapvetően a klasszikus, lineáris, egy gyökérokot meghaladó kivizsgálási módszereinek a hátra hagyását jelentette. A megjelent új módszerek alkalmasak voltak már a többtényezős balesetek feltárásához is. A rendszerelméletet az

1940-es évek környékén vetette papírra egy osztrák biológus, Ludwig von Bertalanffy. A célja alapvetően az volt, hogy a különböző tudományágakban megjelenő rendszereket közös szabályok mentén tudja leírni, lehetővé téve, hogy ezeket a tudományokat ne különálló halmazként, hanem azok egymásra való hatását is vizsgálni tudja. [10] Azonban az alapvető rendszerelmélet nem volt alkalmas számos műszaki rendszerben kialakult baleset (például atomerőművek vagy repülőgépek) vizsgálatára, azok komplexitása és összetettsége miatt. Itt jelentett áttörést a James Reason által 1990-ben bemutatott „Swiss cheese modell" („Svájci sajt modell"). Könnyen tudta szemléltetni, hogy az iparban bekövetkezett, bonyolultabb balesetek a többrétegű védelmi vonalak áttörésével jelentkeznek, rendszerszintű hibák együttes meglétével. [11]

A 2000-es évektől Nancy Leveson STAMP (Systems-Theoretic Accident Model and Processes) modellje hozott újabb áttörést, mely a rendszerirányítási folyamatokat, visszacsatolásokat és szabályozási hiányosságokat is vizsgálta, megalakítva ezzel a nemlineáris modelleket. Ezen modellek jellemzői, hogy az időben eltolódó, rejtett okokat is képesek vizsgálni. [12] Az eddig ismertetett történelmi háttérre építve jutunk el a napjainkban használt balesetkivizsgálási módszerekhez, mint a HFACS (Human Factor Analysis and Classification System), FRAM (Functional Resonance Analysis Method), és a Tripod Beta, amelyek a modern rendszerelméletekre épülnek. Ezek a módszerek már összességében képesek vizsgálni a szervezeti kultúra, a kommunikációs csatornák, a munkakörnyezet változékonysága vagy az emberi döntéshozatal összesített hatását. A cél már nem csupán a kiváltó okok meghatározása, hanem a hosszútávó kockázatok csökkentése is, elősegítve ezzel a hatékony prevenciót. [13]

A BALESETKIVIZSGÁLÁS ELTÉRŐ MEGKÖZELÍTÉSEI

A kivizsgálássokkal kapcsolatban különböző szemléletek alakultak ki, melyek mind más-más nézőpontból közelítik meg a balesetek okait és más jelleggel, más fókusszal tárják fel a problémákat. A továbbiakban 3 fő megközelítést különböztetünk meg:

- A technikai (lineáris) megközelítés, mely szempont lényege, hogy a balesetek egyetlen vagy kisszámú technikai vagy emberi hiba következményeként alakulnak ki, ahol lineáris ok-okozati összefüggések állnak fenn. Például: RCA, FTA, 5Why. A megközelítés előnye lényegében a hátránya is mivel egyszerű, ezért könnyen hajlamos lehet az egyén hibáztatásra a rendszerszintű tényezők és nemmegfelelőségek figyelembevétele nélkül. A megközelítés helyes használatához nagyon fontos a kivizsgáló kompetenciája és a beérkező adat minősége.
- Az emberi tényezőkre épülő megközelítés a baleseteket az emberi hibák, döntési problémák és viselkedési tényezők szempontjából vizsgálja. Fókuszát a dolgozók képzettségére, mentális állapotára, valamint kommunikációs és vezetői problémákra helyezi. Például: HFACS. Előnye, hogy átfogóbban értelmezi az emberi hibát és kicsit tágabban tekint a körülményekre, kulturális tényezőkre. Azonban emellett hátrányuk továbbra is, hogy a nem megfelelő minőségű információk esetén könnyen az egyén szintjén keresi a felelősöket.
- A rendszerszemléletű megközelítés a baleseteket mélyebb, komplexebb rendszerek nem megfelelő működésének, strukturális hibáinak tekinti. Vizsgálat során figyelembe veszi a visszacsatolásokat, szabályozási hiányosságokat és külső környezeti

tényezőket is. Például: STAMP/STPA, FRAM, Tripod Beta. Ezen megközelítésnél fontos megemlíteni, hogy kiválóan alkalmazható összetett, komplex rendszerekre is, a vizsgálat eredménye pedig elősegítheti a megfelelő prevenciós gyakorlat kialakítását. Emellett nagy hátránya, hogy meglehetősen idő és tudásigényes, ezáltal nem használható minden balesetre könnyedén. [14]

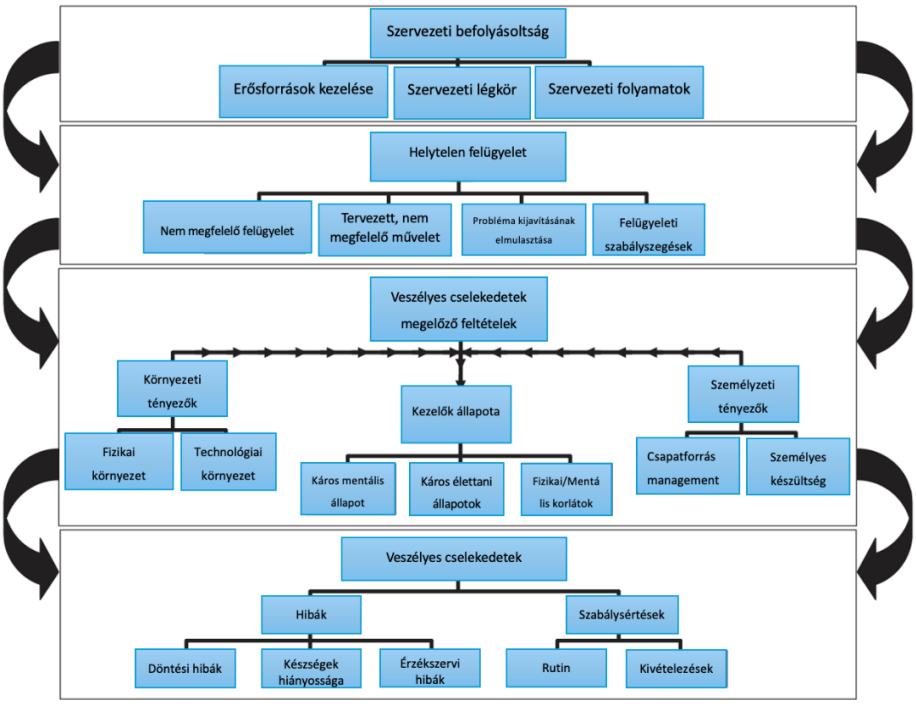
Legújabb trendek a munkabalesetek kivizsgálásában

Napjaink irányvonalát követve a balesetek kivizsgálásai is egyre inkább tolódnak a digitalizáció irányába, ezzel együtt az AI irányába is, ami a jelenlegi szintjén kiváló segítséget nyújt az adatok feldolgozásában, különféle szempontok elemzésében és a mintázatok értékelésében. A hibák rendszerszemléletű megközelítésének hatására teret nyertek a proaktív célkitűzések is, melyek elsődleges célja a gyenge jelekből eredő balesetveszélyes helyzetek korai felismerése.

- Mesterséges intelligencián alapuló elemzések: Egyre inkább elterjednek az ilyen módszerek [15], amelyeknek legnagyobb előnye a mintázatok, ismétlődések felismerése, ezáltal az előre jelezhető kockázatok észlelése, melyeket akár figyelmen kívül is hagyhatnak a szakemberek, főleg, ha jelentkezik az „üzemi vakság”.
- Digitális eseményrögzítés és valós idejű monitoring: A munkahelyeken egyre sűrűbben előfordulnak a különböző okos eszközök, melyek folyamatosan gyűjtik az adatokat működési karakterüknek megfelelően. Általuk a kivizsgálás tényszerű adatokra, képi elemekre is támaszkodhat, konkrét időpontokkal, elfogultság nélkül. Kiváló példa az eseményrögzítésre a számos analitikai funkció mellett dőlésérzékelővel vagy személyi védőeszköz érzékelési funkcióval ellátott kamerák.
- Rendszerszintű szemlélet: Egyre több szervezet és cég ismeri fel, hogy a balesetek kivizsgálásnak nem egy adott, hibás személy megtalálása a célja, hanem sokkal inkább a rendszerszintű hiányosságok feltárása, megfelelő megelőző intézkedések meghatározása és alkalmazása a gyakorlatban. Ezek által a hangsúly sokkal inkább a visszacsatolási ciklusok fejlesztésén lesz. Legismertebb eszköze ezen szemléletnek a „Just culture” („Igazságosság kultúra”).
- Kiterjesztett valóság (AR), virtuális valóság (VR) és szimulációk: Ezen eszközök és technológiák nagyon sok helyen és nagyon színesen használhatóak. Feltűnhetnek például a balesetek rekonstruálásában, mint interaktív szimulációs eszközök, melyek a döntéshelyzetek újra játszásában és elemzésében nyújthatnak segítséget. A VR eszközök ezen felül oktatási célból nyithatnak meg új lehetőségeket (pl.: egyéni védőeszközök oktatása, ahol következmény nélkül betekintést nyerhetnek a munkavállalók a balesetekbe is akár). Az AR eszközök pedig gyakorlati feladatoknál helyezhetik új alapokra a jelenlegi módszertanunkat (pl.: Kizárás-kitáblázás (Lock out-Tag out, LOTO) utasítások térbeli megjelenítése egy egyszerű telefon segítségével, esetleg termelői gépek átállásánál az utasítások a digitális térben is megjelenhetnek).
- Integrált biztonsági management rendszerek (pl.: ISO 45001): Összefoglalja, egységesíti a különböző kockázatok értékelését, incidensek kezelését, nyomon követését, ezáltal elősegíti a balesetek kivizsgálását és feldolgozását, azokból az adatok kinyerését (pl.: különböző, kulcsfontosságú teljesítménymutatókhoz (Key Process Indicator - KPI). [16]

MÓDSZERTAN

HFACS (Human Factor Analysis and Classification System) egy alapvetően a „Swiss Cheese" modell által inspirált módszer, mely lényege, hogy meghatározott struktúra alapján (1. ábra) osztályozza az emberi hibákat és az ezek mögött fellelhető szervezeti tényezőket. A vizsgálatot 4 szinten folytatja, melyek hierarchiája az alábbi módon néz ki. [13]

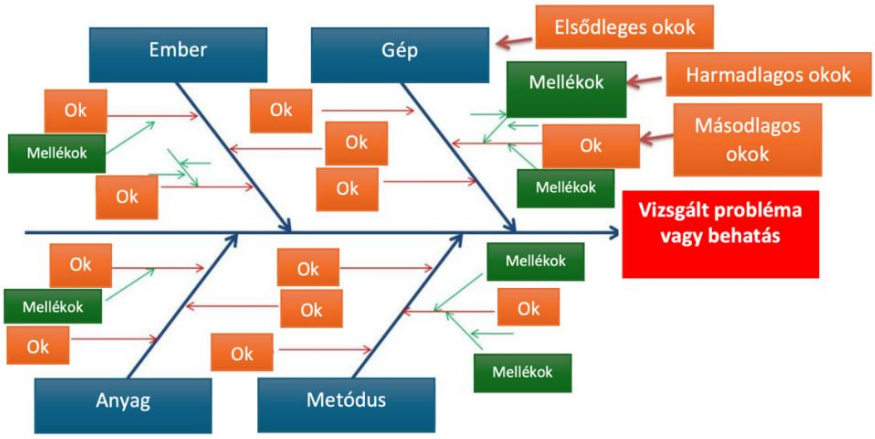


1. ábra HFACS struktúra, a szerzők szerkesztése [17]

Az analízis elvégzésével egy összességében átfogó, minden réteget érintő eredményt fogunk kapni, melyekben a rendszerszintű, emberi tényezők részletesen elemzésre kerülnek. Hátránya, hogy a megfelelő végzéshez tréningek szükségesek, előzetes ismeretek nélkül téves megállapításokhoz vezethet. A korlátaihoz tartozik, hogy kvalitatív jellegű. [13]

Root Cause Analysis (RCA - Gyökérok elemzés) Az elemzés célja, hogy a balesetek mögött meghúzódó gyökérokokat feltárja. Alapvetően napjainkban is használatos, eléggé elterjedt eszköz. Az elemzés elvégzéséhez kettő eszközt szoktak jellemzően használni:

- 5 Miért (5-Why): az eseménylánc feltárását szolgáló eszköz. Folyamatos „Miért?" kérdések feltételével deríti fel a vizsgált esemény történéseit. Kutatások alapján 5 kérdés után már elég mélyen a probléma gyökeréhez kerülhetünk.
- Ishikawa - vagy halszálka diagram (2. ábra): 4-6 kategóriába sorolja a lehetséges okokat, melyek általában: ember, módszer, gép, anyag, de ezektől el lehet térni. Erőssége, hogy gyors és nagyon jól strukturált módszer, valamint már a köztudat részét képezi. Emellett hátránya, hogy elsősorban a lineáris ok-okozati logikán alapszik, amely nem mindig tükrözi néhány eset komplexitását. [18]

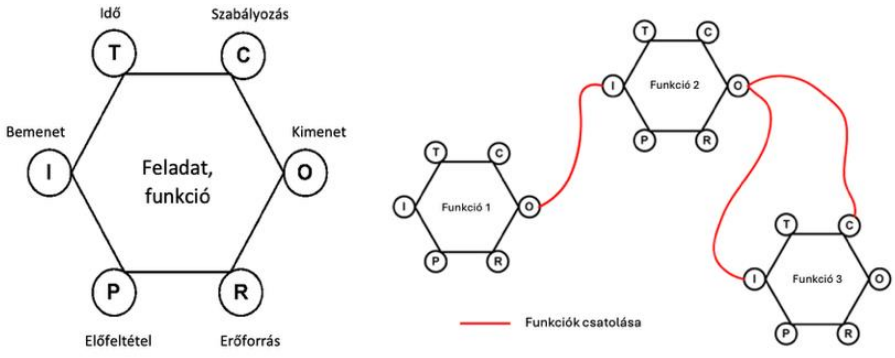


2. ábra Ishikawa diagram felépítése, a szerzők szerkesztése [19]

Napjainkban az RCA elemzéshez már léteznek „polcról levehető”, azaz előre elkészített keretrendszerek. Ezek közül világvezetőként talán a TapRooT® említhető. Egy előre definiált, magasan standardizált szoftver, amely könnyen implementálható bármilyen ipari környezetben, akár más célra is. [18]

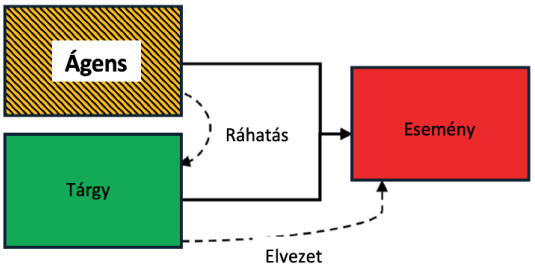
Accident Tree Analysis (ATA - Hibafa elemzés) a baleseti vagy hibafa elemzés egy erős vizualitáson alapuló módszer, mely az eseményláncokat tárja fel hatékonyan (3. ábra). AND/OR (ÉS/VAGY) kapuk segítségével mutatja, hogy az esemény milyen döntések mentén következhetett be. Előnye az átláthatóságában rejlik, mivel jól dokumentálható, és összességében egy jó logikai struktúrát nyújt. Hátránya, hogy komplex esetekben alkalmazása időigényes lehet, valamint függ az eredménye a beérkezett adatok minőségétől, pontosságától. [18]

FRAM (Functional Resonance Analysis Method - „Funkcionális rezonancia-elemző módszer”) A módszert Hollangel dolgozta ki, azzal a céllal, hogy a komplex rendszerek viselkedését elemezze. Alapvetően az események helyett a funkciók kölcsönhatásait vizsgálja és azok egymásra gyakorolt rezonanciáját (3. ábra). Előnye, hogy képes nagyon összetett rendszereket is vizsgálni, viszont cserébe a modellezése bonyolult és egyedi szakismeretet igényel. [14]



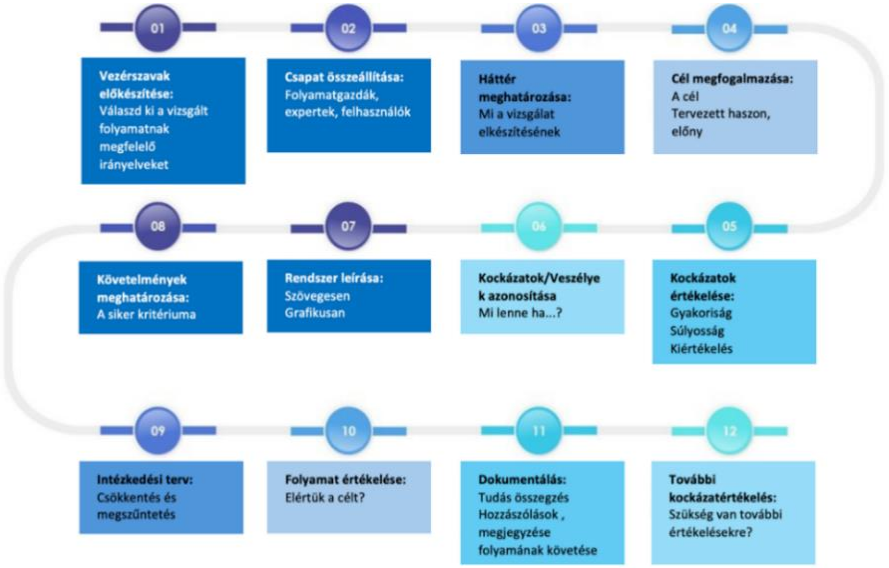
3. ábra FRAM modell felépítése, a szerzők szerkesztése [20]

Tripod beta módszer az alapvető hibamódok és a védelmi rések feltárására szolgál (4. ábra). Elősegíti főként a szervezeti és a rendszerbeli hiányosságok, valamint a balesethez vezető rejtett okok feltárását. Általában nem, mint önálló módszer, hanem mint más módszerek támogatására szolgáló eszköz használják. A metódus főként a „mit", „hogyan", és „miért" kérdésekre válaszol. [21]



4. ábra Tripod beta vizuálisan, a szerzők szerkesztése [21]

SWIFT (Structured What-If Technique – Strukturált „Mi lenne, ha" technika) egy alapvetően proaktív, jövőbe tekintő módszer. „Mi lenne, ha" kérdésekkel operálva a projektek, munkafolyamatok elején használják, mely segítségével különböző baleseti veszélyforrásokat a csapat előre azonosíthat (5. ábra). Segít a kockázatokkal szembeni érzékenyítésben, illetve mélyíti a csapat jövőorientált (proaktív) kockázatkezelését. [22]



5. ábra SWIFT metódus, a szerzők szerkesztése [23]

ÖSSZEFOGLALÁS

A következtetéseket levonva megállapíthatjuk, hogy a kivizsgálási módszerek elsősorban a hadiparból, másodsorban az atomenergia iparból, illetve a légi közlekedésből származnak, azokon belül is főként a minőségbiztosítás területéről, melyeket átvett a mun-

kavédelem és végül a civilszféra. Ezen szakterületekre elmondható, hogy hatékony, a problémát feltáró módszerekre van szüksége, hiszen egy nem azonosított hiba könnyen százak, ezrek életét követelheti. Az általunk elsőként vizsgált módszer a HFACS volt, melynek legfőbb fókusza az emberi és szervezeti hibák feltárásán van, mivel alapvetően egy preventív és rendszerszintű vizsgálatot tesz lehetővé. Hátránya, hogy használata meglehetősen tréningigényes, és kvalitatív módszer, amely mellőzi a kvantitatív eredményeket. A második módszer a már klasszikusnak mondható RCA, azaz gyökérok-elemzés volt. Tény, hogy ez nem a legújabb eszköz, azonban fontosnak találtuk megemlíteni, mivel napjainkban ez az egyik legelterjedtebb és a munkavédelem területén is legjobban használható kivizsgálási módszer. Előnye, hogy gyorsan elvégezhető, nagyon részletekbe is mehet és strukturált képet ad vissza a végén a balesetről és annak miértjeiről. Hátránya viszont, hogy nagyon lineárisan szemléli az esetet, valamint könnyen hibás konklúziót eredményezhet a beérkezett adatok és a csapat munkájának függvényében (lehet, gyors, de nem szabad a gyorsaságra törekedni az alaposság rovására). Fontos, hogy mindig a Jéghegy modell-el együtt alkalmazzuk. A következő módszer az FTA, azaz Hibafa elemzés volt, mely a logikai események láncolatát vizsgálja. Előnye, hogy könnyen átlátható és a kivizsgálás alatt végig strukturált marad, főleg ÉS/VAGY kapukkal operál, azonban ezt a metódust kifejezetten csak az egyszerűbb balesetekre érdemes használni, mivel a komplexitást nem kezeli. Egyszerű események egyszerű sorozatát tárja fel. A soron következő a FRAM volt, mely a funkcionális kölcsönhatásokra helyezi a hangsúlyt, ezáltal a komplex események vizsgálatára is alkalmas. Sajnos emiatt hátránya, hogy maga a modellezés nagyon bonyolult, ténylegesen tréning szükséges a használatához. Ezt követően megvizsgáltuk a Tripod beta módszert. Itt a szervezeti kockázati tényezők vizsgálatára kerül a hangsúly, feltárva ezáltal a szervezetek hiányosságait a munkabalesetek tükrében, ezáltal kifejezetten kerüli a személyek hibáztatását. Ez a módszer is meglehetősen kvalitatív, nagyon kevés kvantitatív szempontot foglal magában. Végül az utolsó eszköz a SWIFT volt, mely nem is kifejezetten a balesetek bekövetkezésének okát vizsgálja, hanem egy preventív szemléletet biztosít, melyben főként baleseti forgatókönyveket készít az adott csapat, például egy új technológia bevezetése, egy projekt megkezdése előtt. Viszont fontos megemlíteni, hogy ez csak egy szubjektív eszköz, nagyon függ a használhatósága a csoport hozzáállásától. Amennyiben egy igazi, akár kompromisszumkész és munkavédelmi szempontból érett csapat gyűlik össze, úgy kifejezetten jól működhet. Ezáltal összességében elmondható, hogy kutatómunkánk 6 módszert mutatott be, melyből 2 napjainkban is már jelen van a munkavédelem területén. Ugyanakkor 4 még nem igazán terjedt el, azonban felépítésüknek köszönhetően feltételezhető, hogy pár éven belül találkozni fogunk velük a szakmában is.

FELHASZNÁLT IRODALOM

[1] „1993. évi XCIII. törvény - Nemzeti Jogszabálytár”. Elérés: 2025. november 18. [Online]. Elérhető: https://njt.hu/jogszabaly/1993-93-00-00

[2] International Labour Organization, „Investigation of occupational accidents and diseases | International Labour Organization”. Elérés: 2025. november 18. [Online]. Elérhető: https://www.ilo.org/publications/investigation-occupational-accidents-and-diseases

[3] M. Ghisi *és mtsai.*, „Psychological Distress and Post-Traumatic Symptoms Following Occupational Accidents”, *Behavioral Sciences*, köt. 3, sz. 4, o. 587–600, okt. 2013, doi: 10.3390/bs3040587.
[4] Dr. habil. Kollár Csaba PhD, „A mindennapok mesterséges intelligenciája”, Slideshare. Elérés: 2025. november 18. [Online]. Elérhető: https://www.slideshare.net/slideshow/a-mindennapok-mesterseges-intelligenciaja-pptx/278737871
[5] Heinrich H. W., *Industrial Accident Prevention (1941)*. Mcgraw-hill Book Company Inc., New York and London, 1941. Elérés: 2025. november 18. [Online]. Elérhető: http://archive.org/details/dli.ernet.14601
[6] U.S. Nuclear Regulatory Comission, „NUREG-0492, »Fault Tree Handbook«.”.
[7] D. H. Stamatis, *Failure mode and effect analysis: FMEA from theory to execution*, 2. ed., rev.Expanded, [Nachdr.]. Milwaukee, Wis: ASQ Quality Press, 2008.
[8] E. Salzano és A. Basco, „Simplified model for the evaluation of the effects of explosions on industrial target”, *Journal of Loss Prevention in the Process Industries*, köt. 37, o. 119–123, szept. 2015, doi: 10.1016/j.jlp.2015.07.005.
[9] F. H. Hawkins és H. W. Orlady, *Human factors in flight*, 2nd ed. Hampshire: Avebury technical, 1993.
[10] L. Von Bertalanffy és J. W. Sutherland, „General Systems Theory: Foundations, Developments, Applications”, *IEEE Trans. Syst., Man, Cybern.*, köt. SMC-4, sz. 6, o. 592–592, nov. 1974, doi: 10.1109/TSMC.1974.4309376.
[11] James Reason, „(PDF) "Human Error, " by James Reason (Book Review).”, *ResearchGate*, aug. 2025, Elérés: 2025. november 18. [Online]. Elérhető: https://www.researchgate.net/publication/220108440_Human_Error_by_James_Reason_Book_Review
[12] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press, 2012. doi: 10.7551/mitpress/8179.001.0001.
[13] D. A. Wiegmann és S. A. Shappell, „A Human Error Approach to Aviation Accident Analysis”.
[14] E. Hollangel, „The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems”. Ashgate, 2012.
[15] British Safety Council, „AI: a powerful new tool for managing safety risks”, British Safety Council. Elérés: 2025. november 18. [Online]. Elérhető: https://www.britsafe.org/safety-management/2024/ai-a-powerful-new-tool-for-managing-safety-risks
[16] K. H. D. Tang, „Artificial Intelligence in Occupational Health and Safety Risk Management of Construction, Mining, and Oil and Gas Sectors: Advances and Prospects”, *J. Eng. Res. Rep.*, köt. 26, sz. 6, o. 241–253, máj. 2024, doi: 10.9734/jerr/2024/v26i61177.
[17] Douglas A. Wiegmann, „Figure 1. The Human Factors Analysis and Classification System (HFACS)”, ResearchGate. Elérés: 2025. november 18. [Online]. Elérhető: https://www.researchgate.net/figure/The-Human-Factors-Analysis-and-Classification-System-HFACS_fig1_252682635
[18] Bjørn Andersen, „(PDF) Root Cause Analysis: Simplified Tools and Techniques, Second Edition”, ResearchGate. Elérés: 2025. november 18. [Online]. Elérhető: https://www.researchgate.net/publication/233862776_Root_Cause_Analysis_Simplified_Tools_and_Techniques_Second_Edition

[19] TQP, „What is a Fishbone Diagram? Ishikawa Diagram | Cause & Effect Diagram”, Tech Quality Pedia. Elérés: 2025. november 18. [Online]. Elérhető: https://techqualitypedia.com/fishbone-diagram-ishikawa-diagram/
[20] J. Vankeirsbilck, „FRAM in a nutshell – PAN-EUROPEAN TRAINING, RESEARCH AND EDUCATION NETWORK ON ELECTROMAGNETIC RISK MANAGEMENT”. Elérés: 2025. november 18. [Online]. Elérhető: https://etn-peter.eu/2021/02/11/fram-in-a-nutshell/
[21] Stichting Tripod Foundation, „Tripod Beta | Tripod”. Elérés: 2025. november 18. [Online]. Elérhető: https://tripod.energyinst.org/beta
[22] „SWIFT - Acquisition Safety and Environmental Management System”. Elérés: 2025. november 18. [Online]. Elérhető: https://www.asems.mod.uk/printpdf/toolkit/swift
[23] Jeremiah Genest, „Structured What-If Technique as a Risk Assessment Tool”, Investigations of a Dog. Elérés: 2025. november 18. [Online]. Elérhető: https://investigationsquality.com/2021/05/08/the-swift-risk-assessment-tool/

DOI: https://doi.org/10.12700/btsz.2026.8.1.119

LABOUR SAFETY OF ROBOTIC SURGICAL DEVICES: RISKS ARISING FROM THE USE OF ROBOTIC SURGICAL INSTRUMENTS

ROBOTSEBÉSZETI ESZKÖZÖK MUNKAVÉDELME: ROBOTSEBÉSZETI ESZKÖZÖK HASZNÁLATÁBÓL SZÁRMAZÓ KOCKÁZATOK

SIMON Mátyás[1] – SZABÓ Gyula[2]

Abstract

Robotic surgery poses new challenges in the field of occupational health and safety, where it is necessary to identify the pathogenic factors and risks associated with robot-assisted surgeries. Our research was conducted by means of a questionnaire survey of surgeons and residents working at the largest healthcare, teaching and research university in Hungary and an ergonomic analysis for both robotic surgery and laparoscopic and conventional procedures. The results show that robotic surgery is more ergonomic than open or laparoscopic surgeries. Analyses of occupational risk factors in healthcare workers showed that the most common risk factors are ergonomic, psychosocial and biological risk factors. Ergonomic measures and the management of pathogenic factors are very important in robotic surgery, as they can optimise surgical performance and minimise health risks.

Keywords

occupational safety, ergonomics, occupational health protection, robotic surgery, occupational safety measures

Absztrakt

A robotizált sebészet a munkavédelem szakterületén új kihívásokat jelent, ahol azonosítani kell a robotasszisztált műtétekkel kapcsolatos kóroki tényezőket és kockázatokat. Kutatásunk Magyarország legnagyobb egészségügyi ellátó, oktató és kutató egyetemen dolgozó sebészek és rezidensek kérdőíves felmérésével és az ergonómiai elemzéssel történt mind a robotsebészeti, mind a laparoszkópos és hagyományos eljárásokhoz. Az eredmények azt mutatják, hogy a robotsebészet ergonomikusabb, mint a nyitott vagy laparoszkópos műtétek. Az egészségügyi dolgozók munkahelyi kockázati tényezőinek elemzései azt mutatták, hogy a leggyakoribb kockázati tényezők az ergonómiai, pszichoszociális és biológiai kockázati tényezők. Az ergonómiai intézkedések és a kóroki tényezők kezelése nagyon fontosak a robotsebészetben, mivel optimalizálhatják a sebészeti teljesítményt és minimalizálhatják az egészségügyi kockázatokat.

Kulcsszavak

munkavédelem, ergonómia, munkahelyi egészségvédelem, robotsebészet, munkabiztonsági intézkedések

[1] matyas.simon86@gmail.com | ORCID:0000-0002-2714-857X | PhD Student, Óbuda University Doctoral School of Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szabo.gyula@bgk.uni-obuda.hu | ORCID: 0000-0002-3963-2916 | Associate Professor, Óbuda University | egyetemi docens, Óbudai Egyetem

INTRODUCTION

Robotic surgery is the most advanced technology of the 21st century. In the field of occupational health and safety, it is necessary to identify the causal factors and risks associated with robot-assisted surgery, as well as the occupational safety measures and consequences of the coronavirus pandemic and medical gases used in healthcare. [10][11] Since robot-assisted surgery improves the effectiveness of medical interventions in terms of successful surgical outcomes and patient recovery, it is very important to create an appropriate working environment and ergonomics, ensure the availability of occupational safety equipment and reduce psychosocial risks.

LITERATURE REVIEW

Medical robots facilitate surgeries, simplify clinical processes and hospital logistics, and improve patient care and workplace safety. [1] For example, tissue damage, bleeding, complications, duration of surgery, length of hospital stay and time off work. The introduction of laparoscopic surgical techniques greatly reduced these risks, although this technique made it difficult or impossible to access certain areas, and the cameras used only provided a two-dimensional image of the surgical site.

Industrial robots became widespread in the 1980s. In the mid-1980s, brain biopsies were performed under CT guidance using a modified PUMA-560 industrial robot. In the United Kingdom, the PROBOT robot was developed to perform prostate surgery through the urethra, which allowed for the reconstruction of the prostate and the proper removal of the organ. Prostatectomy was thus considered the first robotic surgery, and in the late 1980s, Integrated Surgical Supplies developed the Robodoc robot specifically for hip replacement surgery. [2]

In the 1990s, robotic surgery and the tools necessary for its wider application were further developed. Robotic abdominal surgery became possible with the introduction of Computer Motion AESOP (Automatic Endoscopic System for Optimal Positioning). AESOP was a robotic arm that allowed surgeons to control the orientation of a conventional laparoscope using foot pedals and voice commands. Four years later, Computer Motion introduced the second-generation Zeus robotic system, which was the first robotic system to offer instrument control in addition to camera control. Zeus consisted of three robotic arms (one for 2D laparoscopy and two for controlling surgical instruments). The camera was controlled by voice commands similar to those used for AESOP, while the surgeon controlled the manipulators from a remote console. The computer translated the surgeon's movements to the laparoscopic instruments; the Zeus system had the same 2D video screen as the laparoscope. [2] Using the Zeus robotic system, surgeons in New York performed the first remote robotic in situ surgery, a cholecystectomy on a patient in Strasbourg. A special optical network was used for this surgery, and several similar transatlantic surgeries have already been performed on pigs. Remote surgery was limited by bandwidth and cost; while ZEUS was under development, Intuitive Surgical introduced the da Vinci robotic surgical system. The da Vinci Surgical System is the most sophisticated robotic surgical system; in March 2006, the first remote surgery using the da Vinci robotic system was performed via the public internet between the , University of Cincinnati, and Intuitive Surgical in California. [2] Robots are now used not only in operating theatres but also in clinical settings

to support healthcare professionals and improve patient care. During the COVID-19 pandemic, for example, hospitals and clinics introduced robots to perform a wider range of tasks in order to reduce exposure to pathogens. [1] [10]

METHODOLOGY

The research was conducted at the patient care unit of Hungary's largest healthcare, teaching and research university. Data collection was carried out through an on-site visit to a clinic using a robotic surgical device, observation of surgery, review of occupational safety documentation, and a questionnaire survey. The on-site visit took place on one occasion, where a qualitative survey and interviews were conducted with the doctors operating the robotic surgical device and the staff assisting during preparation and surgery. In addition, a questionnaire survey was conducted with seven doctors on the use of the robotic surgical device and a comparison of traditional surgical and laparoscopic procedures. The results of the questionnaire survey were compared with the results of international research. During the review of occupational safety documentation, 200 pages of professional material were reviewed.

CONCLUSIONS

The growing popularity of robotics constantly poses new challenges for occupational health and safety. Working with robots must always be considered from an occupational health and safety perspective as they evolve. In many cases, people still need to adapt to the possibility of working with robots. In the coming years, robot-human collaboration will take on increasingly diverse forms, robots will become more autonomous, and human-robot collaboration will take on entirely new forms. Existing approaches and technical specifications for working with robots, which protect workers from task-related risks, must be continuously reviewed.

Introduction to robotic surgical tools

Doctors use a variety of technologies to extend their capabilities beyond the human body. Magnetic resonance and computer tomography scanners, for example, allow doctors to see inside the body. Similarly, many surgeons use the da Vinci system to perform robotic surgery. [3]

Intuitive, a pioneer in robotic surgery and manufacturer of the da Vinci surgical system, was founded in 1995. [4] The first da Vinci system, a special surgical robot designed for minimally invasive surgical procedures, was launched in 1999. A fourth surgical arm was added in 2003. The latest version, the da Vinci Xi model, was released in 2014; according to Intuitive, the Xi offers improved functionality compared to previous models and is optimised for complex procedures. [5]

Today, da Vinci continues to develop and improve its robotic systems, enabling surgeons to expand their capabilities. [4] The da Vinci robot is not an automated surgical system, but a teleoperative tool for the specialist, who usually sits directly next to the robot in the operating theatre with the patient. The main advantage of the da Vinci system is that the specialist can use smaller robotic instruments that require smaller incisions, as well as visual enhancements such as thermal imaging, which provide valuable information that is

not available to the human eye alone. [5] The da Vinci vision system provides high-resolution three-dimensional imaging, giving the surgeon a clear view of the surgical site magnified ten times larger than the human eye.

The da Vinci surgical system consists of four arms equipped with interchangeable surgical instruments. One arm is typically equipped with a camera, while the other arms are equipped with instruments such as scalpels, graspers, cauterisers and staplers. [6] Surgeons use small instruments that move like the human hand, but with a much greater range of motion. The system's built-in tremor filter technology allows the technician to move all instruments smoothly and accurately. The da Vinci system translates the surgeon's hand movements to the console in real time and performs the bending and rotation of the instruments as the procedure progresses. The small articulated instruments move like the human hand, but with a wide range of motion, allowing for very precise surgical manipulation [4].

Figure 1: Structure of a robotic surgical instrument [6]

The da Vinci robot is also equipped with haptic feedback: early models vibrate when the software detects a collision, while newer models give a similar signal if the surgeon moves too quickly or moves outside the field of view. The ergonomic console also ensures the comfort of the surgeon's body. They no longer have to crouch over the operating table for hours. [6] Doctors at Semmelweis University say the following about the surgical robot and its capabilities: "With this robot and this application, we will be able to reliably apply the most advanced surgical techniques." Robotic surgery will play an important role, especially in cancer surgery. For the patient, a significant advantage of the robotic surgical device programme is that the movements performed by the surgeon will be more delicate and precise, leading to a significant reduction in collateral trauma. This significantly reduces recovery time, time spent in intensive care and the need for blood transfusions. The device has seven degrees of freedom, allowing it to move its arm through 520 degrees. As a result, areas that were previously very difficult to reach with open surgery, and sometimes even with laparoscopy, are now easily accessible. The system consists of three main parts. The part that comes into direct contact with the patient is the robot itself, which in this case has four arms. Next to it is a surgical console through which the surgeon communicates with the robot's body and performs the surgery. The third part contains all the equipment necessary for the surgery, including screens and displays, as well as a high-frequency cutter that ensures surgical safety and haemostasis.

A surgeon sits at the surgical console. What could only be seen in two dimensions during laparoscopic surgery can now be seen in three dimensions. The resolution starts at 10x magnification and can be increased from there. Furthermore, as it can be controlled with the fingers, it allows for greater freedom and finer movements. This is a special device with two consoles. There are not many of them in the world, as universities are educational institutions that train doctors and medical graduates. Robotic surgery is divided into the five stages shown in the figure below, with the main focus on robot preparation and use. Each stage has a starting and ending point and involves one or more tasks.

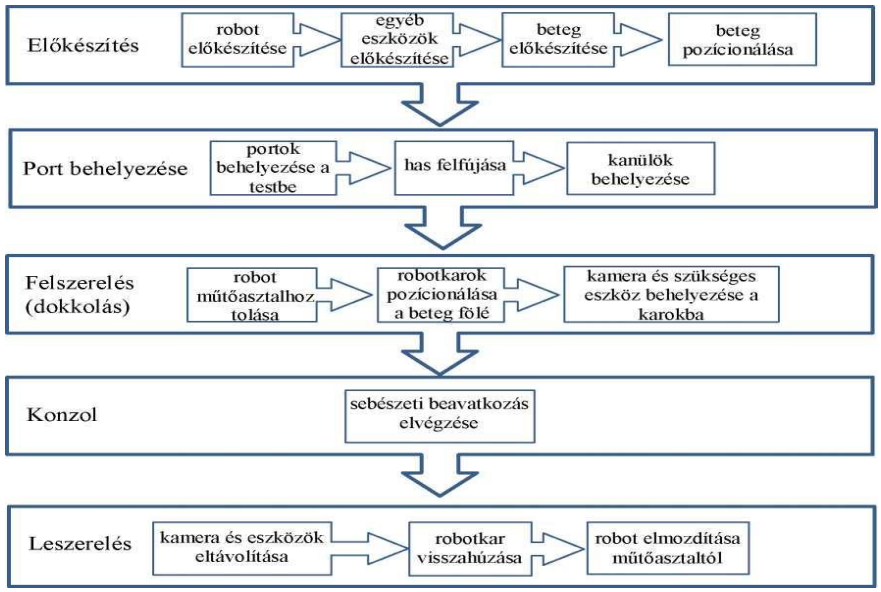


Figure 2: Phases of the robotic surgery procedure. 15]

Processes:

Preparations - During the preparation phase, the assistant performs four tasks, including preparing the robot and positioning the patient on the operating table. Anaesthesia begins after induction of anaesthesia and ends immediately before the first skin incision. This includes preparing the robotic equipment, other surgical instruments and the patient.

Port insertion - During the port placement phase, the surgeon, with the help of an assistant, inserts the cannula into the patient's abdomen and inflates the abdominal cavity to ensure working space. It begins with the initial skin incision and ends when all cannulas are in place and the robot is ready for docking.

Equipment - The preparation phase is divided into three steps: (1) moving the robot from the corner of the room to the operating table; (2) positioning and securing the robot arm to the patient's cannula; and (3) inserting the instruments and cameras into the robot arm. This begins when the team member first starts moving the robot towards the operating table. It ends when the camera and the last instrument are properly secured to the robotic arm and connected to the patient's cannula. These tasks are performed by the surgeon and assistants.

Console - Once the robotic arm is in place, the surgeon walks over to the robotic console in the operating theatre, sits down, and begins the operation. The surgeon usually works alone. For example, he or she changes instruments, cleans the camera, or performs suction. It begins when the surgeon first sits down at the console, announces that the surgeon has finished, and ends when the surgeon steps away from the console.

Dismantling - At the end of the operation, the robotic arm retracts and the assistant places the robot in a corner of the operating theatre. Figure 3 shows the area of the operating theatre where the surgeon and assistant work.

Figure 3: Operating theatre with robotic surgical equipment (source: author's own work)

The workflow analysis provided an overview of the tasks required for robotic surgery. Five stages of robotic surgery were identified to describe the typical steps of robotic surgery. The surgical team works to achieve goals related to safety, timeliness, sterility, resources, roles, and location. However, the order and emphasis of these goals may vary depending on the culture of the operating theatre. [7]

Identifying and assessing risks

Prolonged surgery causes eye strain. Looking at the monitor during surgery can cause discomfort, which has a negative effect on the surgeon. When surgery is performed with the aid of a surgical robot, the surgeon controls the robot from a surgical console, while an assistant monitors the operation on an external monitor. e concentration on the display can cause eye fatigue. Since the work takes place in a virtual space, this can easily lead to headaches and is very dangerous in this profession, as it affects concentration, accuracy and attention stability. In addition to the above complaints, working with monitors often causes dry eyes, which can also be uncomfortable. Dry eyes refer to the inability of the eyes to produce and maintain sufficient quantities of quality tear fluid.

Since the eyes and head are reflexively connected, any tension or discomfort in the eyes can spread to the head and neck, causing headaches. The combined effect of these factors can lead to errors, reduced work efficiency and stress, all of which must be taken into account from a health and safety perspective. Although surgical procedures require great effort on the part of the surgeon performing the operation, factors other than the use

of surgical robots also influence the physician's performance. During surgery, the physician controls the robot and the robotic arm via a console, but is not directly present at the surgical site. Poor coordination between surgical instruments and a lack of three-dimensional spatial awareness can cause additional stress. The need to deal with unforeseen situations can be stressful even for experienced surgeons. When workers are already stressed, it is difficult for them to concentrate and think. Problem-solving skills may decline and reaction times may increase. Since the robotic arm has no sensors, the surgical team must be fully aware of the robotic arm and its movements. The use of robotic surgery does not negate the importance of teamwork. Poor communication or disruption of teamwork can lead to morbidity. Inadequate flow of necessary information can also lead to surgical errors and complications.

New procedures and learning processes can place a significant psychological burden on clinicians. Starting to use new instruments or working with new instruments is a significant psychological burden until it becomes routine. This morbidity factor can be significantly reduced through training and simulation exercises in which doctors participate before performing the actual procedure. In addition, after training, the patient must undergo an examination, the success of which determines whether the surgeon will subsequently be authorised to perform the procedure. Although only indirectly related to the robotic surgical procedure, an appropriate working environment is also important. Proper lighting is key to preventing eye strain and fatigue during surgery. The proper placement of monitors is also important. If the monitors are not positioned at the correct height, it will be difficult to follow the surgery, which will affect image clarity, visibility and perception. Every member of the team must be able to monitor what is happening. The role of the surgeon's hands is taken over by the robotic arm, so the same regulations that apply to the surgeon's hands and the surgical instruments used also apply to the arm and the instruments it contains. There is also a risk of droplet infection if the doctor and the robot control centre are in the same operating theatre as the patient. Surgical instruments must be handled and disinfected in the same way as in normal medical procedures. Care must be taken to ensure that disposable instruments are used for their intended purpose. Surgical instruments must be cleaned and disinfected in accordance with safety regulations, as damage to surgical instruments poses the same risk to the outcome of the operation. It is also important that the surgical instruments on the arm are properly secured. At the start of each operation, the correct functioning of the surgical robot must be checked, for example, the correct functioning of the arm and the correct securing of the instruments.

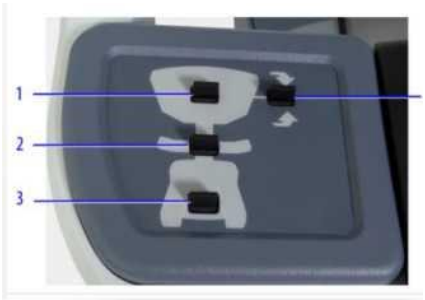
Ergonomics

In this context, the machine-human relationship is the relationship between the robot and the surgeon controlling it, and the work environment is the operating theatre. However, it is not only the surgeon who is present in the operating theatre, but also the assistants working alongside the surgeon. While controlling the robot, the surgeon continuously monitors the progress of the operation in a virtual space. Therefore, the surgeon sits for several hours watching the 3D display (Figure 14). In the case of long operations, the doctor spends a considerable amount of time watching the events unfold with his head in front of the 3D display. This part of the control centre, where the doctor

observes events taking place in 3D space, must be ergonomically designed to provide comfortable head support.

Figure 4: 3D viewing display of a robotic surgical device [12]

It is also important that they are at the correct angle and height adjustable, but even so, it can be difficult for the neck after a while if the head is held at a constant angle. Lack of blood circulation can lead to headaches, numbness and pain. In addition, keeping your head in the same position for a long time while looking at the 3D display can cause discomfort in the forehead area. It is important that the surface is easy to clean, yet soft and flexible. During surgery, doctors sit in the same position, which puts a lot of strain on the spine and skeletal muscles and requires great physical effort. The surgeon's seat must also be ergonomically designed so that the doctor can sit in the correct posture. The adjustment options for the surgical console are shown in Figure 5.



1. 3D viewer height
2. Armrest height
3. Foot switch panel depth
4. 3D viewer tilt

Figure 5: Robotic surgery console adjustment options [13]

Surgeons experience high levels of mental stress during operations. Headaches or back pain during surgery can affect the outcome of the surgical procedure. Risk factors must always be taken into account because lives are at stake. Incorrect posture during surgery can lead to health and musculoskeletal problems later on. When using robotic surgical

technology, the hands and fingers are also subjected to increased stress, as the robot's arm simulates the surgeon's movements and provides the working surface for the arm.

Figure 6: Surgical console control options [14]

Surgical robots performing operations have multiple arms, so there are multiple control panels and consoles in the work area. Since doctors operate these panels and consoles throughout the operation, ergonomic design and placement are very important. If not designed properly, the controls will be uncomfortable and fingers and hands will tire quickly. The controls must be easy to operate, and the forces applied must not exceed the dynamic and static loads permitted on the surgeon's operating limb. It is important that they are designed so that the surgeon can distinguish them by touch without moving his head. Supports designed to rest the surgeon's hands and facilitate the holding of instruments should be comfortable and designed to enhance comfort. 's poor ergonomic settings can lead to: - incorrect posture - uncomfortable working position - numbness in the hands - insufficient blood circulation in the fingers - hand fatigue The surgeon controls the pedals with their feet, and their adjustment can also have a significant impact on the quality of work. The pressure surface, shape and size of the pedal have a significant impact on the ease and comfort of using the foot and pedal. The surface and width of the foot pedal should be such that the foot can rest comfortably on it. The pressure surface should have a suitable non-slip surface to prevent the surgeon's foot from slipping during surgery. Ergonomic considerations and the management of pathological factors are critical in robotic surgery in order to optimise surgical procedures and minimise health risks.

Comparison of research results

The above results are confirmed by international research, such as a survey conducted by Sara Monfared and her colleagues, in which 20 surgeons and surgical trainees analysed 29 robotic and 48 laparoscopic procedures. After the laparoscopy, numbness in

the right finger and stiffness in the right shoulder were observed, as well as irritability in the surgeon, while after the robotic surgery, increased back stiffness was observed. The aim of the study was to compare the ergonomic risks between surgeons and surgical trainees performing robotic and laparoscopic procedures. Robot-assisted surgery resulted in lower postoperative discomfort and muscle tension in both upper limbs, especially on the surgeon's dominant side, but compared to laparoscopy, it increased static neck position with subjective back stiffness. These recognised ergonomic differences between the two platforms can be used to develop preventive measures. [8]

The analysis conducted by Ian Jun Yan Wee and colleagues included 29 articles. Studies using objective measurement tools showed that robotics offers significant ergonomic advantages and reduced workload compared to laparoscopy for both surgeons and trainees. Survey studies also showed that self-reported discomfort was lower during robotic procedures than during laparoscopy and open surgery. Robotic surgery is ergonomically superior to open and laparoscopic surgery. However, the level of physical exertion remains significant and should be addressed through formal ergonomic training and proper familiarisation with the console. [9]

CONCLUSIONS AND RECOMMENDATIONS

Simulation and practical training should be at the centre of training, as this can provide surgeons with a routine that can prevent musculoskeletal disorders and reduce potential stress and psychological strain. Staff should be routinely trained in correct posture and the adjustment of the surgeon's console during surgery. Warm up before surgery (fingers, wrists, shoulders and hips) and, for longer surgeries, perform various exercises for the hands, arms and hips. Drink water regularly during surgery (sometimes coffee during longer surgeries). After a complex operation, the patient must be allowed to rest and recover mentally before moving on to the next patient. Well-thought-out work schedule: scheduling of operations (taking into account the number, complexity and duration of operations); sufficient quantity and quality of rest time for recovery.

SUMMARY

Our lives and work – whether in an office, industrial or medical setting – are often unimaginable without interaction with machines. In many cases, machines facilitate human tasks, but the right balance between humans and machines must be found. Ergonomic considerations and the management of pathological factors are very important in robotic surgery, as they can optimise surgical performance and minimise health risks. Regular expert evaluation, appropriate training, education and continuous improvement of techniques can all contribute to improving the ergonomics of robotic surgery. The aim of our research is to confirm the risk factors I have identified and to identify the health risks they pose. The risk factors involved are closely related to the work environment, as the occurrence of risk factors is strongly influenced by the work performed by the employee, the work process, and the tools and materials used during the work. Analyses of occupational risk factors for healthcare workers have shown that the most common risk factors are ergonomic, psychosocial and biological risk factors.

REFERENCES

[1] INTEL: Robotics in Healthcare: The Future of Robots in Medicine https://www.intel.com/content/www/us/en/healthcare-it/robotics-in-healthcare.html (Referenced: 15 January 2025)

[2] Alberto Mendivila, Robert W. Hollowayb, John F. Boggess: Emergence of robotic assisted surgery in gynaecological oncology: American perspective https://www.researchgate.net/publication/51437277 Emergence of robotic assisted surgery in gynaecological oncology American perspective#pf2 (Referenced: 15 January 2025)

[3] DURANGO Outpatient Surgery Centre website: Da Vinci X ROBOTIC ASSISTED SURGERY https://www.durangooutpatient-sc.com/robotic-assisted- surgery/ (Accessed: 15 January 2025)

[4] INTUITIVE: Robotic-Assisted Surgery with da Vinci Systems https://www.intuitive.com/en-us/patients/da-vinci-robotic-surgery (Accessed: 15 January 2025)

[5] IEEE - Advancing Technology for Humanity: Robots, Da Vinci https://robotsguide.com/robots/davinci (Accessed: 15 January 2025)

[6] IEEE Spectrum - Matt Beane: TODAY'S ROBOTIC SURGERY TURNS SURGICAL TRAINEES INTO SPECTATORS https://spectrum.ieee.org/robotic-surgery (Accessed: 15 January 2025)

[7] Stacey Cunningham, Amine Chellali, Isabelle Jaffré, Jean-Marc Classe, Caroline G L Cao: Effects of Experience and Workplace Culture in Human-Robot Team Interaction in Robotic Surgery: A Case Study https://www.researchgate.net/ publication/235459563_Effects_of_Experience_and_Wor kplace_Culture_in_Human -Robot_Team_Interaction_in_Robotic_Surgery_A_Case_Study (Accessed: 15 January 2025)

[8] Sara Monfared, Dimitrios I. Athanasiadis, Luke Umana, Edward Hernandez, Hamed Asadi, Cameron L. Colgate, Denny Yu & Dimitrios Stefanidis (2022) 2021 SAGES Oral Volume 36, pages 8397–8402, (2022)

[9] Ian Jun Yan Wee, Li-Jen Kuo, James Chi-Yong Ngu (2020), A systematic review of the true benefit of robotic surgery: Ergonomics, https://doi.org/10.1002/rcs.2113

[10] Simon Mátyás (2022), Work safety during COVID-19 Work safety measures and consequences of the coronavirus pandemic in healthcare, BIZTONSÁGTUDOMÁNYI SZEMLE 4 : 2 pp. 103-110. , 8 p.

[11] Simon, Mátyás ; Dr. Daruka, Norbert ; Dr. Szabó, Gyula (2024), The dangers of medical gases in terms of critical healthcare infrastructure, In: Horváth, Richárd; Lukács, Judit; Stadler, Róbert; Pinke, Péter (eds.) Engineering Symposium at Bánki Lectures: Proceedings of the Engineering Symposium at Bánki (ESB 2023), Budapest, Hungary: Óbuda University 367 p. pp. 355-360. , 6 p.

[12] Operate with efficiency, https://sofmedica.com/wp-content/uploads/2024/06/da-Vinci-Xi-Brochure-EU.pdf] (Referenced: 15 January 2025)

[13] Intro to daVinci Robotic Surgery Simulation, https://surgicalskillslab.ucsf.edu/ sites/default/files/umbraco/media/14274857/intro-to-robotic-surgery-simulation-3-9-2021.pdf (Accessed: 15 January 2025)

[14] Wireless Teleoperation Control Interface of Articulated Forceps for Minimally Invasive Surgery - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/da-Vinci-Handle-Diagrams-4_fig6_327561755 (Accessed: 15 January 2025)

[15] Stacey Cunningham, Amine Chellali, Isabelle Jaffre, Jean-Marc Classe, Caroline G. L. Cao. Effects of Experience and Workplace Culture in Human-Robot Team Interaction in Robotic Surgery: A Case Study. International Journal of Social Robotics, 2012, 5 (1), pp.75-88. ff10.1007/s12369-012-0170-yff. ffhal-00757340f

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