



ISSN 2676-9042

Vol 5, No 2, 2023.

2023, V. évf. 2. szám

Safety and Security Sciences Review

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

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált,
szakmai és tudományos folyóirata



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

On the cover can be seen | A borítón

BORS Györgyi

painter/festőművész

The flower of life | Az élet virága

painting | című festménye látható

© Bors Györgyi, 2021

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



Electronic Periodicals Archive & Database

Elektronikus Periodika Adatbázis

<https://epa.oszk.hu/04100/04186>



Hungarian Periodicals Table of Contents Database

Magyar folyóiratok tartalomjegyzékeinek kereshető adatbázisa

https://matarka.hu/szam_list.php?fsz=2267&nyelv=hun



Digital Archives of Óbuda University

Óbudai Egyetem Digitális Archívum



Országos Széchényi Könyvtár - Digitális Könyvtár

National Széchényi 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>

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságstudomány nemzetközi, lektorált, szakmai és tudományos folyóirata
<p style="text-align: center;">COLUMNS</p> <p style="text-align: center;">Material Safety Philosophy and History of the Safety and Security Security Policy Security Systems Security Awareness Domotics Health Security Food Safety Economic Security War Security and Law Enforcement Information Security Industrial and Operational Safety Legal and Social Security Book Review Security of Environment Traffic Safety Facility Security Private Security Artificial Intelligence Safety and Security in General Technical Security</p>	<p style="text-align: center;">ROVATOK</p> <p style="text-align: center;">Anyagbiztonság Biztonságfilozófia és -történet Biztonságpolitika Biztonságtechnika Biztonságtudatosság Domotika Egészségbiztonság Élelmiszer-biztonság Gazdasági biztonság Hadbiztonság és rendvédelem Információbiztonság Ipar- és üzembiztonság Jog- és társadalombiztonság Könyvismertetés Környezetbiztonság Közlekedésbiztonság Létesítménybiztonság Magánbiztonság Mesterséges intelligencia Munkabiztonság Műszaki biztonság</p>
<p>The aim of the journal is to publish studies, research reports, book reviews for professionals working in the field of security science or related sciences, 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.</p> <p>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.</p> <p>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.</p> <p>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).</p>	<p>A folyóirat célja a biztonságstudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek, vagy a téma iránt érdeklődők számára a katonai műszaki tudományok, s így a biztonságstudomány tágan értelmezett diszciplináris keretében tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetőik megjelentetése, s ennek révén a biztonság-tudatosság és a biztonsági kultúra fejlesztése. Tudjuk, hogy a biztonságstudományok művelésébe beletartozik a had-, rendészeti- és biztonságstörténet 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.</p> <p>Megjelenés negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.</p> <p>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.</p> <p>Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).</p>

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>

Edited by Editorial Board | Szerkeszti a Szerkesztőbizottság

Chairman of the Editorial Board | A Szerkesztőbizottság elnöke

Prof. Dr. RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Scientific Secretary of the Editorial Board, person responsible for editing | A szerkesztőbizottság tudományos titkára, a szerkesztésért felelős személy

Dr. habil. KOLLÁR Csaba PhD

kollar.csaba@uni-obuda.hu

Members of the Editorial Board | A szerkesztőbizottság tagjai

Prof. Dr. BÁNÁTI Diána banati@mk.u-szeged.hu

BEREK László berek.laszlo@lib.uni-obuda.hu

Dr. habil. BEREK Tamás PhD berek.tamas@uni-nke.hu

Prof. Dr. BESENYŐ János besenyo.janos@uni-obuda.hu

Prof. Dr. CVETITYANIN Livia cpinter.livia@bgk.uni-obuda.hu

Prof. Dr. Dragan JOVANOVIĆ draganj@uns.ac.rs

Prof. Dr. Jeffrey KAPLAN kaplan@uwosh.edu

Dr. habil. KOVÁCS Tünde PhD kovacs.tunde@bgk.uni-obuda.hu

Dr. Cyprian Aleksander KOZERA PhD c.kozera@akademia.mil.pl

Prof. Dr. Maashutha Samuel TSHEHLA samuel@sun.ac.za

Prof. Dr. Manuela TVARONAVIČIENĒ manuela.tvaronaviciene@vgtu.lt

Staff of the Editorial Board | A szerkesztőbizottság munkatársai

BELÁZ Annamária, SZALÁNCZI-ORBÁN Virág

English language lecturer | Angol nyelvi lektor

BEKE Éva

Technical editor | Technikai szerkesztő

HARTMANN László

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

The Journal's Professional-Scientific Advisory Board	A Folyóirat Szakmai-Tudományos Tanácsadó Testülete
---	---

Chairman of the Advisory Board | A Tanácsadó Testület elnöke

Prof. Dr. GODA Tibor DSc.

Az Óbudai Egyetem Biztonságtudományi Doktori Iskola vezetője

Members of the Advisory Board | A Tanácsadó Testület tagjai
in alphabetical order | ABC sorrendben

Prof. Dr. HAIG Zsolt mk. ezredes

A Nemzeti Közsolgálati Egyetem Katonai Műszaki Doktori Iskola vezető helyettese
A Védelmi elektronika, informatika és kommunikáció kutatási terület vezetője

Prof. Dr. KÓNYA Zoltán DSc.

A Szegedi Tudományegyetem Környezettudományi Doktori Iskola vezetője

Prof. Dr. KORINEK László akadémikus

A Magyar Rendészettudományi Társaság elnöke

LONTAI Márton

A Nemzeti Szakértői és Kutató Központ főigazgatója

Prof. Dr. PADÁNYI József DSc. mk. vezérőrnagy

A Nemzeti Közsolgálati Egyetem Katonai Műszaki Doktori Iskola vezetője

Prof. Dr. RÉGER Mihály DSc.

Az Óbudai Egyetem Anyagtudományok és Technológiák Doktori Iskola vezetője

TIKOS Anita

WOMEN IN IT SECURITY (WITSEC) Egyesület elnökségi tagja

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 5, No 2, 2023. | **2023. V. évf. 2. szám**

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

BAKOSNÉ DIÓSZEGI Mónika

dioszegi.monika@bgk.uni-obuda.hu

Mónika DR. BAKOSNÉ DIÓSZEGI is associate professor at the Institute of Natural Sciences and Basic Subjects of the Donát Bánki Faculty of Mechanical and Safety Engineering at Óbuda University, deputy director of the Institute. Head of the Biogas Research Laboratory at Óbuda University. She has been involved in research related to anaerobic fermentation since 2012. She wrote his doctoral dissertation on this topic, entitled: Investigation of the effect of special mechanical pretreatment to increase biogas yield. The main topic related to anaerobic research, for example, aims to utilize the energy and raw material content of municipal wastewater and sewage sludge. The new technological elements: pre-hydrolysis of the secondary sludge before digestion, extraction of organic matter and plant nutrients in the leachate of the fermentation bioreactor, extraction of nutrients from the leachate from the dewatering of the digested sludge, a new composting-vermicomposting process. An important research direction is also the effect of mechanical pretreatment of substrates on the yield and quality of biogas.

BAKOSNÉ DR. DIÓSZEGI Mónika, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Természettudományi és Alapozó Tantárgyi Intézet docense, az Intézet igazgatóhelyettese. Az Óbudai egyetem Biogázkutató laboratóriumának vezetője. Az anaerob fermentációhoz kapcsolódó kutatási tevékenységgel 2012 óta foglalkozik. A doktori disszertációját is ebből a témakörből alkotta meg, melynek címe: Speciális mechanikus előkezelés hatásának vizsgálata biogáz hozam növelése céljából. Főbb anaerob kutatással kapcsolatos témakör például a kommunális szennyvizek és szennyvíziszapok energia- és nyersanyag-tartalmának hasznosítását célozza. Az új technológiai elemek: a szekunder iszap rothasztás előtti előhidrolizálása, a fermentációs bioreaktor csurgalékvizében lévő szervesanyagok és növényi tápanyagok kinyerése, tápanyag kivonás a rothasztott iszap víztelenítéséből származó csurgalékvízből, új komposztálási-vermikomposztálási eljárás. Fontos kutatási irány továbbá a szubsztrátumok mechanikai előkezelésének a biogáz hozamra és minőségére vonatkoztatott hatása is.

BAUMGARTNER Helga

baumgartner.helga@phd.uni-obuda.hu

Helga BAUMGARTNER, safety engineer, PhD Student at the Doctoral School for Safety and Security Sciences Óbuda University. Her reserach focuses on face recognition in crime prevention and countering terrorism.

BAUMGARTNER Helga biztonság-technikai mérnök, az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási területe az arcfelismerés alkalmazása a bűnmegelőzésben és a terrorizmus elleni védekezésben.

BEZSENYI Anikó

bezsenyia@fcsm.hu

I have been working at Budapest Sewage Works Pte Ltd. as a biologist-engineer since 2007. I am currently managing research and development projects. In the course of my work, I come across almost all biological aspects of wastewater treatment (measurement development, biofilters, anaerobic digestion, composting, wastewater treatment). I worked as an expert in several countries, usually as a member of a team at wastewater treatment plants (Bucharest, 2011 and 2013; Szófia, 2013; Zagreb, 2017; Nur-Szultan, 2019). I teach the subject of hydrobiology at

2007 óta dolgozom a Fővárosi Csatornázási Művek Zrt-nél biológus-mérnökként. Jelenleg kutatás-fejlesztési projekteket tartok kézben. A munkám során a szennyvíztisztítás szinte összes biológiai aspektusával találkozom (mérésfejlesztés, biofilterek, rothasztás, komposztálás, a szennyvízkezelés optimalizálása). Szakértőként több külföldi nagyvárosban is dolgoztam, általában szakértői csapat tagjaként szennyvíztisztító telepeken (Bukarest, 2011 és 2013; Szófia, 2013; Zágráb, 2017; Nur-Szultan, 2019.). Hidrobiológia tantárgyat oktatok az Óbudai Egyetem

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

the Urban Wastewater Management Engineer training course of the University of Óbuda (ÓU) and also Environmental Protection and Wastewater Treatment subjects as a guest lecturer. Between 2017 and 2022, I was a PhD student at the Doctoral School of Material Sciences and Technologies of ÓU. I am currently writing my dissertation "Enhancing of the biological removal of pharmaceutical residues in wastewater treatment technology".

Települési szennyvízgyártóközadási szakmérnök képzésén, illetve vendégelőadóként részt veszek Környezetvédelem és Szennyvíztisztítás tárgyak oktatásában. 2017 és 2022 között voltam az Óbudai Egyetem Anyagtudományok és Technológiák Doktori Iskolájának PhD-hallgatója. Jelenleg a disszertációmot írom. Kutatási területem „A gyógyszermaradványok biológiai eltávolításának serkentése a szennyvíztisztítási technológiában”.

BODNÁR László

bodnar.laszlo@uni-nke.hu

Fire Captain László BODNÁR, is a professional fire officer at the National Directorate General for Disaster Management of the Ministry of Interior. He works as an assistant lecturer at the University of Public Service, Faculty of Law Enforcement Institute of Disaster Management Department of Fire e Protection Engineering. He began his studies at the University of Public Service and obtained the BSc degree in defence administration as a Defence Administration Organizer in 2014 and in 2016 the MSc degree in defence administration as a Defence Administration Manager. He began his PhD studies in 2016 at the Doctoral School of Military Engineering at the University of Public Service and defended his thesis in 2021. His research interest is Research and development of methods to increase the effectiveness of fire-fighting in case of wildfires.

BODNÁR László tűzoltó százados a BM Országos Katasztrófavédelmi Főigazgatóság hivatásos állományú tagja. Szolgálatát tanársegédként a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Tűzvédelmi Mérnöki Tanszékén látja el. Tanulmányait a Nemzeti Közszolgálati Egyetemen végezte, ahol 2014-ben védelmi igazgatási szervező, majd 2016-ban védelmi igazgatási vezetői diplomát szerzett. Doktori tanulmányait 2016-ban kezdte meg a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolában, ahol 2021-ben sikeresen megvédte doktori értekezését. Kutatási területe az erdőtűzek oltásának hatékonyságát növelő módszerek kutatása és fejlesztése.

BODOR Károly

bodor.karoly@ek-cer.hu

Károly BODOR works at the Centre for Energy Research (15 years) and ELI ALPS (10 years). He has been involved in the radiation protection design and implementation of ELI ALPS since 2008. ELI ALPS is a huge opportunity not only for Hungary but also for the EU. It was immediately clear that in addition to traditional radiation protection knowledge, new procedures should be developed, and new knowledge and visions, as well as an interdisciplinary approach, would be needed. To this end, he participated in the meetings and conferences held during the preparatory phase of ELI, and mastered the FLUKA Monte Carlo code, then unavailable in Hungary. During his career, he supervised several diploma theses with his colleague and one-time supervisor Dr. Péter Zagyvai. As a radiation protection expert and designer, he supports the implementation of radiation protection at ELI ALPS. In order to make the actual operation as safe as possible in terms of radiation protection, we need to understand the pro-

BODOR Károly vagyok, az Energiatudományi Kutatóközpont (15 év) és az ELI ALPS munkatársa (10 év). Az ELI ALPS sugárvédelmi rendszerének tervezésébe és megvalósításába 2008-ban kapcsolódtam be. Az ELI ALPS óriási lehetőség nemcsak Magyarországon, de az EU számára is. Rögtön világossá vált, hogy a hagyományos sugárvédelmi tudás mellett új eljárásokat kell kidolgozni, illetve új ismeretekre és látásmódra, interdiszciplináris megközelítésre lesz szükség. Ennek érdekében részt vettem az ELI előkészítési fázisában megtartott találkozókban, konferenciákban, valamint elsajátítottam az akkor még Magyarországon nem használt ún. FLUKA Monte Carlo kódot. Munkám során több diplomamot vezettem Dr. ZAGYVAI Péter kollégámmal, témavezetőmmel. Sugárvédelmi szakértőként és tervezőként támogatom az ELI ALPS üzemelését. Ahhoz, hogy sugárvédelmi szempontból a lehető legbiztonságosabb legyen a tényleges üzemelés, meg kell értenünk az ELI-ben a lézerfény-anyag kölcsönhatás során zajló

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

cesses taking place in the laser-matter interactions at ELI ALPS. We are also developing methods to be practiced, for which we have started the implementation of training courses.

folyamatokat. Módszereket kell kidolgozni, amelyek begyakorlásához kezdtük el megvalósítani a sugárvédelmi gyakorló tanpályákat.

DÉR Attila Tibor

der.attila@uni-obuda.hu

Attila DÉR is a student at the Doctoral School of Safety Sciences at the Bánki Donát Faculty of Mechanical and Safety Engineering, University of Óbuda. He holds a degree in Certified electrical engineer from the Specialization in industrial surveillance and communication systems of Kandó Kálmán Faculty of Electrical of engineer. His research interests include cybersecurity, protection of critical infrastructures in particular energy supply.

DÉR Attila az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán lévő Biztonságtudományi Doktori Iskola hallgatója. Okleveles villamosmérnöki végzettségét a Kandó Kálmán Villamosmérnöki Karán szerezte Ipari felügyeleti és kommunikációs rendszerek specializációján. Kutatási területei a kiberbiztonság, kibervédelem, kritikus infrastruktúrák védelme különös tekintettel az energiaellátásra.

EDELMANN Dóra

edelmann.dora@phd.uni-obuda.hu

Dóra EDELMANN is a PhD student at Doctoral School on Safety and Security Sciences, Óbuda University. She graduated as civil engineer from the Faculty of Civil Engineering of the Budapest University of Technology, and as fire protection engineer from the Faculty of Architecture of the Budapest University of Technology. Her research area is crowd dynamics and safety.

EDELMANN Dóra az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója. Okleveles építőmérnöki végzettségét a Budapesti Műszaki Egyetem Építőmérnöki Karán, tűzvédelmi szakmérnök végzettségét a Budapesti Egyetem Építészmérnöki Karán szerezte. Kutatási területe az embertömegek mozgása és biztonsága.

ELEK Barbara

elek.barbara@bgk.uni-obuda.hu

Barbara ELEK is a geophysical environmental engineer, fire protection engineer. She is an associate professor at the Institute of Safety Science and Cybersecurity of the Donát Bánki Faculty of Mechanical and Safety Engineering of Óbuda University. She is the head of training of the faculty's EHS engineer and specialist training. Lec-turer and supervisor of the university's Doctoral Scholl on Safety and Security Sci-ences. Her research areas are: fire and explosion protection, safety issues of vital energy systems and facilities, environmental safety.

ELEK Barbara okl. környezet-geofizikusmérnök, tűzvédelmi szakmérnök. Jelenleg az Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar Biztonságtudományi és Kibervédelmi Intézetében egyetemi docens, valamint a kari EHS szakmérnök és szakember képzés képzésvezetője. Az egyetemi Biztonságtudományi Doktori Iskola oktatója, témavezetője. Kutatási területei: tűz- és robbanás elleni védelem, energetikai létfonosságú rendszerek és létesítmények biztonsági kérdései, környezetbiztonság.

HEGYI Henrietta

hegyi.henrietta@uni-obuda.hu

Henrietta HEGYI is a student at the Doctoral School of Safety Sciences at the Bánki Donát Faculty of Mechanical and Safety Engineering, University of Óbuda. She holds a degree in Information Security from the National University of Public Service, Faculty of Electronic Information Security Management

HEGYI Henrietta az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán lévő Biztonságtudományi Doktor Iskola hallgatója. Információbiztonsági végzettségét a Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakán és az Óbudai Egyetem Etikus Hacker

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

and the Ethical Hacker course at the University of Óbuda. His research interests include cybersecurity, information security, IT security, geopolitics. Besides his studies, he works as an IT security consultant and project manager.

tanfolyamán szerezte. Kutatási területei a kibertudomány, információbiztonság, informatikai biztonság, geopolitika. Tanulmányai mellett IT-biztonsági tanácsadóként és projektmenedzserként dolgozik.

HORVÁTH-KÁLMÁN Eszter

kalman.eszter@ybl.uni-obuda.hu

I have a PhD in geotechnical engineering and since graduating I have been teaching continuously in universities, first at the Budapest University of Technology and then at the Óbuda University. In addition to my teaching career in universities, I have worked continuously in the industry. I was involved in the construction of metro line 4 as a geotechnical engineer for the contractor. After the completion of metro line 4, I participated in the design preparation works of Paks 2 as a geotechnical engineer and since then I have been continuously present in Paks as a geotechnical expert, where I am still learning a wide range of professional knowledge and experience in the identification, management and mitigation of risks.

Geotechnikai szakterületen szereztem PhD fokozatot. Az egyetem befejezése óta folyamatosan tanítok a felsőoktatásban, először a Budapesti Műszaki Egyetemen, majd utána az Óbudai Egyetemen. A felsőoktatási oktatói pályafutásom mellett folyamatosan dolgoztam a szakmában. Részt vettem a 4-es számú metróvonal kivitelezésben, mint a beruházó geotechnikus szakembere. Majd a 4-es metró befejeztével a Paks 2 tervezés előkészítési munkáiban vettem részt, mint geotechnikus és azóta is folyamatosan jelen vagyok Pakson mint geotechnikai szakértő, ahol szerteágazó szakmai tudást és tapasztalatot tanulok a mai napig a kockázatok meghatározása, kezelése és csökkentésének lehetséges megoldásai témában.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Csaba KOLLÁR is a communications engineer, certified communications specialist, electronic information security manager, doctor of economics (PhD), habilitated doctor (Dr. habil.) of military engineering (safety and security sciences), cybernetic, consultant, coach, mediator. His research interests include the social aspects and economic impacts of the digital age, with a focus on the human aspects of information security, information security awareness, human-robot interaction, smart city, artificial intelligence, social credit systems, domotics. He is a senior research fellow at the Óbuda University, head of the Artificial Intelligence Workshop, 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. Chairman of the professional qualification exams. Senior consultant and coach of PREMA Consulting, expert of the Hungarian Society of Military Science and the National Association of Human Professionals. Member of the Artificial Intelligence Consortium since Q4 2018.

KOLLÁR Csaba kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), a katonai műszaki tudományok (biztonságtudomány) 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, a domotika. Az Óbudai Egyetem tudományos főmunkatársa, 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. Elnök a szakmai képesítő vizsgákon. A PREMA Consulting vezető tanácsadója és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévtől a Mesterséges Intelligencia Konzorcium tagja.

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

KOVÁCS-SZELECZKI Xénia

xeniaszelezcki@googlemail.com

She completed her bachelor's degree at Szent István University's Faculty of Agriculture and Environmental Sciences, where she graduated in 2009 as a certified agricultural engineer in environmental management. She spent a year in Stuttgart as an Erasmus scholar, where, in addition to her studies, she worked as a research assistant at the University of Hohenheim. After that, in 2010 she participated in projects related to wastewater treatment in Germany as a fellow of the Institute for Environment and Energy, Technology and Analytics e.V. as a scholar of The German Federal Foundation for the Environment. She completed her Fire Safety Engineering studies at the Ybl Miklós University, obtained her professional engineering degree in 2016, after which he deepened his occupational safety technician studies at the Budapest University of Technology and Economics, where she obtained a professional Occupational Safety and Health Engineer diploma in 2019. Since 2011, she has been active in the industry in the areas of environmental, occupational and fire protection.

A Szent István Egyetem Mezőgazdaság- és Környezettudományi Karán végezte az alapidplomáját, ahol okleveles környezetgazdálkodási agrármérnök diplomát szerzett 2009 -ben. Stuttgartban egy évet töltött Erasmusos ösztöndíjasaként, ahol tanulmányai mellett tudományos segédmunkatársként dolgozott a Hohenheimi Egyetemen. Ezt követően 2010-ben a Deutsche Bundesstiftung Umwelt ösztöndíjasaként vett részt szennyvíztisztítással kapcsolatos projektekben Németországban az Institut für Energie und Umwelttechnik eV. munkatársaként. Tűzvédelmi tanulmányait az Ybl Miklós Egyetemen végezte, szakmérnöki diplomáját 2016-ban szerezte meg, ezt követően munkavédelmi technikus tanulmányait a Budapesti Műszaki és Gazdaságtudományi Egyetemen mélyítette el, ahol munkavédelmi szakmérnök diplomát szerzett 2019-ben. 2011 óta az iparban tevékenykedik környezet- munka és -tűzvédelmi területeken.

KUN Tamás

kun.tamas@uni-obuda.hu

Tamás KUN, is certified economist and currently pursuing a PhD in Military Sciences at Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary, where he has been lecturing since 2019. His expertise is in the areas of social engineering and geopolitics, pertaining to cyberspace activities. In the course of his research, he examines the operation of communication channels and their application trends, the impact of which is closely related to changes in geopolitical processes, such as the inevitable role of social media and the appearance of topics about military activities in daily information. In his writings, the examination of the human factor as a vulnerable point of systems, which is important not only in information security, but also in the analysis of social processes, comes into focus several times. He's author of a chapter titled as The War on Disinformation: The Structure of Trust in Understanding the Contemporary Information Landscape: A Handbook.

KUN Tamás, okleveles közgazdász és jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola katonai műszaki tudományok keretein belül PhD tanulmányait végzi, ahol 2019 óta előadásokat is tart, szakterülete a pszichológiai manipuláció és a geopolitika, a kibertéri tevékenységekhez kapcsolódóan. Kutatásai során a kommunikációs csatornák működését és azok alkalmazásának trendjeit vizsgálja, amelyek hatása szoros kapcsolatban áll a geopolitikai folyamatokban bekövetkező változásokkal, ilyen például a közösségi média megkerülhetetlen szerepe, valamint a katonai tevékenységekről szóló témák megjelenése a napi tájékoztatásban. Írásaiban több alkalommal kerül fókuszba az emberi tényező vizsgálata, mint a rendszerek sebezhető pontja, amely nemcsak az információbiztonságban fontos, hanem a társadalmi folyamatok elemzése során is. Szerzője egy fejezetnek, amely A dezinformáció elleni háború: A bizalom szerkezete címmel szerepel a Kézikönyv a kortárs információs környezet megértéséhez című kiadványban.

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

LEISZTNER PÉTER

leisztner.peter@uni-obuda.hu

My name is Péter LEISZTNER, Certified Environmental Engineer, Occupational Safety Engineer, Factory Mechanic Plant Engineer, student of the Doctoral School on Safety Sciences at Obuda University. I have been dealing with occupational safety for more than ten years, primarily in the micro and SME sector, where I consider it my mission to create businesses built around safety. My research area is occupational safety and health advocacy, measuring the performance of occupational safety and health representatives, defining their tasks and roles in the occupational safety and health organization of enterprises, as well as measuring the occupational health and safety knowledge level of employees and exploring their development opportunities. It is an honor for me to be able to participate in the educational activities of the University of Óbuda during trainings related to occupational safety and health preservation. I am proud to be able to contribute to the work of dissertation students as an institute (internal) consultant.

LEISZTNER Péter vagyok, Okleveles Környezetmérnök, Munkavédelmi Szakmérnök, Gyárszerelő Üzemmérnök, az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának hallgatója. Több, mint tíz éve foglalkozom munkabiztonsággal, elsősorban a mikro, illetve a KKV szektorban, ahol küldetésemnek tekintem a biztonság köré épülő vállalkozások kialakítását. Kutatási területem a munkavédelmi érdekképviselők, a munkavédelmi képviselők teljesítménymérése, feladataik és szerepük meghatározása a vállalkozások munkavédelmi szervezetében, valamint a munkavállalók munkavédelmi tudásszintjének mérése, és fejlesztési lehetőségeinek feltárása. Megtiszteltetés számomra, hogy részt vehetek az Óbudai Egyetem oktatási tevékenységében a munkabiztonsággal és az egészségmegőrzéssel kapcsolatos képzések során. Büszke vagyok, hogy intézeti (belső) konzulensként szakdolgozók munkájában működhetek közre.

NAGY-MEZEI Csenge

pribelszkycs@fcsm.hu

I have been working at Budapest Sewage Works Pte Ltd. since 2020, including as a process engineer at the South-pest Wastewater Treatment Plant. During my work, my main tasks are monitoring and supporting the operation of the wastewater treatment plant, optimizing and developing the technology, active participation in research and development projects. Since September 2022, I have been a PhD student at the Doctoral School of Environmental Sciences of the Hungarian University of Agriculture and Life Sciences, my research area is improving the placement of dewatered sewage sludge produced in municipal wastewater treatment plants.

2020 óta dolgozom a Fővárosi Csatornázási Művek Zrt-nél, azon belül a Dél-pesti Szennyvíztisztító Telepen technológus mérnökként. Munkám során fő feladataim a szennyvíztisztító telep üzemszerű működésének ellenőrzése, támogatása, a technológia optimalizálása, fejlesztése, kutatás-fejlesztési projekteken való aktív részvétel. 2022. szeptember óta a Magyar Agrár- és Élettudományi Egyetem Környezettudományi Doktori Iskolájának PhD-hallgatója vagyok, kutatási területem a kommunális szennyvíztisztító telepeken keletkező víztelenített szennyvíziszap elhelyezhetőségének javítása.

NÉMETH Antal

nemeth.antal@uni-obuda.hu

Antal NÉMETH (1975) is a qualified historian and teacher of Russian and a university expert in human resources management. He is currently the managing director of the Kaposvár Science and Innovation Park Nonprofit Ltd., a majority-owned subsidiary of Óbuda University, and a first-year PhD student at the University of Óbuda's Doctoral School of Security

NÉMETH Antal (1975) okleveles történész és orosz szakos tanár, valamint humánmenedzser egyetemi szakértői szakképzettséggel rendelkezik. Jelenleg az Óbudai Egyetem többségi tulajdonában lévő Kaposvári Tudományos és Innovációs Park Nonprofit Kft. ügyvezetője, valamint Óbudai Egyetem Biztonságtudományi Doktori Iskolájának első éves PhD hallga-

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

Sciences. Research interests: history of tank development, impact of robotics on tank development.

tója. Kutatási területe: a harckocsik fejlődéstörténetének vizsgálata, a robotika hatása a harckocsik fejlődésére.

ÓSZI Arnold

oszi.arnold@bgk.uni-obuda.hu

Dr. ÓSZI Arnold is a Safety Engineer, Assistant Professor at Óbuda University. As a supervisor in the Doctoral School on Safety and Security Sciences, he supervises several students and teaches subjects to other PhD students in the Doctoral School. His scientific research areas are security, IT, biometric identification, UAV-s, and the movement of crowds. He has been teaching at Óbuda University since 2008. He is currently a teacher in the following courses: Safety Engineer BSc and MSC, Occupational Safety Engineer, Information Security Engineer. Main subjects taught by him: Risk analysis, Case study, Biometric identification, Vehicle protection systems, Physical protection systems, Protection, Weapon knowledge. He teaches subjects in both Hungarian and English at the University. So far, he has been the thesis supervisor of more than 100 students. He has participated in many projects and professional work related to security technology.

Dr. ÓSZI Arnold oklevelesbiztonság-technikai mérnök, az Óbudai Egyetem Adjunktusa. A Biztonságtudományi Doktori Iskolában témavezettként több hallgatót vezet, más PhD hallgatóknak pedig tárgyakat oktat a Doktori Iskolában. Tudományos kutatási területe a biztonság, IT, biometrikus azonosítás, drónok, embertömegek mozgása. Az Óbudai Egyetemen 2008 óta oktat. Jelenleg a következő szakokon oktató: Biztonságtechnikai mérnök BSc és MSC, Munkavédelmi szakmérnök, Információbiztonsági szakmérnök. Főbb, általa oktatott tantárgyak: Kockázatelemzés, Esettanulmány, Biometrikus azonosítás, Gépjármű védelmi rendszerek, Fizikai védelmi rendszerek, Őrzésvédelem, Fegyverismeret. A tantárgyakat magyar és angol nyelven is oktatja az Egyetemen. Eddig több mint 100 hallgatónak volt szakdolgozat témavezetője. Számos biztonságtechnikával kapcsolatos projektben és szakmai munkában vett részt.

PÁL Anita Brigitta

pal.anita@hm.gov.hu

In the past 15 years, I represented law firms, economic companies and commercial companies as an English and German Consecutive Interpreter in various projects. In terms of my studies, I started with law, but since my goal was to find a position in the diplomatic environment, I rather obtained my first diploma as a Specialist in Foreign Affairs and International Relations. After that, I completed my master's degree at the Faculty of Military Science and Defense Officer Training of the National Public Service University as an Expert in International Security and Defense Policy. I would like to deepen my knowledge in the strategic planning of security and defense systems and the effective operation of their organizations as well as in optimizing the possibilities between the defense organizations and institutions, that play a role in central and local defense administration. I am serving with my knowledge the International Directorate of the Defense Economics Bureau of the Ministry of National Defense as a soldier. As a PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University, I research the impact of artificial intelligence on civil and military security.

Az elmúlt 15 évben ügyvédi irodák, gazdasági cégek és kereskedelmi vállalatok angol és német nyelvű képviselőjét láttam el különböző projekteken belül. Tanulmányaimat tekintve először jogot tanultam, majd diplomát szereztem nemzetközi tanulmányokon, lévén, hogy célom a diplomáciai környezetben való elhelyezkedés volt. Ezt követően a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának mesterképzésén végeztem nemzetközi biztonság- és védelempolitikai szakértőként. Tudásomat szeretném elmélyíteni a védelmi szervezetek, a központi és a helyi védelmi közigazgatásban szerepet játszó intézmények optimalizálásának lehetőségében, illetve a biztonsági és védelmi rendszerek stratégiai tervezésében és szervezeteinek hatékony működtetésében. Tudásommal a Honvédelmi Minisztérium Védelemgazdasági Hivatal Nemzetközi Igazgatóságát szolgálom katonaként. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktoranduszaként a mesterséges intelligencia hatását kutatom a polgári és katonai biztonságra.

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

PAUKÓ Andrea

andrea.pauko@bgk.uni-obuda.hu

Dr. Andrea PAUKÓ, assistant professor of the Institute of Natural Sciences and Basic Subjects of the Donát Bánki Faculty of Mechanical and Safety Engineering at the University of Óbuda, lecturer of the Institute's Safety Engineering course Energy Safety, Environmental Protection. He prepared his doctoral dissertation in the framework of the Wood Science (F1) program of the József Cziráki Doctoral School of Wood Science and Technology of the University of West Hungary on a comparative study of the wood quality of Spruce and Scots pine plantations. He is an employee of the university's Biogas research laboratory.

Dr. PAUKÓ Andrea, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Természettudományi és Alapozó Tantárgyi Intézetadjunktusa, az Intézet Biztonságtechnikai mérnök képzés Energiabiztonság, Környezetvédelem tantárgy oktatója. Doktori disszertációját a Nyugat-Magyarországi Egyetem Cziráki József Faanyagtudomány és Technológiák Doktori Iskolája Faanyagtudomány (F1) programja keretében a Lucfenyő és erdeifenyő ültetvények faanyagminőségének összehasonlító vizsgálatából készítette. Az egyetem Biogáz kutató laboratóriumának munkatársa.

RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Zoltán RAJNAI (1962) engineer colonel, dean of the Óbuda University, Donát Bánki Faculty of Mechanical and Security Engineering, operating manager of the Doctoral School of Security Sciences of the University, cyber coordinator of Hungary. He completed his military studies at the Máté Zalka Military Technical College and then at the Miklós Zrínyi Military Academy. From 1993 he worked as a university adjunct at the Miklós Zrínyi Military Academy and the Miklós Zrínyi National Defense University, the predecessor institutions of the University of Public Service. Under its leadership the Telecommunication Department at NKE was established in 2008 by merging the Faculties of Telecommunication of the János Bolyai Faculty of Military Engineering and the National Defense University. He received his doctorate in 2001 and his habilitation in 2006. He won a research scholarship named after János Bolyai of the Hungarian Academy of Sciences. Between 2007 and 2011 he was the Hungarian program director of the COMMIT French-Hungarian International Science (R & D & I) project, and at the same time a guest lecturer in France at the Military Technical College in Rennes. He is the president of the Puskás Tivadar Telecommunication Comrades Association since 2012. His research interests include security of communication networks in qualified periods, protection of critical infrastructure, information security.

RAJNAI Zoltán (1962) mérnök ezredes, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar dékánja, az Egyetem Biztonságtudományi Doktori Iskolája operatív vezetője, Magyarország kiberkoordinátora. Katonai tanulmányait a Zalka Máté Katonai Műszaki Főiskolán, majd a Zrínyi Miklós Katonai Akadémián végezte. 1993-tól a Zrínyi Miklós Katonai Akadémián, illetve a Zrínyi Miklós Nemzetvédelmi Egyetemen, a Nemzeti Közszolgálati Egyetem jogelőd intézményeiben dolgozott egyetemi oktatóként. A vezetésével alakult meg 2008-ban a Bolyai János Katonai Műszaki Kar és a Nemzetvédelmi Egyetem Híradó tanszékeinek összevonásával az NKE-n ma is működő híradó tanszék. 2001-ben doktori fokozatot, 2006-ban habilitációt szerzett. Elnyerte a Magyar Tudományos Akadémia Bolyai Jánosról elnevezett kutatási ösztöndíját. 2007 és 2011 között a COMMIT francia-magyar nemzetközi tudományos (K+F+I) projekt magyarországi programigazgatója volt, ezzel párhuzamosan vendég-oktató Franciaországban a Rennes-i Katonai Műszaki Főiskolán. 2012-től a Puskás Tivadar Híradó Bajtársi Egyesület elnöke. Kutatási területei: minősített idő-szakok kommunikációs hálózatainak biztonsága, kritikus infrastruktúra védelme, információbiztonság.

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

RÉKÁSI Márk

rekasi.mark@atk.hu

Márk RÉKÁSI is a senior research fellow of the Institute for Soil Sciences, Centre for Agricultural Research. After finishing his investigations in the topic of acid-base buffering capacity of soils, he has been working on the field of potentially toxic elements mobility in soil-plant system and the utilisation of waste materials in agriculture since 2005. During these works he took part in the evaluation of the institute's trace element contamination field experiments and investigated the fertiliser and soil amendment value of different sewage sludges and combustion waste materials. He has 69 scientific publications so far.

RÉKÁSI Márk az Agrártudományi Kutatóközpont Talajtani Intézetének tudományos főmunkatársa. A talajok sav-bázis pufferképességének vizsgálatát követően, 2005. óta foglalkozik a potenciálisan toxikus elemek mobilitásával a talaj-növény rendszerben, illetve hulladékok mezőgazdasági hasznosíthatóságának kérdésével. Ezen munkák során részt vett az intézet szabadföldi nyomelem-szennyezési kísérleteinek értékelésében, különböző szennyvíziszapok, égéstermékek trágyahatásának, potenciális talajjavító értékének vizsgálatában. Eddig összesen 69 tudományos közleménye jelent meg.

SÁNDOR Barnabás

sandor.barnabas@gmail.com

Barnabás SÁNDOR is a security engineer and cybersecurity researcher. He currently holds the position of Cyber Security Architect at MOL Group. He has more than ten years of experience in IT design, operation, and security. His main area of expertise is cybersecurity, where he is involved in the design and vulnerability assessment of IoT devices, software, and system platforms. His main research area is cyber security for smart buildings. The experience and knowledge gained over the years have led to continuous development being of utmost importance to him, which is why he is currently a Ph.D. candidate at the Doctoral School of Security Sciences at Óbuda University. Since 2018, he has also been an external lecturer at the university. Furthermore, he regularly participates in national and international conferences and is constantly invited by the media on professional issues.

SÁNDOR Barnabás okleveles biztonságtechnikai mérnök és kiberbiztonsági kutató. Jelenleg a MOL-csoportnál Cyber Security Architect pozíciót tölt be. Az informatika területén több, mint 10 éves tervezői és üzemeltetői és biztonsági tapasztalattal rendelkezik. Fő szakterülete a kiberbiztonság, ahol az IoT eszközök, szoftverek és rendszerterek tervezésében és sérülékenység-vizsgálatában vesz részt. Fő kutatási területe az intelligens épületek kiberbiztonsága. Az évről évre megszerzett tapasztalat és tudás vezetett oda, hogy kiemelten fontos számomra a folyamatos fejlődés, éppen ezért jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában doktorjelölt. Mellette 2018 óta külsős óraadó az egyetemen. Folyamatosan vesz részt hazai és nemzetközi konferenciákon, illetve szakmai kérdésekben folyamatos felkéréseket kap a médiában.

SZÉCSY Orsolya

szecsy.orsolya@atk.hu

Orsolya SZÉCSY is a research associate at the Institute for Soil Sciences, Centre for Agricultural Research. She graduated from university as environmental engineer and as English-Hungarian specialist translator. Before defending her PhD dissertation in 2017, she completed a soil protection professional postgraduate training. In her dissertation she evaluated the effects of fertilisation on the potentially toxic element content and also the enzyme activity of the soil. Since then she has been studying the aspects of agricultural application of organic wastes, especially sewage sludges and working in ecotoxicological testing.

SZÉCSY Orsolya tudományos munkatárs az Agrártudományi Kutatóközpont Talajtani Intézetében. Okleveles környezetmérnök, angol-magyar szakfordító és talajvédelmi szakelőadó. Doktori disszertációjában, amit 2017-ben védett meg, a műtrágyázás hatásait vizsgálta a talaj potenciálisan toxikus elemtartalmára, valamint az enzimaktivitásra. Ezt követően különböző szerves hulladékok, elsősorban szennyvíziszapok mezőgazdasági hasznosíthatóságát tanulmányozza, illetve ezekkel összefüggésben ökotoxikológiai vizsgálatokkal foglalkozik.

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

SZÜCS Endre

szucs.endre@bgk.uni-obuda.hu

Dr. Endre Szűcs (1963), PhD in military sciences, certified engineer of Safety and Security Sciences, Mechanical Engineer, Senior Lecturer. At present leading lecturer at Óbuda University Doctoral School of Safety and Security Sciences, teaching review and analysis of history of security techniques. Also teaching at Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering. Field of research is the possible application of renewable energy sources in security techniques and the research in history of security techniques.

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

ZAGYVAI Péter

zagyvai.peter@ek-cer.hu

Péter ZAGYVAI graduated as a chemical engineer at Budapest University of Technology (BME) in 1976. He was engaged in radioanalysis already when working on his diploma thesis, and has remained in this area of expertise ever since. Between 1990 and 2010, he was the head of the Radiation Protection Department of the training reactor of the Institute of Nuclear Techniques at BME. In 2010, he accepted a full-time job at the Centre for Energy Research. He is a senior research associate of the Environmental Physics Laboratory. He retired in 2021, but still he holds the position of the radiation protection officer of the campus. As a part-time job he gives lectures in BSc and MSc subjects at the Faculties of Natural Sciences, Mechanical Engineering and Chemical Technology and Biotechnology. In addition, he supports the work of the ELI ALPS Laser Centre at Szeged, and occasionally he contributed, as a course lecturer or consultant, to the working units of the International Atomic Energy Agency (IAEA) involved in emergency management and response, and the decommissioning of facilities.

ZAGYVAI Péter vagyok, okleveles vegyészmérnökként végeztem 1976-ban a Budapesti Műszaki Egyetemen (BME). Már a diplomázás alatt is radioanalitikával foglalkoztam, és utána is ezen a tudományterületen maradtam. 1990-től 2010-ig a BME Nukleáris Technikai Intézetéhez tartozó oktatóreaktor sugárvédelmi vezetője voltam, 2010-től fő munkahelyem a jelenlegi Energiatudományi Kutatóközpont. A Környezetfizikai Laboratórium tudományos főmunkatársaként dolgozom, 2021 óta nyugdíjasként, emellett ellátom a telephelyi sugárvédelmi megbízott feladatait. Másodállásban megmaradtam a BME-n, a Természettudományi Kar, a Gépészmérnöki és Energetikai Kar, valamint a Vegyész- és Biomérnöki Kar BSc és MSc képzésein tartok előadásokat. Ezek mellett sugárvédelmi szakértőként segítem a szegedi ELI ALPS lézerközpont munkáját, és alkalmanként tanfolyami előadóként és konzulensként részt vettem az International Atomic Energy Agency (IAEA) bal- eset-elhárítással és létesítmények leszerelésével foglalkozó munkacsoportjaiban.

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

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 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.

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 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 szójának 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. Kifejezőmódja 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 5, No 2, 2023. | 2023. V. évf. 2. szám

CONTENT | TARTALOM

Philosophy and History of the Safety and Security column	Biztonságfilozófia és -történet rovat
---	--

NÉMETH Antal – SZÚCS Endre

History of the development of autonomous land combat vehicles (part 1.) <i>1-10</i>	Autonóm szárazföldi harcjárművek alkalmazásának fejlődéstörténete (1. rész)
--	---

Security Policy column	Biztonságpolitika rovat
-------------------------------	--------------------------------

BAUMGARTNER Helga – ŐSZI Arnold

Overview of the main resolutions of the United Nations in countering terrorism <i>11-20</i>	Az Egyesült Nemzetek Szervezete főbb határozatainak áttekintése a terrorizmus elleni védekezésben
--	---

PÁL Anita Brigitta

The complex connection of warfare, terrorism and the use of drones <i>21-32</i>	A hadviselés, terrorizmus és drónhasználat komplex kapcsolata
--	---

Domotics column	Domotika rovat
------------------------	-----------------------

SÁNDOR Barnabás – RAJNAI Zoltán

Smart Buildings and IoT: A Comprehensive Review of Global Practices <i>33-46</i>	Okos épületek és az IoT: A globális gyakorlatok átfogó áttekintése
---	--

Information Security column	Információbiztonság rovat
------------------------------------	----------------------------------

HEGYI Henrietta

Information Security of Passenger Vehicles from the Perspective of Information Security Experts <i>47-58</i>	A személygépjárművek információbiztonsága az információbiztonsági szakértők szemszögéből
---	--

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

Industrial and Operational Safety column	Ipar- és üzembiztonság rovat
---	-------------------------------------

BAKOSNÉ DIÓSZEGI Mónika – RÉKÁSI Márk – SZÉCSY Orsolya – BEZSENYI Anikó – NAGY-MEZEI Csenge – PAUKÓ Andrea

Effect of microwave pretreatment on biogas production during anaerobic digestion in a model experiment	Mikrohullámú előkezelés hatása a biogázhozamra szennyvíziszap anaerob rothasztása során modellkísérletben
59-67	

BODOR Károly – ZAGYVAI Péter

Investigation of ablation decontamination technology generated by laser light	Lézerfény által generált ablációs dekontaminálási technológia vizsgálata
69-82	

DÉR Attila Tibor

Determination of threats to the world's energy supply through the concept and objectives of infocommunication strategies	A világ energiaellátása veszélyeinek meghatározása infokommunikációs stratégiák fogalmán és céljain keresztül
83-92	

EDELMANN Dóra

Terminology of emergency mass movements	A vészhelyzeti tömegmozgások terminológiája
93-106	

ELEK Barbara – BODNÁR László – HORVÁTH-KÁLMÁN Eszter

Risk analysis of the reservoir of a mining waste management facility	Bányászati hulladékkezelő létesítmény tározójának kockázatelemzése
107-121	

HORVÁTH-KÁLMÁN Eszter – ELEK Barbara – KOVÁCS-SZELECZKI Xénia

Fire safety issues of thermoforming technology	Melegalakítási technológia tűzbiztonsági kérdései
123-135	

Safety and Security in General column	Munkabiztonság rovat
--	-----------------------------

LEISZTNER Péter

The role of occupational safety and health representatives in performing occupational safety and health duties	A munkavédelmi képviselők szerepe a munkavédelmi feladatok ellátásában
137-147	

Book Review column	Könyvismertetés rovat
---------------------------	------------------------------

KOLLÁR Csaba

Review about the book Peter Norvig and Stuart J. Russell: Artificial Intelligence A Modern Approach	Recenzió Peter Norvig és Stuart J. Russell Mesterséges intelligencia modern megközelítésben című könyvéről
149-155	

KUN Tamás

Review about the book Conflict and Peace in Western Sahara by János Besenyő	Recenzió Besenyő János: Konfliktus és béke a Nyugat-Szaharában című könyvéről
157-160	

**HISTORY OF THE
DEVELOPMENT OF AUTONOMOUS
LAND COMBAT VEHICLES (PART 1.)****AUTONÓM SZÁRAZFÖLDI
HARCJÁRMŰVEK ALKALMAZÁSÁNAK
FEJLŐDÉSTÖRTÉNETE (1. RÉSZ)**NÉMETH Antal¹ – SZÚCS Endre²**Abstract**

Over the last three decades, progressive changes in information and communication technologies have made it possible to partially or even fully automate the targeted movement of various vehicles in changing terrain, weather and environmental conditions. The aim of our research is to describe the objectives that have determined the direction of development, and the stages of advancement that have led to the current autonomous, multi-purpose combat vehicles. This article describes the early development phase and provides a review of the development history and achievements of autonomous military vehicles.

Keywords

autonomous vehicle, Unmanned Ground Vehicle (UGV), land-based torpedo, improvised explosive device, crawler chassis

Absztrakt

Az elmúlt három évtizedben az informatika és a kommunikációs technológiák ugrásszerű fejlődésének köszönhetően elérhetővé vált a különböző járművek célzott közlekedésének változó terep-, időjárás- és környezeti viszonyok közötti részleges vagy akár teljes automatizáltsága. Kutatásunk célja bemutatni, milyen célok határozták meg a fejlesztések irányát, milyen fejlődési szakaszokon keresztül jutottunk el a jelenlegi autonóm, többcélú harcjárművekig. Jelen cikk a fejlesztések korai szakaszát mutatja be, és áttekinti az autonóm katonai járművek fejlesztési előzményeit, eredményeit.

Kulcsszavak

autonóm jármű, vezető nélküli szárazföldi jármű (UGV), szárazföldi torpedó, önjáró robbanótöltet, lánctalpas futómű

¹ nemeth.antal@uni-obuda.hu | ORCID: 0009-0002-5404-9435 | managing director, Kaposvár Science and Innovation Park Nonprofit Ltd. | ügyvezető, Kaposvári Tudományos és Innovációs Park Nonprofit Kft.

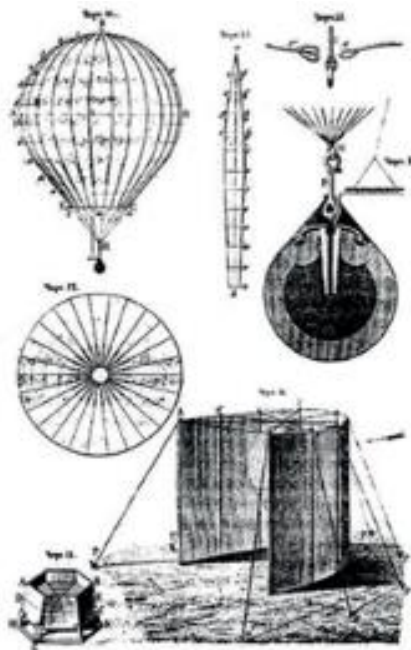
² szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X | senior lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary

BEVEZETÉS

Az elmúlt két évtizedben exponenciális növekedés volt tapasztalható a pilóta nélküli eszközök területén. Ezen járművek katonai alkalmazásától elsősorban az élőerő veszteségeinek csökkenését várják el a különböző katonai műveletek során [1]. A katonai drónok örökre megváltoztatták a háború lefolyását, folyamatos megfigyelést, fokozott irányítást, valamint precíziós csapásmérő képességeket biztosítva, míg a földi robotok életmentő szerepet játszanak a taposóaknak és a rögtönzött robbanószerkezetek semlegesítésében. A polgári oldalon az önvezető autók, teherautók, buszok nem vágyálmok, már a zsúfolt utakon keverednek a személyzettel ellátott járművekkel. Autonóm anyagmozgató robotok ezrei dolgoznak éjjel-nappal, és több millió terméket hoznak be az internetes kereskedelemmel foglalkozó multinacionális nagyvállalatok hatalmas raktáraiba, a légi és utcai szintű drónokat már tesztelik házhozzállítási céllal. Az elmúlt időszak háborúiban már nem csak speciális hadműveletekben alkalmazzák, hanem folyamatos a pilóta nélküli drónok jelenléte: a 2020-as hegyi-karabahi háborúban vagy a jelenleg is zajló orosz-ukrán háborúban már befolyásoló tényező a harcsteren. A felderítő hadműveletekben és az ellenséges haditechnika és élő erő megsemmisítésében vagy a harcból való kivonásukban meghatározó szerepet játszanak. Hosszú út vezetett idáig. Célunk, hogy bemutassuk a folyamatot – második ipari forradalomtól az első világháború végéig – az autonóm harcjárművek egy speciális szegmensének, a szárazföldi autonóm harcjárművek fejlesztésének az előzményeit és első fejlesztési szakaszát, eredményeit.

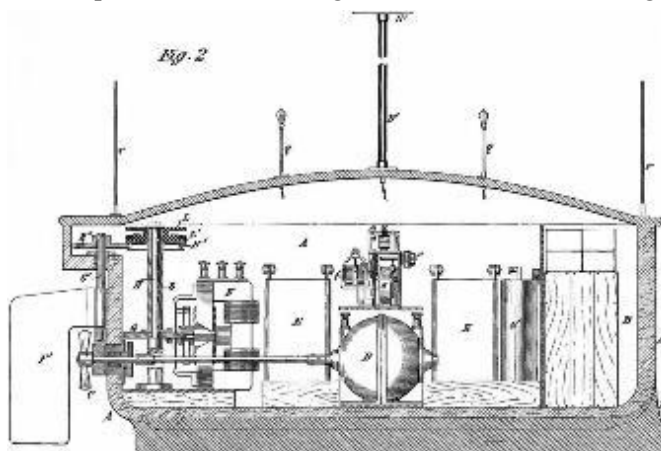
A KEZDETEK: FÖLDÖN, VÍZEN, LEVEGŐBEN

A közhiedelemmel ellentétben a robotok és drónok iránti érdeklődés jóval korábbra nyúlik vissza, mint hogy azt a legtöbb ember gondolná, mivel több mint egy évszázada alkalmazunk pilóta nélküli katonai rendszereket. Az egyik legkorábbi kísérlet 1849. augusztus 22-én történt, amit Velence szenvedett el az első pilóta nélküli légi járművek által. A ballonokról végrehajtott légitámadást Ausztria vetette be 1849-es ostroma során Velencében a függetlenségi háború alatt. Bombákat csatoltak pilóta nélküli léggömbökhöz és hagyták, hogy a szél azokat Velence fölé fújja. Sajnos az időzítő technikai megoldásáról és magáról a léggömbről nem maradtak fenn pontos információk. Annyit tudunk, hogy hajóról indították a becslések szerint 200 léggömböt 1849. augusztus 22-én, amelyek mindegyike több mint 14 kg robbanóanyagot szállított. Néhány ballon elérte a célját, de katonai értelemben a károk minimálisak voltak, viszont a pszichológiai hatás annál nagyobb volt. Vélhetően ez volt az a pillanat, amikor egy *„új háborús filozófia egy új dimenziót nyitott a reguláris hadseregek közötti harcérintkezésben, mert felvetette annak a lehetőségét, hogy a polgári lakosság jóval a hadseregek elülső vonala mögött a támadás célpontjává váljon. Ezzel a háborús fogalmakhoz hozzá lehetett adni egy új szót, a „légitámadás” kifejezést.”* [2]



1.Ábra: A bombával ellátott léggömb feltételezett kinézete. (forrás: <https://www.italyonthisday.com/2017/08/historys-first-air-raid-Venice-Republic-of-San-Marco-Austria.html>)

Az 1860-as évek önműködő torpedó fejlesztései mellett, amelyek már katonai alkalmazásba is kerültek (pl. 1864. Giovanni Luppis-Robert Whitehead: Minenschiff), megjelentek az első elektromos meghajtású, de vezetékes távirányítású járművek (unmanned surface vehicles, a továbbiakban: USV), az autonóm vízfelszíni járművek. Az első rádióvezérelt USV-t Nikola Tesla fejlesztette ki 1897-ben[3] és a rá következő évben mutatta be a Madison Square Gardenben megrendezett elektrotechnológiai kiállításon.

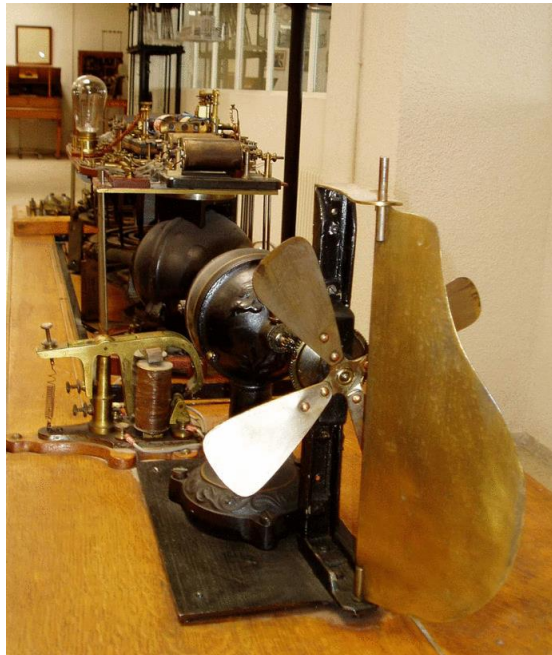


2. Ábra: Tesla rádióvezérelt hajója, amely körülbelül 1,2 m hosszú és 0,9 m magas, egy sor E tárolóelemet alkalmazott a D hajtómotor és az F kormánymotor meghajtására (a 613,809 XNUMX amerikai szabadalomtól adaptálva). forrás: <https://mechanixillustrated.technicacuriosa.com/2017/02/19/a-brief-early-history-of-unmanned-systems/>

Nikola Teslával szinte egy időben egy spanyol tudós és feltaláló Leonardo Torres-Quevedo is áttörést ért el a távirányítású járművek területén. Ennek háttérében az emberi élet megóvása volt a pilóta nélküli kísérleti légi járművek tesztelése során. 1903-ban mutatta be a Párizsi Tudományos Akadémián a Telekinót, amelyet Franciaországban, Nagy-Britanniában, Spanyolországban és az Egyesült Államokban is szabadalmaztatott. A találmány egy távvezérlő rendszer volt, amelyhez két dologra volt szükség: egy adóra, amely rádióhullámok (Hertz-hullámok) segítségével képes volt különböző bináris kódszavakat küldeni, és egy vevőre, amely a kódszó függvényében képes volt az irányított eszközben különböző működési állapotot beállítani és ezáltal különböző manővereket tudott végrehajtani az adot jármű, legyen az vízben, földön vagy levegőben. Leonardo Torres-Quevedo a találmányát Telekinónak nevezte el.

Két szót összekapcsolásával alkotta meg a Telekinót. A szó a görögből származik: tele (messze, távol) és kino (mozgás), aminek eredménye a "távolban történő mozgás". Torres-Quevedo a szabadalmának leírásában így írt a Telekinóról:

„A találmány lényegében egy távirányítású, vezetékekkel vagy anélkül működő, a tű helyzetét meghatározó távirójelet tartalmaz, amely egy 'szervomotort' (vezérlő, kapcsoló vagy motor) szabályoz, amely bármilyen készüléket működtet”. [4]



3.Ábra: A Telekinó prototípusa. Universidad Politécnica de Madrid, Spanyolország, forrás: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4399975>

A Telekinó elektromos meghajtású hajókra történő alkalmazásával Torres-Quevedo képes volt arra, hogy a kormánymotor különböző pozícióit és a hajtómotor különböző sebességeit egymástól függetlenül válassza ki. Egyidejűleg képes volt más mechanizmusokat is működtetni, mint például a világítás fel- és lekapcsolása, valamint a zászló fel- és leengedése. Összességében akár 19 különböző műveletre is képes volt prototípusaival. Torres-Quevedo 1904-ben megépített egy háromkerekű elektromos

meghajtású kísérleti autót, amelyet rádióval irányított, amely képes volt előre vagy hátrafelé menni, illetve jobbra vagy balra fordulni. Ennek hatótávolsága mindössze 20-30 méter volt, és úgy tűnik, az ez volt az első ismert példánya a rádióvezérlésű pilóta nélküli földi járműnek (UGV). A további fejlesztések eredményeképpen 1905. november 7-én a bilbaói öbölben egy hajóval sikerült a 2 km irányítási hatótávolságot is elérni. Sajnálatos módon a további kísérletek – mivel a spanyol királyi haditengerészet nem finanszírozta tovább a fejlesztéseket, – megszakadtak. A további fejlesztések és gyakorlati katonai alkalmazások a földi területen csak az első világháborúban jelentek meg, viszont a rádióvezérelt szárazföldi járművek fejlesztése esetében ez közvetlenül a második világháború előtt vesz újra lendületet.

AZ ELSŐ PILÓTA NÉLKÜLI HARCJÁRMŰVEK: TORPEDÓK A SZÁRAZFÖLDÖN

Az első ilyen jellegű, legalábbis tesztelésig jutott projektek, amelyeket az első világháború lövészárkainak pusztító patthelyzete ösztönzött, Franciaországban jelentek meg és a haditengerészet által a korábban már kifejlesztett víz alatti önműködő torpedók analógiáján szárazföldi vagy elektromos torpedónak nevezték el. Ezen eszközöket önjáró robbanótölteteknek is nevezhetjük.

Aubriot-Gabet elektromos torpedója (Aubriot-Gabet Torpille Electrique)



4. Ábra: Aubriot-Gabet Torpille Electrique kísérleti modell, forrás: <https://en.topwar.ru/123927-suhoputnaya-torpeda-aubriot-gabet-torpille-electrique-franciya.html>

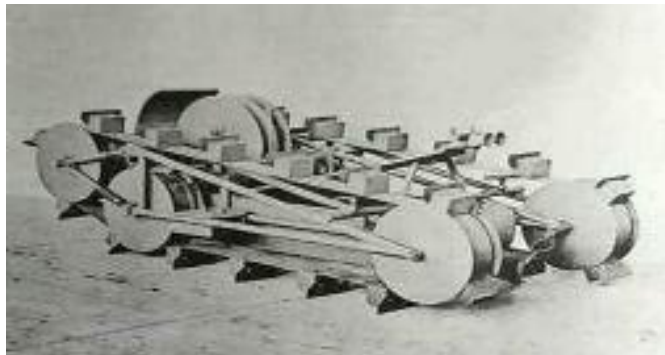
A modellt 1915-ben tervezte meg Paul Aubrio és Gustave Gabe mérnökpáros. Pontos technikai paraméterek nem maradtak fenn, de a leírások alapján egy 1,5 m-t nem meghaladó, kb. 50 cm magas és 200 kg összsúlyú járművet jelentett elektromos motorral és lánctalpas meghajtással. Robbanótöltetek hordozására tervezték (kb. 30-50 kg), amelynek célja az ellenséges létesítmények vagy akadályok megsemmisítése. A járművet a platform hátsó részén elhelyezkedő elektromos motorral hajtották meg, amely tengelyen keresztül forgatta meg a fogaskerékre erősített lánctalpat. A jármű nem volt kormányozható, csak előre és hátra tudott mozogni, ezért indításkor kellett a cél felé irányítani, utólag már nem tudott irányt változtatni. Az elektromos motor áramot vezetéken keresztül kapott, mint ahogy az irányítás és a töltet aktiválása is ezen a vezetéken keresztül történt. A jármű elején

látható harmadik lánctalp vélhetően a harcmezőn lévő drótkadályok leküzdésére szolgált. A járműnek az Aubriot-Gabet Torpille Electrique nevet adták[5]. A jármű nem volt harci alkalmazásban, egy kísérleti példány készült.

Méreték (becsült)	Meghajtás	Irányítás módja/Hatótáv	Összsúly/Hasznos teher	Védelem	Fegyverzet
1500-1700x400-500x400-500 mm	elektromos motor	vezetékes/nem ismert	200 kg/kb. 30-50 kg	nincs	robbanótöltet

1. Táblázat: Aubriot-Gabet elektromos torpedó technikai adatok. forrás: <https://dzen.ru/a/X70Od9garxgbBDyh>

Schneider “Krokodil” szárazföldi torpedó (Torpille Terrestre Schneider Crocodile typ A/B)



5. Ábra: Torpille Terrestre Schneider Crocodile typ A, forrás: <https://dzen.ru/a/X70MGwtK-AFJsh1m>



6. Ábra: Torpille Terrestre Schneider Crocodile typ B, forrás: <https://dzen.ru/a/X70MGwtK-AFJsh1m>

Az Aubriot-Gabet mérnökpárossal szinte egyidőben (1915) indult Schneider-Creusot haditechnikai cég önjáró robbanótöltet projektje. A leendő szárazföldi torpedó a Schne-

ider Crocodile projektnevet kapta [6]. A súlycsökkentés érdekében a Schneidernél a leg-egyszerűbb megoldást, egy egyszerű csővázszerkezetet választottak (5. ábra). A vázon az akkumulátorok, egy pár villanymotor és egy orsó volt a vezérlőhuzal számára. A motorokat vezetéken keresztül lehetett vezérelni. Minden elektromos részt vízzáró réteggel burkoltak, hogy képes legyen vizes akadályokat is leküzdeni. A meghajtás egyszerű volt, egy vezető és két támasztó görgő segítségével valósult meg. A hátsó támasztógörgő vezetőkerékként működött. Minden görgő egyforma kialakítású volt. A görgőkre egy vászonszíjat feszítettek, melyre fakockákat erősítettek, ezzel biztosítva a talajon való kapaszkodást.

A szerkezeti vázba 40 kg-os robbantöltet került, amelyet elektromos detonátorral távolról robbantottak. A kezelő egy kezdetleges elektromos távirányítóval irányította, amelyről a bal vagy jobb oldali hajtóművet ki- vagy bekapcsolhatta, ezzel tudott irányt váltani és ezen keresztül tudta a töltetet felrobbantani. A fordulást az egyik görgőfelület leállításával és fékezésével lehetett elérni.

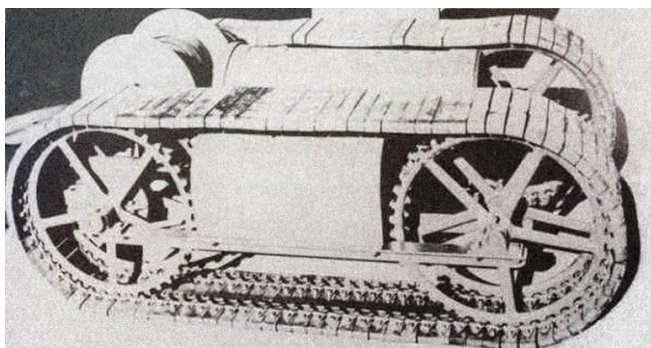
Az első tesztek sikeresek voltak. Az eredmények alapján a Schneider megváltoztatta a futóművet, a gép minden elemét továbbfejlesztette, és a továbbfejlesztett változat lett Torpille Terrestre Schneider Crocodile Typ B (6. ábra), amely gyártásba került. Az új alvázhoz egy másik, kisebb átmérőjű lánchengert adtak. A csővázat teljesen újratervezték. Maga a robbanófej a tartószerkezetbe volt beépítve. A görgőkre bordákat tettek, hogy megakadályozzák a vászonszija talp leoldását a kanyarokban. A vezeték tartalmazó orsót az eszköztől a földre helyezték a kezelő mellé.

A francia hadsereg a tesztek után 20 darabot rendelt éles bevetésre, de nincs dokumentált harci alkalmazása. 1916 után a cég a gyártást leállította, mivel a francia hadvezetés úgy döntött, hogy a sokkal ígéretesebb harcokocsik fejlesztésére és gyártására összpontosít.

Méretek (becsült)	Meghajtás	Irányítás módja/Hajtótáv	Összsúly/Hasznos teher	Védelem	Fegyverzet
1660×820×600 mm	elektromos motor	vezetékes/200 m	142 kg /40 kg	nincs	robbanótöltet

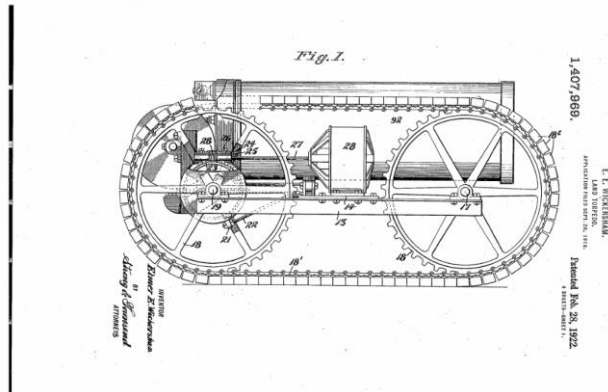
2. Táblázat: Torpille Terrestre Schneider Crocodile Type A/B technikai adatok. forrás: <https://wofind.com/2020/09/22/suxoputnaya-torpeda-francii-schneider-crocodile/>

Elmer E. Wickersham szárazföldi torpedója (Elmer E. Wickersham Land Torpedo)

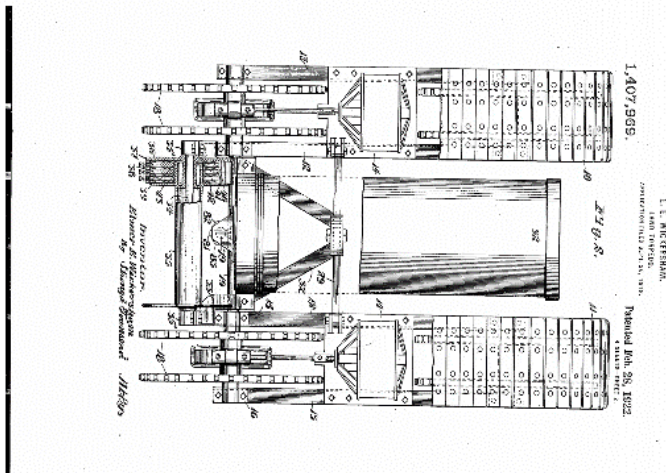


7. Ábra: Wickersham Land Torpedo, forrás: <https://warspot.ru/1632-suhoputnye-torpedy-ot-branderov-k-upravlyaemym-raketam>

A távvezérlésű, robbanótöltet hordozására alkalmas, kompakt önjáró gépek építésének ötlete Franciaországon kívül az Egyesült Államokban is felmerült, ahol hasonló konstrukcióban gondolkodtak. Az első amerikai tervezésű szárazföldi torpedót Elmer I. Wickersham tervező készítette, aki akkoriban a Holt Manufacturing Company alkalmazottja volt. A vállalat fő tevékenysége a traktorok és építőipari berendezések gyártása volt, de számos katonai projekttel is foglalkozott. Wickersham, mint a Holt cég egyik mérnöke 1917-ben kezdett el az önjáró robbanótöltet tervezésével foglalkozni. 1918-ra elkészült az a dokumentációs csomag, amely lehetővé tette a találmány bejegyzését és ez év szeptemberében a tervező szabadalmat jelentett be. Az US 1407969A számú amerikai egyesült államokbeli szabadalom 1922. február végén jelent meg.



8. Ábra: Wickersham Land Torpedo, oldalnézet, forrás: E.E. Wickersham “Land Torpedo” US Patent 1407969A, Feb.28,1922



9. Ábra: Wickersham Land Torpedo, felülnézet, forrás: E.E. Wickersham “Land Torpedo” US Patent 1407969A, Feb.28,1922

A szabadalom címe egyszerűnek és világosnak tűnt: Land Torpedo/szárazföldi torpedó. Az eredeti projekt a Wickersham Land Torpedo átfogóbb nevet kapta. Wickersham egy kompakt és viszonylag könnyű, lánctalpas elektromos jármű gyártását javasolta. A konstrukció azonos volt a francia találmányok konstrukciójával: két elektromos motor hajtotta. A generátor és a motor a felépítményen került elhelyezésre, de az áramot az irányítással együtt egy vezetéken keresztül biztosították, ami a jármű hátulján, egy dobon volt felszelve. A robbanótöltet a váz közepén, a lánctalpak között került elhelyezésre egy fém hengerben (9. ábra). A célpontok megsemmisítésére viszonylag nagy tömegű robbanótöltet alkalmazását tervezték (kb. 40 kg). A szabadalmi leírás alapján több funkciója lett volna a találmánynak:

- Fő feladata a robbanótöltet célba juttatása volt. A szükséges mennyiségű robbanóanyagot a központi hengeres testbe kellett elhelyezni. A robbanás egy távirányítású elektromos gyújtószerkezet segítségével lépett működésbe. A robbanás következtében a szerkezet is megsemmisül és a szétrepülő fém alkatrészek srapelként szolgálva fokozzák a robbanás erejét [8].
- A támadó szerep mellett logisztikai/támogató szerepet is elláthatott volna. Így a lánctalpas alvázra szerelt robbanóanyaggal ellátott hengeres test helyett egy könnyű teherplatformot is felszerelhetek volna. Ebben a konfigurációban egy távirányítású önjáró szállító eszközként lehetett volna használni lőszer vagy ellátmány szállítására [9].
- Kommunikációkiépítésre is használni lehetett volna oly módon, hogy két pont között a kábeldobra feltekert vezeték lefektetésre kerülne, így élő személyek veszélyeztetése nélkül táviró- vagy telefonösszeköttetést lehet általa kiépíteni [10].

A Wickersham torpedó fejlesztéséről és teszteredményeiről nem állnak rendelkezésre technikai adatok, sem technikai információk. Mivel a projekt meglehetősen későn – az első világháború legvégén – jelent meg, nem tudták befejezni a szükséges fejlesztési munkákat, lezárni és véglegesíteni a prototípust az európai harcok befejezése előtt. A békeszerződés aláírása után a hadseregnek már nem volt szüksége új fegyver- és felszerelési modellekre. 1922-ben ugyan szabadalmat szereztek, de ennek a dokumentumnak a megjelenése volt az egyetlen igazi sikere a projektnek. Megrendelői érdeklődés hiányában a Holt Manufacturing Company nem folytatta a további fejlesztést.

ÖSSZEGZÉS

A szárazföldi autonóm harci eszközök fejlődésének ez volt az első szakasza, amely az első világháború végéig tartott. Ezen első szakasz a felhasználásnak az elveit fektette le, illetve az irányítási lehetőségek és funkciók alapjainak a kidolgozása és tesztelése történt meg. Az első prototípusok elsődleges célja az ellenséges lövészárkok rendszer akadályainak megszüntetése és a gyalogság támadásának előkészítése, valamint a szállítási és támogató funkciók ellátása is kidolgozásra került.

A fentiek alapján összefoglalható ezen eszközök közös jellemzői: lánctalpas futómű, elektromos motormeghajtás, vezetékes irányítás, és az, hogy lényegében egy alkalommal lehetett volna őket bevetni, mivel a robbanótöltet aktiválásával önmagát is megsemmisítette volna. A vezeték nélküli irányítás ötlete már kidolgozásra került, és maga az irányítási eszköznek egy működő prototípusa is elkészült, de néhány látványos bemutatonál

nem jutott tovább. Még nem álltak össze ezek a fejlesztések egy hatékony, működő gépezetté. Ezek az eszközök magukon hordozták a prototípusok fő hátrányait, a kis motorteljesítményt és az ennek megfelelően alacsony, mindössze néhány km/h mozgási sebességet. Magának a meghajtásnak az erőforrását sem tudták ebben a méretben biztosítani, ez viszont jelentősen lekorlátozta a hatótávolságot és a sebezhetőségét is nagy mértékben növelte. A viszonylag kis méretű és alacsony építésű gépeket nagyon nehezen lehetett volna követni, különösen a csata közben, az árkokkal és bombatölcsérekkel teli terepen. Mivel semmilyen védelemmel nem rendelkeztek, ezért az ellenséges lövedékek és repeszek viszonylag könnyen megsemmisíthették volna. A hatótávolság csak néhány száz méter volt, de az első világháború körülményei között ez elég lett volna ahhoz, hogy egy aknát a drótakadályok alá vezessenek, és a megfelelő helyen felrobbantsák. A kor technológiai fejlettségi szintjén ennél több nem volt elvárható, főleg annak ismeretében, hogy a haditechnikai fejlesztések elsősorban a harcokosokra fókuszáltak. Viszont az irányokat ezek a fejlesztések kijelölték, ezek a járművek voltak az első vezető nélküli szárazföldi járművek (Unmanned Ground Vehicle - UGV) ősei [11]. A későbbiekben erre alapozva fejlesztették tovább közvetlenül a második világháború előtt és a háború alatt.

FELHASZNÁLT IRODALOM

- [1] Németh, András és Hegedűs, Ernő és Wippenhauser, András és Simó, Réka (2019) A katonai alkalmazású autonóm terepjáró járművek fejlesztésének egyes kérdései I. rész. HADITECHNIKA, 53 (4). pp. 11-16. ISSN 0230-6891
- [2] Szalkai István: “Pilóta nélküli légi járművek alkalmazásának történelmi pillanatai és ezekből levonható következtetések” REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK 31. évfolyam (2019) 3. szám 89–97 p. • DOI: 10.32560/rk.2019.3.447
- [3] H. R. Everett: Unmanned Systems of World Wars I and II. The MIT Press; 1st edition (November 6, 2015). 768 pages, ISBN: 978-0262029223
- [4] A. Pérez-Yuste, “Early Developments of Wireless Remote Control: The Telekino of Torres-Quevedo,” in Proceedings of the IEEE, vol. 96, no. 1, pp. 186-190, Jan. 2008, doi: 10.1109/JPROC.2007.909931.
- [5] Land torpedo Aubriot-Gabet Torpille Electrique <https://en.topwar.ru/123927-suhoputnaya-torpeda-aubriot-gabet-torpille-electrique-franciya.html> (utolsó letöltés: 2023.01.21.)
- [6] Сухопутная торпеда Schneider Crocodile <https://topwar.ru/123648-suhoputnaya-torpeda-schneider-crocodile-franciya.html> (utolsó letöltés: 2023.01.21.)
- [7] Поиск выхода из тупика. Часть 10. Torpille Terrestre Schneider Crocodile typ A/B. 1915., Если не можешь сломать взорви!!! <https://dzen.ru/media/id/5d36b0ffd4f07a00af1a9d3d/poisk-vyhoda-iz-tupika-chast-10-torpille-terrestre-schneider-crocodile-typ-ab-1915-esli-ne-mojesh-slomat-vzorvi-5fbd0c1b0b4af80149b21d66> (utolsó letöltés: 2023.01.21.)
- [8] -[9] -[10] E.E. Wickersham “Land Torpedo” US Patent 1407969A, Feb.28,1922
- [11] Unmanned Ground Vehicles: Timeline <https://www.army-technology.com/comment/unmanned-ground-vehicles-ugvs-2/> (utolsó letöltés: 2023.01.21.)

**OVERVIEW OF THE MAIN RESOLUTIONS
OF THE UNITED NATIONS IN
COUNTERING TERRORISM****AZ EGYESÜLT NEMZETEK SZERVEZETE
FŐBB HATÁROZATAINAK ÁTTEKINTÉSE
A TERRORIZMUS ELLENI VÉDEKEZÉSBEN**BAUMGARTNER Helga¹ – ÖSZI Arnold²**Abstract**

The United Nations (UN) has played a key role in countering terrorism in the past few years. The events on 11 September 2001 have significantly changed the approach to global counter-terrorism, the measures taken against terrorism. Following these events, the UN resolutions initially called for a strong and decisive response against terrorism in general. Over time, the resolutions became more specific, emphasizing the importance of cross-border cooperation. These resolutions highlight the importance of information exchange among member states, sharing best practices, and developing counter-terrorism strategies, for which the UN provides assistance through various organizations.

Keywords

United Nations, Security Council, terrorism, counter-terrorism, international cooperation

Absztrakt

Az Egyesült Nemzetek Szervezete (ENSZ) az elmúlt években aktív és meghatározó szerepet vállalt a terrorizmus elleni küzdelemben. A 2001. szeptember 11-i események jelentősen megváltoztatták a világ terrorizmus elleni védekezéséhez való hozzáállást. Az események után az ENSZ határozatai kezdetben főleg általánosan a terrorizmus elleni határozott fellépést sürgették, az azóta eltelt időben a határozatok már célirányosan, konkrétabb intézkedéseket fogalmaztak meg, kiemelve az országhatáron átnyúló együttműködés fontosságát. Ezek a határozatok kiemelik a tagállamok közötti információcsere fontosságát, a tapasztalatok és legjobb gyakorlatok megosztását és a terrorizmus elleni stratégiák kidolgozását, melyekhez az ENSZ különböző szervezeteken keresztül segítséget is nyújt

Kulcsszavak

Egyesült Nemzetek Szervezete, Biztonsági Tanács, terrorizmus, terrorizmus elleni védekezés, nemzetközi együttműködés

¹ baumgartner.helga@phd.uni-obuda.hu | ORCID: 0009-0003-7938-7614 | PhD Student, Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

² oszi.arnold@bgk.uni-obuda.hu | ORCID: 0000-0001-5988-0143 | adjunct professor, Óbuda University, Bánki Donát Faculty of Mechanical and Security Technology Engineering | adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A terrorizmus a nemzetközi közösség egészét érintő probléma, az ellene való küzdelem országhatárokon átnyúló együttműködést igényel. A terrorcselekmények következtében nemcsak az áldozatok, és azok családjai szenvednek el hatalmas veszteségeket, de az hatással van a társadalomra, a politikára és a nemzetgazdaságra is. Mindamellet, hogy az emberek általános biztonságérzete megrendül, kár keletkezhet a kritikus infrastruktúrában, melynek helyrehozatala hatalmas erőforrásokat emészt fel, és a kármentesítésre átcsoportosított humán és reál erőforrás következtében a nemzetgazdaság más területein keletkezhetnek hiányosságok.

A terrorizmus számos formát ölthet: míg a középkorban az állami apparátus része volt, később a szabadságharcosok éltek sokszor a terror erejével, addig manapság, a modern terrorizmus idején a szélsőséges politikai, ideológiai, illetve vallási nézeteket valló személyek, illetve csoportok eszköze földön, vízen, levegőben és a kiber térben. Hiába napjaink egyik legszélesebb körben alkalmazott, és legjobban üldözött fogalma, mégsem rendelkezik egy globálisan elfogadott meghatározással.

Az Amerikai Egyesült Államokban történt 2001. szeptember 11-i terrortámadások nemcsak Amerikát, de az egész világot megrendítették, melynek következtében egy teljesen új időszámítás kezdődött a terrorizmus és az ellene történő fellépés tekintetében. A biztonságról addig alkotott vélemények megváltoztak, az országok számos intézkedést tettek a mai napig az állampolgáraik biztonságának védelmében, mely lépések elsősorban a repülésbiztonságot és az országhatárokon való átkelést érintették. A terrorizmus elleni szigorú fellépés az országokban alapvető biztonsági kérdéssé, a nemzetközi politikában kiemelt fontosságúvá vált, megváltoztatta az országok közötti viszonyok dinamikáját – míg egyes országok között szorosabb együttműködés jött létre a terrorizmus elleni hatékony fellépés érdekében, addig más országok szankciókkal és háborúkkal sújtottak olyan országokat, akikről a rendelkezésre álló hírszerzési információk alapján feltételezték, hogy összefüggésbe hozhatóak a terrorizmussal.

A szeptember 11.-i események kétségtelenül az Egyesült Nemzetek Szervezetének (ENSZ) határozataira is hatással voltak – míg korábban kisebb számú, hangvételét tekintve kevésbé szigorú határozatot fogalmaztak meg a terrorizmus elleni fellépéssel kapcsolatban, addig a terrortámadások után egyes határozatok kimondottan felszólítják a tagállamokat bizonyos lépések megtételére, mely szintén precedens értékű volt.

A következőkben az ENSZ terrorizmus elleni küzdelem érdekében a 2001. szeptember 11-i események után meghozott legfontosabb határozatait ismertetem. Kiemelt figyelmet fordítok a terrorizmus, illetve a terrorista cselekmények fogalmi meghatározására, a terrorizmus ellen létrehozott szervezetekre, és a határozatok tartalmának összefoglalására.

FOGALMI MEGHATÁROZÁS

Az elmúlt évek-évtizedek alatt számos próbálkozás volt arra, hogy a terrorizmus fogalmát sikerüljön úgy meghatározni, hogy az mindenki számára elfogadható legyen.

Alex P. Schmid, aki kiemelkedő szaktekintélynek számít a terrorizmus kutatásának területén és aki korábban éveken át volt az ENSZ által létrehozott ad-hoc bizottságnak tagja amelynek fő feladata többek között a terrorizmus fogalmának meghatározása volt. Schmid és kollégái már 1988-ban, az akkor megjelent "Politikai Terrorizmus" (angolul Political

Terrorism) című könyvükben 109 definíció elemzését végezték el, több száz oldalon keresztül vizsgálva a terrorizmus fogalmát. Azóta is Schmid a terrorizmus és az az elleni védekezés kiemelkedő kutatója. 2003-ban kiadott könyvében már 250 olyan definíciót találunk, amelyek megtalálhatók a nemzetközi szakirodalomban. Schmid a 2023-ban megjelent "Terrorizmus meghatározása" (angolul Defining Terrorism) című művében részletezi az ENSZ által meghatározott fogalom hiányának problémáját, annak lehetséges okait és az ezekből fakadó következményeket. [1]

Azóta is tanulmányok sorai igyekeztek új fogalmat alkotni, a meglévőket összevetni, azokat értelmezni, hogy mit is nevezhetünk ma tulajdonképpen terrorizmusnak. Az internet különböző keresőmotorjaiban más és más megfogalmazást találhatunk, melyek szövegezésében, szóhasználatában különbözőek lehetnek, de lényegükben hasonlóak. Mindezek ellenére korunk legnagyobb fenyegetését jelentő problémája még a mai napig nem rendelkezik egy olyan definícióval, amely minden ország számára egyértelmű iránymutatást ad és amely mindenki számára kötelező erővel bír.

AZ ENSZ FONTOSABB HATÁROZATAI A TERRORIZMUSSEL KAPCSOLATBAN

Az ENSZ tagállamai közé a világ 193 országa tartozik – ez alól csak Vatikánváros, Palesztina, és a nemzetközileg el nem ismert, úgynevezett, de facto államok kivételek. Joggal merül fel az a feltételezés, hogy az ENSZ tölthetné be a fogalomalkotó szerepet ebben a nagyon is aktuális és az emberiség egészét érintő problémában, hogy egy mindenki számára elfogadható, és kötelező erővel bíró fogalmat megalkosson.

Az ENSZ legfőbb szerve a Közgyűlés, melynek kivétel nélkül minden tagállam tagja. Az ENSZ Alapokmánya szerint a Közgyűlés nem rendelkezik jogalkotói hatáskörrel, tehát a meghozott határozatok nem bírnak kötelező erővel a tagállamok részére, azonban a tagállamok véleményét és erkölcsi tekintélyét fejezik ki, így amennyiben a Közgyűlés valamilyen határozatot elfogad, az a szokásjogi normák alapján akár hozzájárulhat a nemzetközi, illetve a nemzeti jog alakulásához. [2]

Ennek szellemében érdemes megemlíteni, hogy a Közgyűlése 1996-ban az 51/210 (A/RES/51/210). számú határozatában „*A nemzetközi terrorizmus felszámolására történő intézkedések meghozatalára*” egy ad-hoc bizottságot állított fel, amelynek feladata többek között az, hogy kidolgozzon egy átfogó egyezményt a nemzetközi terrorizmus ellen. Az egyezmény megalkotásával az lett volna a cél, hogy egy globális, minden tagállam által elfogadott jogi keretrendszert állítsanak fel, amely lehetővé teszi a tagállamok számára a terrorizmus és az ellene való egységes védekezést. [3]

A tervezett definíció a következőképpen szól: „*A jelen Egyezmény értelmében bűncselekményt követ el az a személy, aki jogellenesen és szándékosan bármilyen eszközzel olyan cselekedetet követ el, amely:*

- a) *halált vagy súlyos testi sérülést okoz bármely személynek; vagy*
- b) *súlyos károkat okoz a köz- vagy magántulajdonban, ideértve a közforgalmú helyeket, az állami vagy kormányzati létesítményeket, a közlekedési rendszereket, az infrastruktúra létesítményeket vagy a környezetet; vagy*
- c) *károkat okoz a (b) bekezdésben említett tulajdonokban, helyszínekben, létesítményekben vagy rendszerekben, amelyek jelentős gazdasági veszteséget okoznak vagy okozhatnak;*

amikor a cselekedet célja, természete vagy körülményei szerint, a lakosság megfélemlítése, vagy egy kormány vagy nemzetközi szervezet bármely cselekedetére vagy tartózkodására való kényszerítése.”

Az ad-hoc bizottság az elmúlt huszonöt évben az egyezmény szövegezését tekintve szinte teljes mértékben megegyezett, azonban a legfontosabb kérdésben, a terrorizmus fogalmában nem jutottak dűlőre. A Közgyűlés szeretne volna, ha a Hatodik (Jogi) Bizottság – mely az ENSZ Közgyűlésének egyik fő bizottsága – a 2022. évi ülésén véglegesíti a korábban említett egyezménytervezetet, azonban ez nem történt meg, a definícióval kapcsolatos egyet nem értés miatt. [4] [5]

Az ENSZ Alapokmányában kinyilatkoztatásra került a nemzetközi béke és biztonság fenntartása, amely az ENSZ politikai döntéshozó és végrehajtó szerve, a Biztonsági Tanácsának (BT) legfőbb feladata. A Biztonsági Tanácsnak öt állandó – Amerika Egyesült Államok, Egyesült Királyság, Franciaország, Kína és Oroszország – és tíz nem állandó, két évente megválasztott taggal rendelkezik, és az egyetlen olyan ENSZ szerv, amely a tagállamokra nézve kötelező erejű határozatot hozhat.

A Biztonsági Tanács a 2001. szeptember 11-i események hatására kiadott legelső határozata a 1368 (2001) számú határozat - amely a terrortámadások másnapján született -, elítélte a terrortámadást, és elismerte a tagállamok önvédelemhez való jogát. A határozatban kijelenti, hogy – hivatkozva az ENSZ Alapokmányának 51. cikkére – „*kész minden szükséges lépést megtenni a válaszadás érdekében*” („*by all necessary measures*”). Itt is, és a későbbiekben is megfigyelhető, hogy egyes tagállamok az ilyen jellegű megfogalmazást sok esetben nem explicit felhatalmazásnak értékelték a terrorizmus elleni fegyveres konfliktusokra és háborús lépésekre. [6]

Nemsokkal később a Biztonsági Tanács az 1373 (2001) számú határozatában kötelezi a nemzeteket „*a terrorizmus, illetve annak finanszírozásának büntetésére, a terroristák illetve olyan személyek részére, akik a terrorizmussal összefüggésbe hozhatóak tagadjak meg a menekült státusz megadását, büntessék azokat a személyeket illetve csoportokat akik terrorista cselekményeket hajtanak végre, illetve azok szabad mozgását akadályozzák meg megfelelő határellenőrzéssel, és megbízható személyazonosító okmányok kiállításával*”. A Biztonsági Tanács a határozatban úgy fogalmaz, hogy a tagállamok „*tegyenek meg minden szükséges lépést*” („*take all necessary steps*”) ezen célok végrehajtásának érdekében. Ez a határozat a terrorizmus elleni küzdelem egyik alapköve, és a globális terrorizmus elleni küzdelem alapjául szolgál. [7]

Mivel az 1373 (2001) számú határozat nem ad egyértelmű megfogalmazást a terrorizmusra, az egyes tagállamok saját maguknak igyekeztek meghatározni, hogy mi számít terrorizmusnak és terrorista cselekménynek, amely egy meglehetősen széttagolt, és nem egységes értelmezéshez vezetett a tagállamok között, ezáltal az ellene való fellépés is hasonló diverzifikált képet mutat. Éppen ez vezetett ahhoz, hogy a jogvédő szervezetek, többek között az Amnesty International – mely az emberi jogok védelmében a világ legnagyobb szervezetének számít – aggodalmukat fejezték ki, hogy a terrorizmus és a terrorista cselekmények elleni védekezés tulajdonképpen az államok szabad értelmezésére van bízva, amely így akár az emberi jogok megsértésével is járhat. [8]

Az Biztonsági Tanács szintén az 1373 (2001) határozatával létrehozta a Terrorizmusellenes Bizottságot (angolul Counter-Terrorism Committee – CTC), melynek legfőbb

mandátuma több határozattal együtt az 1373. számú határozat implementálásának felügyelete az egyes tagállamokban, melyet a Terrorizmusellenes Végrehajtó Igazgatóság (angolul Counter-Terrorism Committee Executive Directorate – CTED) támogat. A tagállamok jelentési kötelezettséggel bírnak a Terrorizmusellenes Végrehajtó Igazgatóság felé, amely a jelentések és országlátogatások alapján elkészíti a saját értékelését a tagállamok terrorizmus elleni védekezés érdekében tett lépéseit, az ezen határozatban foglaltak implementálását, és az esetleges hiányosságok kiküszöbölésére javaslatot tesz. Mivel a jelentés az adott tagállamra nézve szenzitív információkat – a felfedezett esetleges hiányokat, a tagállamok terrorizmus-ellenes stratégiáját, a határozatok implementálásának mérföldköveit, és akár az alkalmazott gyakorlatokat – tartalmazhat, így azok nem nyilvánosak.

1452 (2002) számú határozatában a Biztonsági Tanács engedélyezte, hogy az 1267 (1999) határozatban korábban szankciókkal sújtott terroristák vagyona mentességet élvez abban az esetben, ha alapvető megélhetési és egészségügyi kiadások fedezésére szolgál, illetve egyéb olyan esetekben, melyet a tagállamok kimondottan engedélyeznek. [9]

1456 (2003) számú határozat felszólítja a tagállamokat a korábban terrorizmus ellen hozott határozatok maradéktalan betartására, valamint a Terrorizmusellenes Bizottságnak való jelentési kötelezettségre, illetve az azzal való együttműködésre. Egyben szorgalmazza a Terrorizmusellenes Bizottságot a nem kollaboráló államokkal való határozottabb fellépésre, és a 1373 (2001) határozat implementálásának fokozottabb ellenőrzésére. A határozat a terrorizmus elleni határozott fellépés mellett már az emberi jogok tiszteletben tartását is említi, először a terrorizmus ellen hozott határozatok között. Ettől fogva a Biztonsági Tanács minden határozata kiemeli az emberi jogok tiszteletben tartását a terrorizmus elleni fellépés során. [10]

A Közgyűlés 2003-ban az 57/219 (A/RES/57/219) határozatában felhívta a tagállamok figyelmét az emberi jogok figyelembevételére a terrorizmus elleni fellépés során meghozott lépésekkel kapcsolatban. A határozat jelentősége abban rejlik, hogy hangsúlyozza az emberi jogok minden emberre vonatkozó és korlátozhatatlan jellegét. Ez a határozat kiemelkedő fontosságú, mivel korábban olyan intézkedések voltak tapasztalhatók a terrorizmussal vádolt vagy bűnösnek talált személyekkel szemben, amelyek korlátozták az emberi jogaik gyakorlását. [11]

Az 1540 (2004) számú határozatban a Biztonsági Tanács a nukleáris, vegyi és biológiai fegyverek és hordozóeszközök szigorú ellenőrzésére és terjesztésének megakadályozására és az azokhoz kapcsolódó terrorizmus elleni küzdelemre fókuszál. A határozat felszólítja a tagállamokat, hogy akadályozzák meg hogy a nem állami szereplők ilyen típusú fegyverekhez, illetve eszközökhöz juthassanak. A határozat egyidejűleg létrehozta az 1540-es Bizottságot, melynek feladata nem csak a határozat implementálásának felügyelete, de annak elősegítése érdekében módszerek és ajánlások megfogalmazása is. Bár történt előrehaladás a határozatban foglaltakkal kapcsolatban, annak tartalmát és az 1540-es Bizottság mandátumát ezek után is többször, több határozatban meghosszabbították, egyben felhívták a tagállamok figyelmét a jelentési kötelezettségükre, és az 1540 (2004) számú határozatban foglaltakban történő megfelelésre. [12]

Ezt követően 2004-ben a Biztonsági Tanács az 1566 (2004) számú határozatában terrorista cselekményként határozza meg azt a bűncselekményt, mely „...arra irányul, hogy halált vagy súlyos testi sérülést okozzon civileknek és a harcokban részt nem vevőknek, vagy túszejtésre irányul, és amelynek természetéből és a körülményekből adódóan az a célja,

hogy megfélemlítse a lakosságot, a lakosság egy csoportját, vagy meghatározott személyeket, vagy arra kényszerítsen egy kormányt vagy nemzetközi szervezetet, hogy valamit megtegyen, vagy tartózkodjék valaminek a megtételétől... ”. [13]

Az 1566 (2004) számú határozat részben segített az 1373 (2001) számú határozat hiányosságainak javítását, és szűkítette a fogalmak értelmezésének lehetséges módját, mégsem oldotta meg teljesen a fogalom hiányának problémáját. A definíció elfogadottságát nehezíti, hogy egyes országok a fogalmat túl tágan tartották, mások szerint pedig nem tartalmaz olyan fontos elemeket, mint például az államok által elkövetett terrorizmus. Ezen felül a határozat jellegénél fogva nem bír kötelező erővel a tagállamokra vonatkozóan, így az a tagállamok számára csupán iránymutatással szolgál. [14]

Az 1624 (2005) számú határozat felszólítja a tagállamokat a terrorizmus, illetve terrorista cselekedetekre való felbujtás – vagyis az úgynevezett terrorista propaganda – büntetésére, és megelőzésére, egyben sürgeti, hogy a felbujtóktól tagadják meg a menedékjog biztosításának lehetőségét. Kötelezi a tagországokat az államhatáraik védelmének megerősítésére, a felbujtókat beutazásának megelőzésére, valamint felszólítja őket a fokozott utasbiztonsági szűrések és a terrorizmussal összefüggésbe hozható személyek kiszűrésére tett lépések növelésére. Egyben sürgeti a tagállamokat a vallási és kulturális alapú támadások és terrorista cselekmények elleni fellépésre, és igyekezzenek megakadályozni az oktatási, kulturális és vallási intézmények elleni terrorista támadásokat. [15]

2006-ban az ENSZ Közgyűlése egyhangúlag fogadta el a 60/88 (A/RES/60/288) számú határozatát, amely az ENSZ Terrorizmusellenes Globális Stratégiájaként ismert. A Stratégia egy általános keretrendszer alkot, amely segít a tagállamoknak a terrorizmus elleni hatékonyabb küzdelemben. A Stratégia négy pillérre építve támogatja a nemzeti, regionális és nemzetközi törekvéseket a terrorizmus elleni védekezésben. A négy pillér a következő:

- I. *A terrorizmus terjedéséhez hozzájáruló feltételek kezelése*
- II. *A terrorizmus megelőzése és leküzdése*
- III. *Az államok képességeinek növelése a terrorizmus megelőzésére és leküzdésére, valamint az Egyesült Nemzetek rendszerének szerepének megerősítése e tekintetben*
- IV. *Az emberi jogok és a jogállamiság tiszteletben tartására irányuló intézkedések a terrorizmus elleni harc alapjául szolgáló alapvető tényezőként.*

A Stratégia függeléke a pillérek megvalósításához szükséges Cselekvési Tervet tartalmazza, amely intézkedések széles skáláját fogalmazza meg a terrorizmus elleni küzdelem, valamint a tagállamok közötti szorosabb és hatékonyabb együttműködés érdekében. [16]

A Terrorizmusellenes Globális Stratégiát két évente felülvizsgálja az ENSZ Közgyűlése, hogy naprakészen támogassa a tagállamokat a terrorizmus elleni küzdelemben. A Stratégia elfogadásával a tagállamok egyértelmű üzenetet közvetítenek, hogy a terrorizmust minden formában elfogadhatatlannak, és üldözendőnek tartják. A Stratégia implementálását a Terrorizmus Elleni Végrehajtási Munkacsoport (angolul Counter-Terrorism Implementation Task Force - CTITF) végzi. A Munkacsoportba 38 ENSZ intézmény tartozik, amely szabályzókkal, szakmai ismeretekkel és technikai segítség nyújtással támogatják a tagállamokat a Stratégia mihamarabbi implementálásához.

2011-ben az ENSZ Közgyűlése a 66/10 (A/RES/66/10) határozatában megalapította az ENSZ Terrorizmus Elleni Központját (angolul Counter-Terrorism Centre – CCT),

amely kiválósági központként segíti a tagállamokat a Terrorizmusellenes Globális Stratégiája pillérjeinek minél eredményesebb implementálásában. A Terrorizmus Elleni Központ későbbiekben az ENSZ Terrorizmus Ellenes Hivatalának részeként főleg technikai segítséget nyújt, és a kapacitások növelésében segíti a tagállamokat. [17]

A Biztonsági Tanács 2170 (2014) számú határozatban a külföldi terrorista harcosok (angolul *foreign terrorist fighters – FTF*) ellen való szigorú fellépésre, a terrorista szervezetekhez való csatlakozás céljából történő utazások megakadályozására, és a terrorista szervezetek finanszírozásának büntetését és ellehetetlenítését megakadályozására szólította fel a tagállamokat, illetve ezen szervezetekhez köthető személyeket szankcionált. [18]

A 2178 (2014) számú határozatban a Biztonsági Tanács felszólítja a tagállamokat a terrorizmussal összefüggésbe hozható személyek, ideértve a külföldi terrorista harcosok utazásának megelőzésére és büntetésére. Egyben sürgeti őket, hogy a területükön működő légitársaságok előzetes utasinformációs adatokat (angolul *Advanced Passenger Information – API*) szolgáltatassanak a megfelelő nemzeti hatóságoknak annak érdekében, hogy megelőzzék az adott tagállam területére belépni, vagy területéről kilépni, vagy azon átutazni igyekvőket, akik terrorizmussal vagy terrorista cselekményekkel összefüggésbe hozhatóak. Egyben utasítja a tagállamokat a szorosabb együttműködésre a külföldi terrorista harcosok által jelentett fenyegetés kezelésében, ideértve a radikalizálódást, az utazások megakadályozását, az anyagi támogatást, valamint a hazatérő külföldi terrorista harcosok üldözését, rehabilitációját és integrációját célzó stratégiák kidolgozását és végrehajtását. A Biztonsági Tanács ebben a határozatban ítéli el először az erőszakos extrémizmust (angolul *violent extremism*), mely terrorizmushoz vezethet, és ezek után nem csak a terrorizmus, de az erőszakos extrémizmus elleni megelőzést és küzdelmet is hirdeti (angolul *preventing and countering violent extremism – P/CVE*). [19]

A Biztonsági Tanács a 2253 (2015) számú határozatban a terrorista csoportok vagyionának befagyasztására, utazásainak megakadályozására, részükre fegyverek eladásának tilalmára kötelezi a tagállamokat, valamint, hogy aktívabban vegyenek részt a terrorizmussal vádolt személyek listázásában, hogy ezáltal szankcionálhatóvá váljanak, és felhívja a tagállamok figyelmét az együttműködésre a terrorizmussal vádolt személyek felelősségre vonásakor. Kiemeli a terrorizmus finanszírozásának megelőzése érdekében a nem állami szektorral történő szoros együttműködés fontosságát. Kitér arra, hogy megakadályozzák, hogy terrorista csoportok fegyverzeti, vagy olyan anyagokhoz jussanak, melyből fegyvert, illetve robbanóeszközt állíthatnak elő. Figyelmeztet a terrorista propaganda interneten történő terjesztésének veszélyére, és felszólítja a tagállamokat, hogy tegyenek szigorú intézkedéseket a propaganda terjedésének és az online toborzás megakadályozása érdekében. [20]

A 2309 (2016) számú határozat megerősíti a tagállamok felelősségét a saját és más állam polgárai biztonságáért a területükön működő légi szolgáltatások elleni terrorista támadásokkal szemben. Felszólítja a tagállamokat a Nemzetközi Polgári Repülési Szervezettel (angolul *International Civil Aviation Organization – ICAO*) együttműködve a repülésbiztonsági követelmények maradéktalan betartására, a civil légiközlekedést érintő fenyegetések kezelésére, valamint előírja a kockázatalapú megközelítést a repülőtereken alkalmazott intézkedések során a légiközlekedés-biztonságának javítása érdekében. A határozatban üdvözli az ICAO és a CTED közötti együttműködést a hiányosságok és a sebezhetőségek azonosítása és kezelése terén, és egyidejűleg felkéri a CTED-et, hogy a korábban említett

országprofilok és jelentések elkészítése során kiemelt figyelmet fordítson a repülésbiztonsági szempontokra. [21]

A 2322 (2016) számú határozat sürgeti a tagállamokat, a terrorista cselekedetekhez köthető személyekkel kapcsolatos információk – beleértve a biometrikus adatokat is – egymással való megosztására, valamint kiemeli a Nemzetközi Bűnügyi Rendőrség Szervezetével (angolul International Criminal Police Organization – INTERPOL) való szorosabb együttműködés fontosságát is. Sürgeti a tagállamokat terrorizmus finanszírozásának kiemelt büntetésére, és az egymással való együttműködésre annak megakadályozása érdekében, egyben felszólítja a tagállamokat, hogy az ENSZ Kábítószer- és Bűnügyi Hivatalával (angolul United Nations Office on Drugs and Crime – UNODC), a Nevelésügyi, Tudományos és Kulturális Szervezetével (angolul United Nations Educational, Scientific and Cultural Organization – UNESCO) valamint az INTERPOLLAL együttműködve hozzanak nemzeti intézkedéseket a kulturális javak kereskedelmével kapcsolatban, megakadályozva, hogy azok terrorista csoportok számára előnyt jelentsenek. [22]

Az ENSZ Közgyűlés 71/291 (A/RES/71/291) számú határozatával 2017-ben megalapította a Terrorizmus Ellenes Hivatalát (angolul United Nations – Office of Counter Terrorism – UNOCT), melybe integrálta a Terrorizmus Elleni Végrehajtási Munkacsoportot és a CCT-t. A Terrorizmus Ellenes Hivatal vezető szerepet tölt be a Globális Terrorizmussal Ellenes Stratégia megvalósításának támogatásában, valamint a Biztonsági Tanács által meghatározott célok megvalósításában. Célja a terrorizmus elleni erőfeszítések és a stratégiák összehangolása a globális szinten. A Hivatal támogatja a tagállamokat a terrorizmus elleni képességeik növelésében, ideértve többek között a nemzeti terrorizmus elleni stratégiák ki- illetve átdolgozását, a jogi keretek kialakításában való segítséget, szakmai ismeretek átadását és technikai támogatást. [23]

A Biztonsági Tanács 2396 (2017) számú határozat felszólítja a tagállamokat hogy hatékony határvédelemmel és az úti okmányok hamisításának megelőzését célzó intézkedésekkel akadályozzák meg a terrorizmussal vádolt személyek mozgását, egyben szorgalmazza a tagállamokat hogy az ICAO-val együttműködve utas-nyilvántartási adatállomány (angolul Passenger Name Record – PNR) létrehozására és megosztására a releváns nemzeti hatóságokkal annak érdekében hogy a külföldi terrorista harcosok utazását felderíthessék és adott esetben megakadályozhassák azt. Továbbá felszólítja a tagállamokat az ICAO Globális Légi Biztonsági Tervének (angolul Global Aviation Security Plan – GAsEP) implementálására a légi biztonság világszerte történő javítása érdekében. Szorgalmazza a tagállamokat a biometrikus adatok gyűjtésére alkalmas rendszerek kiépítésére és alkalmazására a terrorizmussal vádolt személyek hatékony azonosítása érdekében, egyben bátorítja a tagállamokat ezen adatok egymással, valamint az INTERPOLLAL és más nemzetközi szervezettel való megosztásra az emberi jogok tiszteletben tartásával. [24]

2482 (2019) számú határozat szorgalmazza a tagállamokat, hogy erősítsék meg a nemzetközi terrorizmus és szervezett bűnözés közötti kapcsolatok kezelését. A szervezett bűnözés, mint például az emberkereskedelem, a fegyverkereskedelem és a droggereskedelem, komoly fenyegetést jelentenek a nemzetközi biztonságra, mivel közvetlenül vagy közvetlenül hozzájárulhatnak a terrorizmus finanszírozásához és a terroristákhoz jutó fegyverekhez vagy fegyverzeti anyagokhoz. A határozat sürgeti a tagállamokat a törvényeik szigorítására, a szervezett bűnözés üldözésére és az ezekkel kapcsolatos információk nemzetközi szintű megosztására. [25]

ÖSSZEFOGLALÁS

A 2001 szeptember 11-i terrortámadásokat követően a világ terrorizmussal kapcsolatos szemlélete egy csapásra változott meg. Az országok általános biztonságérzete meggyengült, a terrorizmussal szemben egyre szigorúbb fellépéseket tettek. Ezt a tendenciát az ENSZ határozatai is követték anélkül, hogy megfelelő fogalmi rendszerrel bírnának a terrorizmus meghatározására.

Az 1373 (2001) számú határozatban felmerült fogalmi hiányosságok és a terrorizmus értelmezésének a tagállamokra bízott szabad döntési lehetősége számos esetben vezetett nem kellően átgondolt vagy szabályozott lépésekhez, mely sok esetben sértett emberi jogokat, amely ellen később jogvédő szervezetek határozottan tiltakoztak. Ezt eszközölve, a Biztonsági Tanács az 1456 (2004) számú határozatába először belefoglalta, hogy a terrorizmus elleni határozott fellépéseket az emberi jogok tiszteletben tartásával kell végrehajtani, de a terrorizmust meghatározó definíció még a mai napig nem született.

A terrorizmus elleni védekezés és a kiadott határozatok során az ENSZ egyre inkább igyekszik a probléma mélyére ásni, és konkrétabb határozatokat megfogalmazni, melyeket az alábbiak szerint csoportosíthatunk:

- a terrorizmussal és terrorista cselekedetekkel kapcsolatba hozható személyek utazásainak megakadályozására, valamint a terrorista személyek utazás során történő kiszűrésére hozott határozatok
- a repülésbiztonságot növelő határozatok
- a terroristák tömegpusztító fegyverekhez való jutását megakadályozó határozatok
- a terrorizmus finanszírozásával, és az azzal kapcsolatba hozható szervezett bűnözést szankcionáló kapcsolatos határozatok
- terrorizmussal kapcsolatba hozható személyek szankcionálására és vagyonuk befagyasztására hozott határozatok
- a tagállamok fellépését és kapacitás növelését segítő apparátusok létrehozásáról szóló határozatok

Az ENSZ terrorizmus elleni védekezés érdekében hozott határozatai a globális fellépés összehangoltabbá tételét, a terrorizmus elleni képességek növelését, az egységes jogi keretek kidolgozását szolgálják, valamint szakmai és technikai segítséget nyújtanak egy terrorizmus nélküli jövő érdekében.

FELHASZNÁLT IRODALOM

- [1] SCHMID, Alex P., Defining Terrorism - International Centre for Counter-Terrorism (ICCT) Report, 2023, DOI: 10.19165/2023.3.01 [Online] [link](#)
- [2] STAUBER Péter, A terrorizmus elleni küzdelem nemzetközi intézményi és jogi kerete, Doktori (Ph.D) értekezés, Pécsi Tudományegyetem Állam és Jogtudományi Kar Doktori Iskola 2017, pp 37-38. [link](#)
- [3] ENSZ Közgyűlésének A/RES/51/210 számú határozata [link](#)
- [4] ENSZ Közgyűlésének A/RES/76/121 számú határozata [link](#)
- [5] ENSZ Közgyűlés Hatodik (Jogi) Bizottság 77. Ülésének Összefoglalója [Online] [link](#)
- [6] ENSZ Biztonsági Tanácsának S/RES/1368 (2001) számú határozata [link](#)
- [7] ENSZ Biztonsági Tanácsának S/RES/1373 (2001) számú határozata [link](#)

- [8] Statement by Amnesty International on the implementation of Security Council Resolution 1373, AI Index No. IOR 52/002/2001, [link](#)
- [9] ENSZ Biztonsági Tanácsának S/RES/1452 (2002) számú határozata [link](#)
- [10] ENSZ Biztonsági Tanácsának S/RES/1456 (2003) számú határozata [link](#)
- [11] ENSZ Közgyűlésének A/RES/57/219 számú határozata [link](#)
- [12] ENSZ Biztonsági Tanácsának S/RES/1540 (2004) számú határozata [link](#)
- [13] GYÚRÚ Attila, A terrorizmus fogalma a nemzetközi jogban, Eötvös Lóránt Tudomány Egyetem, Nemzetközi Jogi Tanszék, Themis 2015. június pp. 113-140. [link](#)
- [14] ENSZ Biztonsági Tanácsának S/RES/1566 (2004) számú határozata [link](#)
- [15] ENSZ Biztonsági Tanácsának S/RES/1624 (2005) számú határozata [link](#)
- [16] ENSZ Közgyűlésének A/RES/60/88 számú határozata [link](#)
- [17] ENSZ Közgyűlésének A/RES/66/10 számú határozata [link](#)
- [18] ENSZ Biztonsági Tanácsának S/RES/2170 (2014) számú határozata [link](#)
- [19] ENSZ Biztonsági Tanácsának S/RES/2178 (2014) számú határozata [link](#)
- [20] ENSZ Biztonsági Tanácsának S/RES/2253 (2015) számú határozata [link](#)
- [21] ENSZ Biztonsági Tanácsának S/RES/2309 (2016) számú határozata [link](#)
- [22] ENSZ Biztonsági Tanácsának S/RES/2322 (2016) számú határozata [link](#)
- [23] ENSZ Közgyűlésének A/RES/71/291 számú határozata [link](#)
- [24] ENSZ Biztonsági Tanácsának S/RES/2396 (2017) számú határozata [link](#)
- [25] ENSZ Biztonsági Tanácsának S/RES/2482 (2019) számú határozata [link](#)

The complex connection of warfare, terrorism and the use of drones | **A hadviselés, terrorizmus és drónhasználat komplex kapcsolata**

PÁL Anita Brigitta¹**Abstract**

The widespread use of drones presents new challenges in Defence and Security sectors. Terrorist groups have also recognized the potential of drones and are actively using them to support their activities. This trend is a cause for concern as drones are readily available and relatively cheap, making it difficult for traditional security measures to be effective. The field of warfare, terrorism and the use of drones represents a dynamic and constantly changing environment in which the international community and the legal system must work better together. The article points out that in order to find appropriate solutions, it is necessary to maintain a balance between human rights and security. This is the only way to ensure that the potential of drones can be beneficially and safely used in the global environment.

Keywords

human rights, international relations, technology, drones, terrorism, war and conflict

Absztrakt

A drónok széleskörű alkalmazása új kihívásokat jelent a védelem és a biztonság terén. A legtöbb terrorista szervezet is felismerte a drónokban rejlő potenciált, és elkezdtek őket aktívan használni saját tevékenységeik támogatására. Ez a trend aggodalomra ad okot, mivel a drónok könnyen hozzáférhetők és viszonylag olcsók, ami megnehezíti a hagyományos biztonsági intézkedések hatékonyságát. A hadviselés, terrorizmus és drónhasználat területe egy dinamikus és folyamatosan változó környezetet jelent, amelyben a nemzetközi közösségnek és jogrendszernek együtt kell működni. A cikk rámutat arra, hogy a megfelelő megoldások megtalálása érdekében szükség van az emberi jogok és a biztonság egyensúlyának fenntartására. Csak így lehet biztosítani, hogy a drónok potenciálja előnyösen és biztonságosan használható legyen a globális környezetben.

Kulcsszavak

emberi jogok, nemzetközi kapcsolatok, technológia, drónok, terrorizmus, háború és konfliktus

¹ pal.anita@phd.uni-obuda.hu | ORCID: 0000-0003-4750-193X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

TERRORIZMUS

Az elmúlt években a technológiai fejlődés jelentős hatással volt a csúcstechnológia területére, különösen az információs és kommunikációs szektorra. Egy ilyen fejlődési ágazat, amelyet kiemelnek, a pilóta nélküli repülőeszközök, azaz a drónok területe, amely sok kérdést vet fel a nemzetbiztonság és a jogos felhasználás szempontjából.

A terroristák is felismerték a drónok fejlődéséből adódó lehetőségeket, és aktívan használják őket támadásokra, megzavarásra, megfigyelésre és propaganda videók készítésére. [1] Jelenleg négy terrorszervezet rendelkezik azonosítható drónprogrammal, köztük a Hezbollah, a Hamász, az Iszlám Állam és a Jabhat Fateh al-Sham.[2]

Fontos hangsúlyozni, hogy a terrorizmus terjedése szorosan összekapcsolódik a globalizációval és a technológia fejlődésével. E két jelenség kölcsönhatásában gyorsul fel a pénzügyi átutalások rendszere, és radikálisan átalakítja a pénzügyi szektor tevékenységét, ami hatással van a társadalmi folyamatokra is. Az új technológiai vívmányok elterjedése lehetővé tette az információs társadalmak kialakulását a 90-es évek után.

A terrorizmus elleni küzdelem már nem csak a hagyományos háborús helyszíneken zajlik, hanem Európa fővárosaiban, a szervereken és az összeköttetésekben. A modern harcműző minden területet behálóz. Tehát már nem kell árokban rejtőzni vagy bombák elől menekülni. Minden generációnak megvannak a saját hiányosságai, amelyekből a következő generáció előnyösen profitálhat a fejlesztések során. A cél mindig a rendszer biztonságos működésének biztosítása kell, hogy legyen.

Az közlekedési eszközök fejlesztése olyan önzetű járművek megjelenését teszi lehetővé, amelyek nem csupán zárt pályákon, hanem a mindennapi közlekedésben is képesek működni. Az autók mellett a repülés terén is kiemelkedő fejlődés zajlik, melynek katonai és polgári alkalmazása egyaránt fontos. A pilóta nélküli légi járművek, vagyis a drónok esetében különösen hangsúlyos, hogy képesek legyenek teljesíteni a rájuk bízott feladatokat, illetve biztonságosan visszatérni a kiindulópontjukra, még akkor is, ha megszakad a kapcsolatuk a földi irányítással vagy hézag keletkezik a kommunikációs csatornában. Az ilyen légi járművekbe beépített mesterséges intelligencia lehetővé teszi a feladatok automatikus végrehajtását a megváltozott körülmények ellenére is.[3]

A média korában a katonai technológia fejlődése olyan változásokat hozott, amelyek a világ minden táján hatást gyakorolnak, még a távoli akciók is helyi hatásokat válthatnak ki. A globális kommunikációs médianak köszönhetően a regionális és helyi konfliktusok akár globális méreteket is ölthetnek, hiszen a zűrzavar és a konfliktusok gyorsan terjednek. Nemcsak a nyugati nagyhatalmak és a feltörekvő államok, hanem a terrorista szervezetek is felismerik a média fontosságát és kihasználják azt. [4]

„A nemzetközi kapcsolatok európai folyóiratában említést tesznek a paneladatok elemzése alapján arról, hogy a hazai terrortámadások és a belföldi és transznacionális terrorista szervezetek által észlelt fenyegetések fokozzák a katonai részvételt a politikában.”[5] A terrorizmus és az erőszakos cselekmények lehetőséget teremtenek a politikai beavatkozásra és az állami intézmények ellenőrzésének elkerülésére. A terrorizmus befolyásolhatja a katonai részvételt a politikában két mechanizmus révén: amikor a kormányzati hatóságoknak katonai szakértelemre van szükségük a terrorizmus elleni küzdelemben és a nemzetbiztonság erősítésében, valamint amikor a fegyveres szereplők kihasználják az információs előnyüket a politikával szemben, hogy beleszóljanak a politikai folyamatokba.[6]

Azonban fontos felismerni, hogy a katonai megoldás csak egy eszköz a terrorizmus elleni harcban. A terrorizmus elleni küzdelem összetett tevékenység, amely politikai, gazdasági, diplomáciai, titkosszolgálati, adminisztratív, felderítő, rendőri és katonai intézkedéseket foglal magába, és kihasználja a különböző tudományágak eredményeit. A válsághelyzetekre összehangolt válaszlépések sorozata szükséges a hatékony terrorizmusellenes stratégia megvalósításához mind nemzeti, mind nemzetközi szinten.[7]

AZ AUTONÓM DRÓNOK ÉS A HADIIPARI FEJLESZTÉSEK ÚJ KORSZAKA

Az elmúlt években a világ legfejlettebb hadseregei izgalmas versenyben vannak az autonóm drónok képességeinek, taktikáinak és doktrínájának fejlesztéséért. Az autonóm drónok és hadiipari fejlesztések egy teljesen új korszakot nyitnak a hadviselésben. A moduláris megoldások lehetővé teszik a teljesen autonóm és ember-gép együttműködő küldetések támogatását a támadó műveleti védelemtől az urbánus hadviselésig.

A drónok szerepe a felderítésben és a légi hadviselésben fokozatosan növekszik, azonban az autonóm irányítással rendelkező drónok fejlesztése és innovációja jelentős kihívást állít eléink. Az autonóm drónok irányításában rejlő potenciális szinergiák kiaknázása, a földi járművek és drónok közötti együttműködés, valamint a drón-rajok összehangolása kritikus kérdésekké válnak a honvédelem szempontjából. A jövőben ugyanis a háborúk nemcsak a hagyományos harctéren zajlanak majd, hanem a virtuális térben is.[8]

Az utóbbi időben jelentősen megnőtt a katonai drónok által szállítható tömeg. A hatótávolságuk fokozatosan növekszik, lehetővé téve, hogy magasabb régiókban is hatékonyan teljesítsék feladataikat. A drónok aktívan részt vesznek konvoj kísérésben, előzetes útvonal ellenőrzésben és más infokommunikációs támogatásban, valamint képesek kiértékelni a támadó csapások hatásait. Légi logisztikai műveletek során pedig a nehezen megközelíthető területekre történő ellátás szállítására is használják őket.[9]

Az autonóm rendszerek a jövőben meg fogják változtatni a harctámogató műveleteket és a logisztikai feladatok végrehajtásának módját is. Az autonóm járművek és eszközök képesek összehangolt együttműködésre és feladatvégrehajtásra.

A harctámogató feladatok során a katonák olyan helyzetekkel szembesülhetnek, amelyek közvetlen veszélyt jelentenek az életükre, például épületek átvizsgálása, városi harc vagy veszélyes terepszakaszok felderítése. Az autonóm felderítő járművek az ilyen helyzetekben megbízhatóan képesek helyettesíteni a katonákat, biztosítva ezzel a védelmet és biztonságot.[10]

A NEMZETKÖZI TERRORIZMUS ELLENI HARC GAZDASÁGI-PÉNZÜGYI FELADATAI

A technikai haladás egyfajta áldásos átok. Ugyan megkönnyítik a kommunikációt és elősegítik az emberi kapcsolatok kiterjedését, ám legalább ugyanakkora veszélyfaktort is jelentenek, melyek érezhetőek a terrorizmus félelmetes következményeinek legkülönbözőbb színterein. A világháló segítségével a nemzetközi terrorizmus elleni háború frontvonala nem mindig a háborús helyeken zajlik, hanem Európa fővárosaiba, a szervereken, valamint az összeköttetésekben. A modern harcmező immáron mindent behálóz. Vagyis többé nem kell lövészárkokban megbújni meg bombákat kerülgetni a megfélemlítés vagy az elrettentés érdekében. A jelenlegi világunkat és az emberek egymáshoz való kapcsolódását azonban

olyan láthatatlan hálózatok szőtték át, amelyek komoly biztonsági kockázatokkal járnak együtt.

A terrorizmus két elágazáson keresztül kezdte meg "hadjárataát", és a választott út az állami reakciók függvénye.[11] „A terrorizmus társadalmi gyökereit kellene megszüntetni, s ehhez a biztonságpolitikai, társadalmi, gazdasági és katonai összetevőinek egyidejű, integrált kezelésre van szükség az átfogó megközelítés elve alapján.”[12]

A világ számos országát fenyegeti ma a nemzetközi terrorizmus, amely nemcsak emberéleteket követel, hanem gazdasági károkat is okoz. A terrorizmus finanszírozása az egyik kulcsfontosságú tényező, amely hajtja és fenntartja ezt a veszélyt. A nemzetközi közösségnek, beleértve a gazdasági-pénzügyi szektorokat, kiemelkedő szerepe van a terrorizmus elleni küzdelemben.[13]

A terrorizmus finanszírozása szorosan kapcsolódik a pénzmosáshoz, amelynek során a bűnözők az illegális forrásaitak törvényes pénzügyi áramlásokba próbálják bevezetni. A gazdasági-pénzügyi szektoroknak létfontosságú szerepük van az ilyen tevékenységek felismerésében és megakadályozásában. Erősíteni kell a pénzmosás elleni intézkedéseket, és javítani kell a bankok és más pénzügyintézetek képességét a gyanús tranzakciók felismerésére és jelentésére.[14]

A terrorizmus elleni gazdasági-pénzügyi intézkedések hatékonysága érdekében kiemelkedő fontosságú feladat kellene, hogy legyen, az országok közötti szoros együttműködés és információcsere.

„Létre kell hozni egy olyan – törvényesen működő – terrorizmus előrejelző rendszert, amely nemzeti és nemzetközi keretekben egybe gyűjti, elemzi, értékeli valamennyi szolgálat és hatóság minden rendelkezésre álló releváns információját. Hiszen az információ csak akkor lehet hasznos, ha azt az összes érintett szervezet időben megkapja és továbbítja a megfelelő döntési szintre. Ezzel együtt viszont nagy figyelmet kell fordítani az információ forrásának védelmére, amelyre a hírszerző- és elhárító szolgálatok általában nagy figyelmet fordítanak.” [15]

Az adatok és az intelligencia megosztása lehetővé teszi azon pénzügyi áramlások azonosítását, amelyek a terrorista csoportokat támogatják. A különböző országoknak és nemzetközi szervezeteknek, mint például az ENSZ és az IMF, összehangoltan kell működniük a terrorizmus finanszírozásának megakadályozása érdekében.

A NEMZETKÖZI TERRORIZMUS ELLENI HARC KATONAI FELADATAI

Ami az új típusú fenyegetések közül leginkább befolyással bír a katonai erő alkalmazására 9/11 óta, az a terrorizmus jelensége. A szövetségi beavatkozás Irakban és Afganisztánban gyűleleget jelentett a dzsihádisták terrorizmus számára.

Az amerikai külügyminisztérium jelenleg 61 terrorista szervezetet tart nyilván, és közülük az ISIS jelenleg a legdominánsabb. Kiemelkedően növekedett az alacsony technikai szintet igénylő okos bombák alkalmazása, melyek főként puha célpontok ellen irányulnak, például rendőri erők vagy kormányzati intézmények.[16]

Az nemzetközi terrorizmus elleni küzdelemben elengedhetetlen felismernünk, hogy a hadsereg bevetése csupán egy eszköz a rendelkezésre álló sok közül. A terrorizmus elleni harc bonyolult, és szükségszerűen országos és globális szinten is végbemenő tevékenység. A legjobb megoldás összehangolt válságreakáló műveletek sorozata, amely magában foglal

politikai, gazdasági, diplomáciai, titkosszolgálati, adminisztratív, felderítő, rendőri és katonai beavatkozásokat, valamint a hadtudomány mellett más tudományok eredményeit is felhasználja.[17]

A nemzetközi kapcsolatok európai folyóiratában megemlítik, hogy a paneladatok elemzése alapján megállapítható, hogy a hazai terrortámadások és a belföldi és transznacionális terrorista szervezetek által észlelt fenyegetések fokozzák a katonai részvételt a politikában.

A polgári-katonai kapcsolatok paradoxona olyan elméleti keret, mely egyszerűnek tűnhet, ugyanakkor politikailag meghatározó jelentőséggel bír. Az állam fegyveres erői, akik felelősek az állam fennmaradásáért és nemzetbiztonságáért, rendelkeznek azzal a hatalommal, amellyel képesek befolyásolni a társadalmat és a politikaalkotási folyamatot. Emellett rendelkeznek olyan eszközökkel is, amelyek segítségével erőszakkal vagy erőszak fenyegetésével képesek eltávolítani a végrehajtó hatóságokat.[18]

AZ ÚJ HADVISELÉSI PARADIGMA

Az autonóm drónok és rendszerek forradalmasítják a hadműveleteket, különösen városi területeken. Az autonóm légi és földi rendszerek formációja lehetővé teszi páratlan ISR-képességek nyújtását a taktikai peremen lévő egységek számára. 3D térképezés, talajhatoló radarképzés és taktikai kibertámadásokkal, amelyek képesek pontosan meghatározni a rádiókommunikációs tevékenységet, valamint tűztámogatást és belső helyszínen történő kutatást és semmisítést nyújtanak.

Az autonóm drónok és hadiipari fejlesztések előnye, hogy maximalizálják az operatív és halálos hatékonyságot, miközben minimalizálják a kockázatot a katonák számára. A folyamatos fejlesztések lehetővé teszik az elavult rendszerek integrálását az új technikai rendszerekbe.[19]

A TERRORISTÁK DRÓNHASZNÁLATA

Serbakov Márton Tibor cikke, mely megjelent a Nemzetbiztonsági Szemlében azt a kérdést taglalja, hogy a drónok és a fejlődő dróntechnológia, milyen szerepet töltenek be a terrorszervezetek legitim felhasználásának és a nemzetbiztonság által viselt kockázatainak szempontjából. A pilóta nélküli repülőeszközök (unnamed aircraft) szerepe az 1991-es öbölháború óta kulcsfontosságú katonai célú felhasználás szempontjából, fegyveres konfliktusok esetén. E piaci szegmens fejlődése visszatekint ugyan az 1960-as évekre, mára dominanciája azonban megoszlik az Amerikai Egyesült Államok és Izrael között.

Az Amerikai Védelmi Minisztérium a 2019-es költségvetésben 9,39 milliárd dolláros összeget igényelt pilóta nélküli rendszerekre és azokhoz kapcsolódó technológiákra. Több ország, például Törökország, Pakisztán és Nigéria is drónokat alkalmaz terrorelhárítás céljából. Az globális terrorizmus elleni hatékony fellépés érdekében nemzetközi együttműködésre van szükség a felderítés és hírszerzés területén.[20]

A tény, hogy a kereskedelmi forgalomban kapható drónok kapacitása alkalmasak lehetnek akár 22 kg tömegű teher szállítására, egy sor lehetőséget rejtenek magukba, ami a bűnözési célokra való felhasználását illeti. Megkönnyíti a kábítószer, a robbanóeszközök, tömegpusztító fegyverek, vegyi- és biológiai fegyverek, nukleáris és más radioaktív anyagok szállítását és bevetését. A bűnözők felhasználják továbbá kémkedésre, az információk

megszerzésére (ATM Automata PIN kódja), megzavarásra, a rendőrség megfigyelésére, propaganda videók készítésére, vagy akár rablások és betörések előkészületéhez. A drogkartellcsempészek és az embercsempészek is előszeretettel használják a drónokat a határőrök elkerülése érdekében.

A távvezérlésű repülőeszközök akár személyi sérülések okozása vagy elszenvedése nélkül könnyen be tudnak jutni biztosított helyekre. Makkay Imre szerint méretüknél és mozgásuknál fogva szinte kezelhetetlenek a légvédelem hagyományos eszközeivel, ráadásul „harc repülőgépek árának töredékéért” biztosítanak légierőt.

Az Egyesült Államok jelenleg jelentős figyelmet fordít az önvezérlő eszközök hadseregbe történő integrálására. A legújabb stratégiai terv, amely 2036-ig szól, a további önvezérlő eszközök és új technológiák fejlesztését és katonai felhasználását javasolja. Ráadásul a dokumentum előírja, hogy a Védelmi Minisztériumnak törekednie kell az önállóbb eszközök bevezetésére annak érdekében, hogy csökkentse az emberi erőforrásokra vonatkozó igényeket, valamint az időben hatékonyabb döntéshozatalt biztosítson a szélessávú kommunikációtól való függést csökkentve.[21]

Az izraeli fejlesztésű Skylock a világ élen járó drónelhárító rendszere, mely alkalmazható kritikus infrastruktúrák, konvojok és repülőterek védelmére vagy akár határvédelemnél. Rendszerspecifikussága abban rejlik, hogy képes átvenni a drónok feletti irányítást és semlegesíteni azok hatáskörét, valamint kinyerni belőlük a meglévő adatokat az elfogása előtti pillanatig.

Egy másik drónelhárító rendszer az Elbit Systems ReDrone egyedisége abban rejlik, hogy képes átvenni az irányítást több repülőeszköz fölött és földreszállítani őket anélkül, hogy kár keletkezne a készülékekben. A Legion-X egy moduláris robotikus és autonóm megoldásokból álló rendszer, amelyet a teljes mértékben autonóm és ember-gép együttműködő küldetések támogatására szabtak, ahol az üzemeltető kiválaszthatja a küldetéstípust, meghatározhatja az üzemelési területet, és hozzárendelheti a megfelelő önvezérlő rendszereket a különböző szerepekhez és feladatokhoz.[22]

2021 májusában Izrael mérföldkőnek számító innovációt vezetett be a nemzetközi hadviselés terén: drónrajokat vetettek be a Hamász ellen a Gázai övezetben. Az Elbit Systems által fejlesztett drónok gyakorlatilag elárasztották a célterületet, és rendkívül nehezítették a semlegesítésüket. Ezek a repülőgépek képesek voltak azonosítani a potenciális célpontokat és az adatokat központi egységbe továbbítani. Az intézmény által alkalmazott mesterséges intelligencia rendszer elemzés alá vette a beérkező adatokat, és precízen meghatározta, hogy pontosan mely fegyvereket, mely célpontra kell irányítani. Rövid időn belül az izraeli tüzérség hatékonyan megsemmisítette az ellenfelet, biztosítva az operatív sikerességet.[23]



1. ábra: Biztonság digitális vezeték nélküli kommunikációs rendszer [24]

A szakértők baljós ítéletet hirdettek, miszerint nem az a kérdés hogy valós lehet-e a félelem, hogy visszaélnék-e a fenyegetéssel, hanem hogy hogyan lehet minél erőteljesebb választ kidolgozni a fenyegetés elleni védekezésben. Fennáll a veszélye, hogy a technológiai fejlődések kommercializálódása támogatni fogja a legitim felhasználás elterjedését.

A katonai kutatások természetesen nem tűntek el, de alapvetően elmondható, hogy a kutatás–fejlesztés (K+F) dimenziójában a civil szféra dominál, alapvetően magántőke befektetésével, az itt eredmények fognak majd felhasználásra kerülni a katonai szektorban is. Ennek oka elsősorban a költséghatékonyság, ami a piaci lefedettségéből eredeztethető. Egy hadiipari cég nem csak katonai, hanem civil oldalra is termelést folytat a gazdaságosság és versenyképesség jegyében. A gyakorlatban így válnak majd az alkalmazott kutatások alkalmazott találmánnyá, amely később felhasználásra kerül, akár a nemzetbiztonsági szervek tevékenysége során.

A rakéták kilövése pilóta nélküli repülőgépekből elősegítheti egy viszonylag költséghatékony terrorellenes stratégia kialakítását. A drón támadások gyakran alacsonyabb költséggel és kevesebb kockázattal szembesítik a terrorista vezetőket és alkalmazottakat, mint más alternatív módszerek, ezzel potenciálisan csökkentve a támadások tervezési és végrehajtási képességét. A drón támadások ugyan hatékonyak a terrorista célpontok eliminálásában, ám potenciálisan visszahatásokkal járnak. Az ilyen célzott likvidációk miatt felmerülő harag, a jogellenes támadások a háborús övezeteken kívül, valamint a civilek érintéséből adódó mellékhatások mind elősegítik a terrorista propagandát és toborzást. Ennek következtében minden stratégikusan értelmes drónkampánynak törekednie kell az egyensúly megtartására ezen ellentétes tényezők között.[24]

Bár az mesterséges intelligencia már jelen van, a hadviselésben betöltött szerepe számos tényezőtől függ, mint például a kereskedelmi befektetések ütemétől, vagy a törekvéstől hogy versenyben maradjanak a nemzetközi riválisokkal, a kutatóközösség képességétől az mesterséges intelligencia kutatására és fejlesztésére, valamint a katonaság általános hozzáállásától a mesterséges intelligencia alkalmazásaihoz és specifikus háborús koncepciók kifejlesztésétől.[25]

ETIKA

A drónok gyors fejlődése és egyre növekvő alkalmazása komoly etikai kérdéseket vet fel a használatukkal kapcsolatban. Ahogy a katonaság törekszik a drónok nagyobb önállóságára az üzemeltetési költségek csökkentése érdekében, a drónok cselekedeteiért viselt felelősség egyre homályosabbá válik. A drónok etikus viselkedésének biztosítása kapcsán széles körben különböző nézetek fogalmazódnak meg, a bizalmatlanságtól egészen a drónok teljes önállóságát támogató álláspontig. A háborúban nagyrészt az emberi érzelmek által befolyásolt ítélőképesség következménye okozza az etikátlan cselekményeket. A robotok számára azonban nem jelentenek problémát az emberi érzelmek, mint például a harag vagy a bosszúvágy, azonban rendelkeznek fejlett érzékelőkkel és adatfeldolgozási képességgel, amelyek lehetővé teszik számukra, hogy hatékonyabbak és etikusabbak legyenek az emberekkel szemben a harci helyzetekben.

AUTONÓM DRÓNRENDSZEREK FEJLŐDÉSE ÉS A HUMANITÁRIUS JOG KÖZÖTTI KAPCSOLAT

Az autonóm drónok fontos igazságügyi és etikai kérdéseket vetnek fel a nem szándékos károkért való felelősséggel kapcsolatban.[26] A humanitárius jog (vagy háborús jog) a fegyveres konfliktusok során érvényesülő jogi keretet jelenti, amely szabályozza a harcoló felek magatartását, és megvédi a civil lakosságot valamint a háborút túlélte személyeket.

„A probléma nem a törvények hiánya, hanem a már meglévő nemzetközi jog széles körű értelmezése, amely szabályozza az erő alkalmazását a konfliktusövezetekben belül és azon kívül, ahol fegyveres drónok működnek.” [27]

Az autonóm drónrendszerek fejlődése komoly kihívások elé állítja a humanitárius jogot. Fejlődésük, miszerint képesek önálló döntéseket hozni és cselekedni, számos kérdést vet fel a humanitárius jog szempontjából.

Az önvezető harci repülőgépek (UAV) egyedi tulajdonságai, mint például a magas repülési magasság, hatékony információgyűjtési képesség és a civil lakosságra gyakorolt hatás, komplex kihívások elé állítják az ilyen fegyverek jogszerűségéről hozott döntéseket, és befolyásolják a repülőgépek üzemeltetői és a katonai célpontok közötti távolság tekintetében az nemzetközi jog és a humanitárius jog elveit is. [28]

Mivel a drónok egyre elterjedtebbek a modern katonai erők eszköztárában, fontos megvizsgálni, hogy a célzott, halálos támadásokra történő drónhasználat összhangban áll-e a fegyveres konfliktusok jogának szellemével és betartja-e annak szellemiségét (*ius in bello*)[29]:

- Először is, a humanitárius jog alapelvei között szerepel a megkülönböztetés elve, ami azt jelenti, hogy meg kell különböztetni a katonai célpontokat a civil személyektől. Az autonóm drónok esetében ez a képesség kihívást jelenthet, mivel képesek önállóan célpontokat azonosítani és támadást indítani. [29]
- Másodszor a nemzetközi jog összetett kérdéseket vet fel azzal kapcsolatban, hogy szabad-e célzott dróntámadásokat indítani a harcoló felek ellen. a humanitárius jogban szereplő arányosság elve azt jelenti, hogy a fegyverek használata során arányban kell állnia a célok eléréséhez szükséges katonai előnnyel és a civil veszteségek minimalizálásával. Az autonóm drónok képessége, hogy nagy pontossággal támadjanak célpontokat, segíthet az arányosság elvének betartásában, de ugyanakkor felmerülhet a kérdés, hogy az autonóm döntéshozatal megfelelően értékeli-e a környezeti és helyzetbeli tényezőket. [29]

Az, ami a katonák számára veszélytelen, nem feltétlenül jelenti azt, hogy az adott műveleti területen élők számára is az. A hadijog elsősorban a nem résztvevő civil lakosság épségét szolgálja, ezért a pilóta nélküli eszközöknek is inkább a konfliktus területén élők biztonságát kellene elősegíteniük. Ezen eszközöknek képeseknek kell lenniük erre a céllal, különösen bizonyos műveletek (például humanitárius segítségnyújtás) esetén.[30]

- Harmadszor, a humanitárius jogban szereplő felelősség és számadási kötelezettség elve alapján a felelősségre vonás és a jogi felelősség megállapítása fontos. Az autonóm drónok esetében felmerülhet a kérdés, hogy ki viseli a felelősséget, ha egy autonóm rendszer nem megfelelően értékeli a helyzetet vagy hibás döntést hoz.

Azonban az új és fejlettebb fegyverek megjelenése nem új kihívás a fegyveres konfliktusok történelmében. A technológiai fejlődés fokozatosan egyre kifinomultabb eszközöket hozott létre a harcban, miközben a használatukat szabályozó törvények általában jóval lemaradtak.[31]

A történelem során különböző időszakokban olyan fejlesztések, mint az íj, a lőpor, a géppuskák, a tankok, repülőgépek, mérgező gázok, nukleáris bombák és számos más halálos találmány véglegesen megváltoztatták a hadviselés jellegét, és szükségessé tették a csoportok és államok számára a fegyveres konfliktusokat szabályozó jogi keretek felülvizsgálatát.

A Vöröskereszt Nemzetközi Bizottságának (ICRC) Közgyűlésének készített időközi jelentésben, melynek témája a drónok használata a terrorizmusellenes műveletekben, számos olyan jogi kérdéseket azonosítottak, amelyekben jelenleg nincs egyértelmű nemzetközi konszenzus, vagy amelyekben a jelenlegi gyakorlatok és értelmezések megkérdőjelezzik a bevett jogi normákat.[32]

ÖSSZEGRÉS

Írásom fókuszában a hadviselés, terrorizmus és drónhasználat összetett és dinamikus kapcsolata állt. Részletesen vizsgáltam a drónok növekvő szerepét a terrorista tevékenységek támogatásában és a hadviselésben. Megállapítottam, hogy a drónok fejlődése lehetővé tette a terroristáknak, hogy hatékonyan és kreatívan használják ezeket az eszközöket támadások, megfigyelések és propaganda célokra. Emellett kiemeltem, hogy a drónok fokozott autonómiája és képességei új kihívásokat vetnek fel a nemzetbiztonság és az etikai kérdések terén.

Továbbá, rámutattam a terrorizmus és a drónhasználat közötti kölcsönhatásokra. A terrorizmus és az erőszakkal való fenyegetés lehetőségét biztosít a katonai beavatkozásra a politikai színtéren, ami jelentős hatással lehet a nemzetközi kapcsolatokra. Ugyanakkor, igyekeztem felhívni a figyelmet arra, hogy a katonai megoldás csupán egy eszköz a terrorizmus elleni küzdelemben, és hogy komplex megközelítésre van szükség, amely magában foglalja a politikai, gazdasági, diplomáciai és egyéb intézkedéseket.

Végző soron, rávilágítottam arra, hogy a terrorizmus, a hadviselés és a drónhasználat közötti kapcsolatok rendkívül összetettek és változóak. Fontos, hogy folyamatosan vizsgáljuk és értékeljük ezeket a kapcsolatokat annak érdekében, hogy megfelelő válaszokat és politikákat alakíthassunk ki a fenyegetések kezelésére. Az ilyen kihívásokon túlmenően sokkal nagyobb mértékű átláthatóságra van szükségünk a dróntámadások jogszerűségével kapcsolatban.

FELHASZNÁLT IRODALOM

- [1] Ember István, Szilágyi-Kiss Hajnalka: Drónok a Közel-Keleten, Műszaki Katonai Közlöny pp. 57, 31. évfolyam (2021) 1. szám 51–60. • DOI: 10.32562/mkk.2021.1.4 <https://folyoirat.ludovika.hu/index.php/mkk/article/view/4855/4379>
- [2] Vincenzo Bove: Beyond coups: terrorism and military involvement in politics: European Journal of International Relations 2020, Vol. 26(1), DOI: 10.1177/1354066119866499 <https://journals.sagepub.com/doi/pdf/10.1177/1354066119866499>

- [3] Kollár Csaba: A mesterséges intelligencia kapcsolata a humán biztonsággal, Nemzetbiztonsági Szemle MMXVIII/I, <https://folyoirat.ludovika.hu/index.php/nbsz/article/download/1508/826/5657>
- [4] Szternák György, Szternák Nóra, Bolgár Judit: A terrorizmussal kapcsolatos kutatások legújabb eredményei. Felderítő Szemle, Katonai Nemzetbiztonsági Szolgálat 2005 IV. évfolyam 4. szám <https://www.knbsz.gov.hu/hu/letoltes/fsz/2005-4.pdf>
- [5] Bolgár Judit nyá. ezredes, Dr. Szternák Nóra hadnagy, Dr. Szternák György ezredes: A Terrorizmussal kapcsolatos kutatások legújabb eredményei. pp. 5-61, Felderítő Szemle, IV. évfolyam 4. szám 2005. december <https://www.knbsz.gov.hu/hu/letoltes/fsz/2005-4.pdf>
- [6] Sebakov Márton Tibor: A terroristák drónhasználata (The Usage of Drones by Terrorists) Nemzetbiztonsági Szemle, 7. évfolyam (2019) 4. szám, pp. 30-43, DOI: 10.32561/n.sz.2019.4.3 <https://folyoirat.ludovika.hu/index.php/nbsz/article/view/829/3443>
- [7] Finszter Gábor: Biztonsági kihívások a 21. században. (2017) ISBN:9786155680502 <https://www.uni-nke.hu/document/uni-nke-hu/3.%20Szenes%20k%C3%B6nyv.%20k%C3%B6nyvr%C3%A9szlet.pdf>
- [8] Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016. 260–264. old. HU ISSN 1788-7895. ISBN 978-963-9816-34-3. <https://mek.oszk.hu/16100/16182/16182.pdf>
- [9] Autonóm off-road járművek, drón-rajok és kiberbiztonság https://gyartastrend.hu/cikk/autonom_off_road_jarmuvek_dron_rajok_es_kiberbiztonsag
- [10] Szávay István: Drónok elleni védekezés ipari létesítményekben, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi Intézet MSc diplomamunka pp.12.
- [11] Gyarmati József, Simó Réka: Autonóm terepjáró járművek katonai felhasználásának lehetőségei, HADITECHNIKA LV. évf. – 2021/1, DOI: 10.23713/HT.55.1.02, http://real.mtak.hu/121793/1/HT_2021-1_cikk_02.pdf
- [12] Szenes Zoltán: Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek 70-104.old. <https://m2.mtmt.hu/api/publication/3258112> Finszter G. Biztonsági kihívások a 21. században. (2017) ISBN:9786155680502
- [13] Szendrei Ferenc, Magyar Rendészet 2018/5. 77—91. 77 A szervezett bűnözés gazdasági háttere és a pénzmosás, http://real.mtak.hu/132752/1/MR_2018_5_e_5_Szendrei.pdf
- [14] Rada Máttyás, Vajda Viktor: A terrorizmus elleni küzdelem, avagy a 22-es csapdája, Külügyi Szemle, 2010 tavasz https://kki.hu/assets/upload/Kulugyi_Szemle_2010_01_A_terrorizmus_elleni_kezd.pdf
- [15] Németh József: Az iszlám alapú terrorizmus elleni küzdelemről, titkosszolgálati aspektusból, pp. 5-22, A KATONAI BIZTONSÁGI HIVATAL TUDOMÁNYOS TANÁCSÁNAK KIADVÁNYA https://www.knbsz.gov.hu/hu/letoltes/szsz/2006_2_szam.pdf
- [16] Kis-Benedek József: Az Iszlám Kalifátus és a globális dzsiháid új tendenciái, Hadtudomány 2014/3–4. http://real.mtak.hu/19065/1/2014_3_4_2.pdf

- [17] Rada Mátyás – Vajda Viktor: A terrorizmus elleni küzdelem, avagy a 22-es csapdája, Külügyi Szemle https://kki.hu/assets/upload/Kulugyi_Szemle_2010_01_A_terrorizmus_elleni_kezd.pdf
- [18] Gesztei László: A terrorizmus elleni küzdelem egyes jogi kérdései, Doktori értekezés Pécsi Egyetem ÁJK <https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/gesztei-laszlo/gesztei-laszlo-vedes-ertekezes.pdf>
- [19] Bendarzszevszkij Anton: Autonóm katonai rendszerek: elérkezett a büntetlen halál ideje, <https://index.hu/kulfold/2023/03/20/autonom-katonai-rendszerek-dronok-mesterseges-intelligencia/>
- [20] John Harper: Robotics and autonomus systems, National Defense [https://www.nationaldefensemagazine.org/articles/2021/5/27/pentagon-gets-\\$7-5-billion-for-unmanned-systems](https://www.nationaldefensemagazine.org/articles/2021/5/27/pentagon-gets-$7-5-billion-for-unmanned-systems)
- [21] Unmanned Systems Integrated Roadmap FY2011-2036 – USA Department of Defence, Ref.No. 11-S-3613 <http://info.publicintelligence.net/DoD-UAS-2011-2036.pdf>
- [22] Elbit System Ltd, Advanced Technology Center, autonóm műveleti hálózati megoldások <https://elbitsystems.com/product/legion-x/>
- [23] Elbit System Ltd, Advanced Technology Center, megoldások fejlett légi járművek védekezésére <https://elbitsystems.com/product/redrone/>
- [24] Bendarzszevszkij Anton: Autonóm katonai rendszerek: elérkezett a büntetlen halál ideje, <https://index.hu/kulfold/2023/03/20/autonom-katonai-rendszerek-dronok-mesterseges-intelligencia/>
- [25] Grossman, Nicholas (2018): Drones and Terrorism: Asymmetric Warfare and the Threat of Global Security-Drone Strikes. London, I.B. Tauris. pp. 99–104. DOI: [10.5040/9781350986169.ch-003](https://doi.org/10.5040/9781350986169.ch-003)
- [26] Anna Konnert, Tomasz Balcerzak: Military autonomous drones (UAVs) - from fantasy to reality. Legal and Ethical implications. Transportation Research Procedia 59 (2021) pp. 292–299, 10th International Conference on Air Transport – Published by ELSEVIER B.V, open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>), 10.1016/j.trpro.2021.11.121
- [27] Erdész Viktor: A mesterséges intelligencia felhasználási lehetőségei a korszerű nemzetbiztonsági hírszerző elemzés-értékelésben, Doktori (PhD) értekezés pp. 45, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola https://hdi.uni-nke.hu/document/hdi-uni-nke-hu/erdesz_viktor_ertekezes_tervezet.pdf
- [28] Sandra Krähenmann, Geneva Call, and George Dvaladze, Geneva Academy of International Humanitarian Law and Human Rights <https://www.genevacall.org/fr/humanitarian-concerns-raised-by-the-use-of-armed-drones/>
- [29] Ryan J. Vogel: Drone Warfare and the Law of Armed Conflict, 39 Denver Journal of International Law & Policy 101 (2010). <https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1230&context=djilp>
- [30] Varga Attila Ferenc: A drónok, mint a kockázatmentes hadviselés eszközei, Hadtudományi Szemle 2013- 6. évf. 2.sz, pp. 47 http://epa.oszk.hu/02400/02463/00015/pdf/EPA02463_hadtudomanyi_szemle_2013_2_044-058.pdf

- [31] Disruption Network Lab által Berlinben szervezett konferencia a drónokról [Khalil Dewan](https://globalvoices.org/2022/03/30/drone-warfare-can-international-humanitarian-law-catch-up-with-the-technology/) ügyvéddel és nyomozóval készült beszélgetés <https://globalvoices.org/2022/03/30/drone-warfare-can-international-humanitarian-law-catch-up-with-the-technology/>
- [32] <https://casebook.icrc.org/case-study/general-assembly-use-drones-counter-terrorism-operations>

**SMART BUILDINGS AND IOT:
A COMPREHENSIVE REVIEW OF
GLOBAL PRACTICES****OKOS ÉPÜLETEK ÉS AZ IOT:
A GLOBÁLIS GYAKORLATOK ÁTFOGÓ
ÁTTEKINTÉSE**SÁNDOR Barnabás¹ – RAJNAI Zoltán²**Abstract**

Smart buildings that use IoT technologies have revolutionized our interaction with the environment. This study explores the latest trends, challenges, benefits, and future developments in this field. By conducting a thorough literature survey, we have identified the critical applications, frameworks, protocols, and analytics techniques used in intelligent buildings across different regions. We also discuss how IoT impacts various aspects of building management, such as energy efficiency, occupant comfort, security, and maintenance. Finally, we provide insights into potential opportunities and research directions to advance knowledge about smart buildings combined with IoT innovations, which have the potential to revolutionize urban living standards worldwide.

Keywords

Smart Building, Internet of Things (IoT), Cybersecurity, Sustainability, Energy Efficiency

Absztrakt

Az IoT-technológiákat használó intelligens épületek forradalmasították a környezettel való interakciónkat. Ez a tanulmány a legújabb trendeket, kihívásokat, előnyöket és jövőbeli fejlesztéseket vizsgálja ezen a területen. Alapos szakirodalmi kutatás elvégzésével azonosítottuk a különböző régiókban az intelligens épületekben használt kritikus alkalmazásokat, keretrendszereket, protokollokat és adatelemzési technikákat. Kitérünk arra is, hogy az IoT hogyan befolyásolja az épületek irányításának különböző aspektusait, például az energiahatékonyságot, a benne tartózkodók kényelmét, a biztonságot és a karbantartást. Végezetül betekintést nyújtunk a lehetséges kutatási irányokba, hogy az IoT-innovációkkal felszerelt intelligens épületekkel kapcsolatos ismereteket továbbfejlesszük, amelyek világszerte forradalmasíthatják a városi élet színvonalát.

Kulcsszavak

Okos épületek, Dolgok internete (IoT), Kiberbiztonság, Fenntarthatóság, Energiahatékonyság

¹ sandor.barnabas@gmail.com | ORCID: 0000-0001-7133-8082 | PhD-Student, Óbuda University | Doktorandusz, Óbudai Egyetem

² rajnai.zoltan@bkg.uni-obuda.hu | ORCID: 0000-0002-9139-736X | Professor, Óbuda University | Egyetemi tanár, Óbudai Egyetem

BEVEZETÉS

A dolgok internetének (Internet of Things - IoT) intelligens épületekbe történő beépítése alapvetően átalakította az épített környezetek koncepcióját. Az okos épületek, más néven intelligens vagy összekapcsolt épületek, kihasználják az IoT-ben rejlő lehetőségeket, hogy rugalmasan reagáló és a benne tartózkodók jólétét, hatékonyságát elősegítő, energiahatékony tereket tervezzenek. Ez a kutatás az intelligens épületinfrastruktúra kialakítására irányuló világszintű koncepciókat és kialakításokat kívánja megvizsgálni és bemutatni az e területen megvalósuló élvonalbeli innovációk és kihívások elemzésével, miközben a jövőbeli fejlődési kilátásokat is bemutatja. Az IoT eszközök és rendszerek felgyorsult fejlődése és széles körű elfogadása elősegítette az intelligens épületek megjelenését, amelyek a dolgok internetének eszközeit, érzékelőit és aktorait beépítve adatokat gyűjtenek az épület teljesítményének optimalizálására, miközben javítják a felhasználói élményt. Az intelligens épületek olyan összekapcsolt rendszereket használnak, amelyek lehetővé teszik az akadálytalan kommunikációt és koordinációt a különböző épületkomponensek, például a világítás, a fűtési/hűtési rendszerek, a szellőztetőegységek, a biztonsági rendszerek és a foglaltságot figyelő rendszerek között. Következésképpen ezek az épületek képesek autonóm módon, valós időben szabályozni működésüket, ami figyelemre méltó javulást eredményez az energiahatékonysági szintek, a kényelmi biztonsági előírások és az általános működési hatékonyság terén. Kutatási célok az intelligens épületek és a IoT technológiákat alátámasztó alapvető koncepciók és építészeti keretek bemutatása, majd ezen technológiák mélyreható feltárása útján a globális gyakorlatok átfogó elemzése. Illetve, az intelligens épületek és az IoT-megoldások valós alkalmazásait és megvalósításainak vizsgálata és értékelése a különböző földrajzi régiókban. Az esettanulmányok, projektek és bevált gyakorlatok alapos vizsgálatával a kutatás célja, hogy bemutassa a hatékony telepítési stratégiákat és a múltbeli tapasztalatokból nyert kulcsfontosságú felismeréseket a jövőbeli telepítéshez.

AZ OKOS ÉPÜLET ÉS AZ IOT KAPCSOLATA

A dolgok internetének megjelenése a különböző ágazatokban történő kiterjedt integrációját eredményezte, ami az átalakító intelligens technológiák korszakát jelzi. Ennek a trendnek egyik jelentős haszonélvezője az építőipar. Ez a fejezet az intelligens épületek és az IoT bonyolult világába merül el, és mélyrehatóan feltárja ezek kölcsönhatását. Az intelligens épületek a modern építési gyakorlatok megtestesítői, amelyek fejlett technológiákat használnak az energiahatékonyság, a kényelem és az épület általános irányításának javítására. Működésükben központi szerepet játszik az IoT - egy innovatív technológia, amely megkönnyíti az összekapcsolt eszközök közötti adatcserét.

Az IoT integrálása az intelligens épületekbe a technológia és a szerkezeti tervezés érdekes keverékét kínálja, olyan intelligens szerkezeteket hozva létre, amelyek önállóan alkalmazkodnak a környezeti feltételekhez és a felhasználói igényekhez. Ez a fejezet megvilágítja ezeket a fogalmakat, részletes betekintést nyújt az intelligens épületek és az IoT meghatározásába, szinergikus működésükbe, valamint a mai digitális korban rejlő forradalmi lehetőségekbe.

Okosépület meghatározása

Az "okosépület" kifejezés, más néven intelligens épületek, az építés olyan innovatív megközelítését foglalja magában, amely harmonikusan integrálja a technológiát, az építőanyagokat és az építészeti tervezést. Ezeket a modern szerkezeteket az jellemzi, hogy képesek önállóan kezelni számos funkciót, növelve az épített környezet általános hasznosságát és alkalmazkodóképességét. Technológiai szempontból az intelligens épületek egymással összekapcsolt eszközök és rendszerek hálózatát foglalják magukban, többek között érzékelőket, aktorokat és épületirányítási rendszereket. Ezek a komponensek együttesen dolgoznak az adatok gyűjtése, elemzése és kezelése érdekében, ezáltal elősegítve az épület és a használói közötti dinamikus interakciót. Ez az adatvezérelt modell lehetővé teszi a különböző épületrendszerek, például a fűtés, szellőzés és légkondicionálás (HVAC), a világítás, a biztonság és az energiagazdálkodás automatizált vezérlését, amelyek mindegyike a használók igényeihez és preferenciáihoz igazodik.

Az okosépületek egyik fő alkotóelemei az IoT eszközök és rendszerek, amelyek lehetővé teszik a távfelügyeletet és -irányítást, a valós idejű elemzést és a jobb döntéshozatali folyamatokat. Az eszközök és rendszerek ilyen összekapcsolt kerete lehetővé teszi az adatok interneten keresztüli továbbítását és fogadását, ami számos innovatív és hatékony üzelmeltetési stratégia számára nyitja meg az utat. Lényeges annak elismerése is, hogy az intelligens épület fogalma túlmutat a puszta automatizáláson. Ezen épületek "okossága" azt bizonyítja, hogy képesek tanulni, alkalmazkodni és idővel optimalizálni működésüket, ami folyamatos javulást eredményez az energiahatékonyság, a fenntarthatóság és a lakók kényelme terén. Mint ilyenek, az intelligens épületek döntő előrelépést jelentenek a fenntartható és hatékony városfejlesztésre való törekvésünkben, és utat nyitnak egy olyan jövő felé, amelyet intelligens és érzékeny épített környezet jellemez.

Az IoT megértése

A dolgok internete (IoT) egy alapvető technológiai paradigmaváltás, amely a fizikai eszközök internetalapú hálózatokon keresztül történő összekapcsolását foglalja magában, ami egy kiterjesztett, adatcserére képes ökoszisztémát eredményez. Ez a technológiai keret hatalmas lehetőségeket rejt magában különböző ágazatokban, lehetővé téve a mindenütt jelenlévő számítástechnikát és platformot biztosítva az innováció számára. Az érzékelők és aktorok fizikai tárgyakba vannak beágyazva, és vezetékes vagy vezeték nélküli hálózatokon keresztül kapcsolódnak egymáshoz, szabványos és szabadalmaztatott protokollok segítségével. Ezek az eszközök adatokat generálnak a környezetről vagy állapotukról, amelyeket aztán feldolgoznak és elemeznek, hogy tájékoztassák a döntéshozatalt vagy automatizált műveleteket indítsanak el. Az IoT alkalmazásai sokrétűek és széleskörűek, az intelligens otthonoktól és az ipari automatizálástól kezdve az egészségügyi felügyeletig és a várostervezésig. Az egyik kiemelkedő alkalmazási terület az intelligens épületek, ahol az IoT kulcsfontosságúnak bizonyult az épületek működésének automatizálásában és az energiefelhasználás optimalizálásában.

Az intelligens épületekben az IoT eszközök jellemzően adatokat gyűjtenek, például a hőmérsékletről, a páratartalomról, a fényszintekről és a használati szokásokról. Ezeket az adatokat aztán az interneten keresztül továbbítják egy központi irányítási rendszerbe vagy felhőalapú platformra, ahol azokat elemzik, és aszerint cselekszenek. Az így nyert információk alapján a különböző épületrendszerek - például a fűtés, a világítás és a biztonság -

vezérlése dinamikusan alkalmazkodik az épület környezetében vagy a használatban bekövetkező változásokhoz. Lényegében az IoT a hétköznapi épületeket intelligens egységekké alakítja át, amelyek képesek kölcsönhatásba lépni a használókkal és a tágabb környezettel. Ez a paradigma a modern épületirányítási rendszerek sarokköve, amely jelentős javulást kínál az energiahatékonyság, a lakók kényelme és az üzemeltetés hatékonysága terén. Az IoT megvalósítása azonban nem mentes a kihívásoktól. Ezek közé tartoznak az adatbiztonsággal, a magánélet védelmével, az eszközök interoperabilitásával és a technikai összetettséggel kapcsolatos aggályok. Ezeknek a kérdéseknek a kezelése a területen folyó kutatás és fejlesztés tárgyát képezi.

Az okosépületek és az IoT metszete

Az intelligens épületek és az IoT konvergenciája kritikus fordulópontot jelent az épített környezet fejlődésében. Ez a metszéspont olyan épületeket eredményezett, amelyek nemcsak fejlett technológiákat testesítenek meg, hanem képesek kommunikálni, elemezni, tanulni és alkalmazkodni a bennük és körülöttük zajló különböző dinamikákhoz. Az IoT-keretrendszer lehetővé teszi, hogy ezek a rendszerek összekapcsolódjanak, és így olyan eszközök egységes hálózatát hozzák létre, amelyek képesek kommunikálni és együttműködni az épület teljesítményének javítása érdekében. Ez azt jelenti, hogy az egyik rendszerben, például a világításban végzett beállítások szinkronizálhatók más rendszerekkel, például a HVAC-rendszerrel, az általános energiahatékonyság és a kényelem optimalizálása érdekében.

Az IoT-képes rendszerek például érzékelhetik a foglaltsági szintek változásait, és reagálhatnak rájuk. Ha egy helyiség nincs elfoglalva, a rendszerek automatikusan tompítják a fényeket, csökkenthetik a hőmérsékletet, vagy kikapcsolhatják a nem létfontosságú eszközöket, ami jelentős energiamegtakarítást eredményez. Az IoT intelligens épületekbe történő integrálása továbbá elősegíti a prediktív karbantartást, amely stratégia az adattrendek felhasználásával előre jelzi, hogy egy épületrendszer várhatóan mikor fog meghibásodni. Ez lehetővé teszi a proaktív karbantartást, csökkentve az állásidőt és javítva a rendszer általános élettartamát és megbízhatóságát.

Felhasználói szinten az intelligens épületek és a dolgok internetének kereszteződése kibővítette az ember és az épület közötti interakciók körét. Okostelefonok vagy más felhasználói felületek segítségével irányíthatják az épület környezetének különböző aspektusait, javítva ezzel kényelmüket és termelékenységüket. Az intelligens épületek és az IoT egyesülése azonban kihívásokkal is jár, például az adatvédelem és adatbiztonság, az interoperabilitás, valamint a kiterjedt eszközhálózat kezelésének összetettsége miatt. E kihívások kezeléséhez szilárd technológiai megoldásokra és hatékony szakpolitikai keretekre van szükség.

GLOBALIS TRENDEK AZ OKOS ÉPÜLETEK ÉS IOT RENDSZEREK TERÉN

Az intelligens épületek és az IoT integrációja nem egy elszigetelt, egyetlen régióra korlátozódó jelenség, hanem világszerte elterjedt, mivel forradalmasítja az épített környezettel való interakcióinkat. E fejezet célja, hogy részletesen feltárja az intelligens épületek és az IoT globális gyakorlatát, kiemelve a különböző régiókban alkalmazott stratégiák, kihívások és sikerek sokféleségét. Az észak-amerikai kiterjedt intelligens városoktól az európai energiahatékony épületekig, Ázsia nyüzsgő, technológia által vezérelt metropoliszaitól

az ausztráliai fenntartható városfejlesztésekig az intelligens épületek és a dolgok internetének elterjedése egyszerre globális és helyi törekvés. Számptalan lehetőséget kínál, a fokozott energiahatékonyságtól és az üzemeltetési költségek megtakarításától kezdve a lakók kényelmének és termelékenységének javításáig. Ez a globális mozgalom azonban számos kihívással is küzd, többek között az adatvédelem és adatbiztonság, a technológiai szabványosítás és a pénzügyi korlátok terén.

Európa

Európa élen jár az IoT-technológiák intelligens épületeken belüli bevezetésében, amit átfogó szakpolitikák, finanszírozási kezdeményezések és szilárd technológiai infrastruktúra támogat. Az Európai Unió (EU) döntő szerepet játszott e fejlődés előmozdításában az energiahatékonyság, a fenntarthatóság és a digitális innováció fokozását célzó rendeleteivel és irányelveivel. Az egyik példaértékű irányelv, amely kiemeli a dolgok internetének az intelligens épületekbe történő integrálását, a 2018-ban felülvizsgált, az épületek energia-teljesítményéről szóló irányelv (EPBD). Az irányelv célja, hogy az európai épületek 2050-ig nagy energiahatékonyságú és szén-dioxid-mentes épületállományt alakítsanak ki [1].

Az EPBD az épületautomatizálási és -vezérlő rendszerek - amelyek magukban foglalják az IoT-eszközöket - telepítését szorgalmazza az épületgépészeti rendszerek optimális energiafelhasználás érdekében történő kezelésére, szabályozására és vezérlésére szolgáló intézkedésként. Ezen túlmenően a felülvizsgált irányelv bevezeti az "intelligens készlet" fogalmát, amely azt értékeli, hogy az épület képes-e a használat igényeihez igazítani működését, ezáltal javítva az energiahatékonyságot és az általános teljesítményt. Ezt különösen befolyásolja a dolgok internete, amely lehetővé teszi a felhasználók és az épületrendszerek közötti valós idejű interakciót.

Egy másik figyelemre méltó példa a Horizont 2020 program, amely finanszírozásának jelentős részét az intelligens épületek IoT-jének előmozdítására különítette el. Az olyan projektek, mint a SymbIoTe (Symbiosis of smart objects across IoT environments) és az AUTOPILOT (AUTOMated driving Progressed by the Internet Of Things) nagy hatással voltak az IoT elterjedésére az intelligens épületekben [2]. Egyes országok is magukévá tették ezt a tendenciát. Az Egyesült Királyságban például London városának "Smart City Initiative" elnevezésű kezdeményezése magában foglalta az IoT-technológiákkal felszerelt intelligens épületek fejlesztését. A kezdeményezés célja az energiafelhasználás optimalizálása, a kibocsátások csökkentése és a városon belüli általános életszínvonal javítása [3].

A skandináv régióban Dánia "intelligens hálózati stratégiája", amelynek célja, hogy 2020-ra 50%-os szélenergia-ellátást építsen be a hálózatba, szintén integrálja az IoT-t és az intelligens épületeket, hogy lehetővé tegye a keresletre való reagálást [4].

Számos további példa van arra, hogy Európa hogyan integrálta a dolgok internetét az intelligens épületek kontextusába. Íme néhány:

Magyarország: MOL Campus - 2022-ben nyitotta meg kaput Magyarország legzöldebb leginnovatívabb és legmagasabb épülete a MOL Campus, amely az IoT-technológia széles tárházát felhasználta a fenntarthatóság érdekében. Az épületautomatizálás kiterjed minden rendszerre az épületben, kezdve a HAVC, a világítás, az árnyékolás, a pakolás és az energiafelhasználás területére. Az integrált rendszereknek köszönhetően megszerezte a LEED Premium és BREAM Excellent minősítést, ami a közel 900 m² napelemnek, geotermikus energiának és a szürkevíz újrahasznosításnak köszönhet. [5]

Franciaország: Az IssyGrid projekt - Az IssyGrid projekt Issy-les-Moulineaux-ban, egy párizsi külvárosban példázza az intelligens épülettechnológiát [6]. A 2012-ben indult, szomszédsági léptékű projekt több épület energiafogyasztását kezeli, bevonva a helyi közösséget, vállalkozásokat és hatóságokat. Az IoT döntő szerepet játszik a környéken telepített számos érzékelő adatainak összegyűjtésével és feldolgozásával. Ezeket az adatokat elemzik az energiafogyasztás optimalizálása, a költségek csökkentése és a szénlábnyom csökkentése érdekében.

Németország: Fraunhofer Intézet - A németországi Fraunhofer Épületfizikai Intézet (IBP) olyan intelligens épületplatformot fejlesztett ki, amely az IoT-technológiát használja ki [7]. A platform érzékelők és eszközök egész sorának az épület infrastruktúrájába történő integrálásával valós idejű adatfigyelést és -elemzést biztosít, lehetővé téve az optimalizált energiafelhasználást, a beltéri levegő minőségének javítását és a lakók kényelmének növelését. A platform megkönnyíti a prediktív karbantartást is azáltal, hogy a potenciális problémákat még azok eszkalálódása előtt azonosítja, ezáltal csökkentve az állásidőt és a karbantartási költségeket.

Hollandia: The Edge - Az amszterdami The Edge-t a világ legfenntarthatóbb és leginnovatívabb irodaházaként emlegetik [8]. Az IoT kulcsfontosságú szerepet játszik a működésében. Az épületben több ezer érzékelő van elhelyezve, amelyek adatokat gyűjtenek a foglaltságról, a fényről, a hőmérsékletről, a páratartalomról és a CO₂-szintről. Ezek az adatok tájékoztatják az épületirányítási rendszert, amely így képes a környezetet a lakók komfortérzetének növelése és az energiahatékonyság optimalizálása érdekében beállítani. Ezen túlmenően a lakók egy okostelefon-alkalmazás segítségével interakcióba léphetnek az épülettel, hogy személyre szabhassák a munkaterületük körülményeit.

Ázsia

Ázsiában, ahol a világ leggyorsabban növekvő gazdaságai közül sokan élnek, jelentős fejlődés tapasztalható az intelligens épületek és az IoT terén. A gyors urbanizáció, valamint a fenntarthatóságra és a digitalizációra való fokozott összpontosítás az egész régióban élvonalbeli intelligens épületek fejlesztését ösztönözte.

Japán: NTT Facilities - Japánban, a világ egyik vezető technológiai központjában az NTT Facilities Inc. iparági úttörő szerepet tölt be az IoT-technológiákat zökkenőmentesen integráló intelligens épületek fejlesztésében [9]. Figyelemre méltó példa erre a tokiói irodaházuk. Ez IoT-érezékelők egész sorával van felszerelve, amelyek valós idejű adatokat gyűjtenek különböző paraméterekről, például a hőmérsékletről, a páratartalomról, a fényszintről és a foglaltságról. Ezek az adatok egy központi irányítási rendszerbe kerülnek, amely optimalizálja a HVAC-, a világítási és egyéb rendszereket, jelentős energiamegtakarítást érve el és növelve a használók kényelmét. Az épület továbbá az IoT-t használja a prediktív karbantartáshoz, így csökkentve a javítási költségeket és javítva a rendszer megbízhatóságát.

Szingapúr: Fusionopolis - Szingapúr, amely a technológiai bátorságáról és az intelligens városi kezdeményezéseiről ismert, élen jár az intelligens épülettechnológiák bevezetésében. A Fusionopolis, a JTC Corporation által kifejlesztett kutatási és fejlesztési komplexum példaként szolgál az intelligens épületek példájára [10]. Az integrált IoT-érezékelők figyelemmel kísérik a környezeti feltételeket és a használati szokásokat, elősegítve az energiafel-

használás és a működési hatékonyság optimalizálását. A komplexum fejlett biztonsági rendszerrel is rendelkezik, amelyet IoT-képes eszközök működtetnek, amelyek valós idejű felügyeletet és beléptetés-ellenőrzést biztosítanak.

Kína: Shanghai Tower - Kínában a Shanghai Tower, a világ egyik legmagasabb épülete az intelligens épületek tervezésének és megvalósításának megtestesítője [11]. A 632 méter magas felhőkarcoló IoT-érzékelők hatalmas hálózatát alkalmazza, amelyek különböző épületrendszereket felügyelnek és vezérelnek, beleértve a levegő minőségét, az energiafelhasználást, a világítást és a biztonságot. Intelligens épületirányítási rendszere valós idejű adatokat használ a rendszerek és eszközök összetett hálózatának kezelésére, ami lenyűgöző energiahatékonyságot és magas szintű kényelmet biztosít a lakók számára.

Észak-Amerika

Észak-Amerika, különösen az Egyesült Államok és Kanada, jelentős mértékben hozzájárult az IoT-technológiák intelligens épületekben történő fejlesztéséhez és alkalmazásához. Az intelligens városok térnyerése, valamint a fenntarthatóságra és az energiahatékonyságra való nagyfokú összpontosítás katalizálta a technológiák integrálását a régió épített környezetébe.

Egyesült Államok: The Edge, Boston - Az Egyesült Államokban Boston városa ad otthont a "The Edge" amerikai megfelelőjének, egy korszerű intelligens épületnek, amely fenntartható tervezéséről és IoT-integrációjáról ismert. Ez az épület tele van több ezer érzékelővel, amelyek a fénytől és a hőmérséklettől kezdve a foglaltságon át az energiafelhasználásig mindent nyomon követnek [12]. Ezeket az adatokat valós időben elemzik és reagálnak rájuk, így biztosítva az optimális energiafelhasználást, növelve a lakók kényelmét és javítva az épület általános működési hatékonyságát. A lakók egy erre a célra kifejlesztett okostelefon-alkalmazás segítségével interakcióba is léphetnek az épülettel, így környezetük különböző aspektusait, például a világítást és a hőmérsékletet is szabályozhatják.

Egyesült Államok: PNC Tower, Pittsburgh - Egy másik kiemelkedő példa az Egyesült Államokban a pittsburghi PNC Tower, amelyet gyakran a világ "legzöldebb felhőkarcolójának" tartanak. Ez az épület számos IoT-érzékelőt tartalmaz, amelyek figyelik és szabályozzák a beltéri levegő minőségét, a hőmérsékletet és a fényviszonyokat. A begyűjtött adatok alapján egy természetes szellőztető rendszer, egy dupla héjú homlokzat és egy napkollektoros kémény működik, ami hozzájárul a kivételes energiahatékonysághoz és a lakók kényelméhez [13].

Kanada: Telus Garden, Vancouver - Kanadában az egyik figyelemre méltó példa a vancouveri Telus Garden. Ez a vegyes használatú fejlesztés a fenntarthatóság és a digitális innováció iránti elkötelezettségéről ismert. Az IoT kulcsszerepet játszik az épület energiafogyasztásának kezelésében, az érzékelők valós idejű adatokat szolgáltatnak a környezeti feltételekről és a foglaltsági szintekről. Ezeket az információkat a különböző épületrendszerek, köztük a világítás, a fűtés és a légkondicionálás optimalizálására használják fel, ami jelentős energiamegtakarítást és az épület szén-dioxid-kibocsátásának csökkentését eredményezi [14].

AZ OKOS ÉPÜLETEK ÉS AZ IOT ELÉNYEI

Az IoT technológia az intelligens épületekbe való beépítése drámaian forradalmasította az épített környezettel való interakciónkat. Ez a paradigmaváltás számtalan olyan előnnyel jár, amelyek túllépnek az energiahatékonyság és a fenntarthatóság hagyományos határain, és magukban foglalják a fokozott kényelmet, a termelékenység javulását és az üzemeltetési költségek megtakarítását. E fejezet célja, hogy mélyrehatóan feltárja ezeket az előnyöket, megvilágítva az IoT-alapú intelligens épületek átalakító hatását a különböző érdekeltekre, köztük az épületek használóira, a létesítményüzemeltetőkre és a társadalom egészére.

Az intelligens épületek és a dolgok internetének konvergenciája hatalmas lehetőségeket rejt magában, kezdve az épületrendszerek granulás ellenőrzésétől az adatelemzésen keresztül történő értékes információk kinyeréséig. Ez lehetővé teszi a statikus, nem reagáló épületek helyett a dinamikus, intelligens szerkezetek felé való elmozdulást, amelyek képesek tanulni, alkalmazkodni és reagálni a lakók és a környezet változó igényeihez. Ezen előnyök megvalósítása azonban nem mentes a kihívásoktól.

Energiahatékonyság

Az IoT, intelligens épületekbe történő integrálásából származó egyik legjelentősebb előny az energiahatékonyság. Az energiafogyasztás optimalizálása nemcsak az üzemeltetési költségeket csökkenti, hanem az energiatermeléshez kapcsolódó üvegházhatású gázok kibocsátásának mérséklésével a környezeti fenntarthatósághoz is hozzájárul. Az IoT az intelligens épületekben való felhasználása túlmutat az említett példákön. A gépi tanulási algoritmusok és a prediktív elemzések kihasználásával az IoT új magasságokba emelheti az energiahatékonyságot.

Előrejelző karbantartás és energiahatékonyság - Az IoT lehetővé teszi a prediktív karbantartást, ami jelentősen hozzájárulhat az energiahatékonysághoz. Az épületberendezések (pl. HVAC-rendszerek, liftek, világítási rendszerek) teljesítményének folyamatos nyomon követésével az IoT-eszközök felismerhetik az energiapazarláshoz vezető hatástalanságokat vagy meghibásodásokat [15]. Például egy HVAC-rendszer energiafogyasztási mintázatának enyhe eltérése potenciális hibára utalhat. Az ilyen rendellenességek korai felismerésével a megelőző karbantartás megelőzheti az energiapazarlást és csökkentheti a karbantartási költségeket.

Igényre reagálás és energiahatékonyság - Az IoT a keresletre reagáló programokon keresztül az energiahatékonyságot is növelheti. Ezekben a programokban az épületek az energiahálózatból érkező jelzésekre, például magas villamosenergia-árakra vagy csúcskeresleti időszakokra reagálva módosíthatják energiafogyasztásukat. Például a keresleti csúcsidezőszakokban egy épület automatikusan csökkentheti energiafogyasztását a világítás lehalkításával vagy a HVAC-rendszer beállításával. Ez nemcsak az energiahatékonysághoz járul hozzá, hanem az elektromos hálózat stabilitásának fenntartásához is.

Foglaltság-alapú vezérlés és energiahatékonyság - A foglaltság-alapú vezérlés egy másik terület, ahol az IoT növelheti az energiahatékonyságot. Az IoT-érzékelőkkel történő foglaltsági minták megfigyelésével az épületrendszerek a lakók igényeihez igazíthatók. Például a világítás és a HVAC-rendszerek kikapcsolhatók vagy energiatakarékos üzemmódba állíthatók a nem foglalt helyiségekben, ezáltal csökkentve az energiapazarlást.

Adatelemzés és energiahatékonyság - Végül az IoT-rendszerekben alkalmazott adatelemzés feltárhatja az energiafogyasztás rejtett hatékonysági hiányosságait. Az IoT-eszközök által generált nagy mennyiségű adat elemzésével az épületüzemeltetők olyan mintákat és trendeket is azonosíthatnak, amelyek a felszíni megfigyelésből nem feltétlenül tűnnek fel. Ezek a meglátások informálhatják az energiahatékonysági stratégiákat, ami hatékonyabb energia-gazdálkodást és energiatakarékosságot eredményezhet.

Magasabb szintű komfort

A dolgok internetének szerepe az intelligens épületek lakókomfortjának javításában a beltéri környezet különböző aspektusaira is kiterjed. Itt mélyebben megvizsgáljuk, hogy az IoT hogyan járul hozzá ehhez a szempontoz. [16]

Zaj- és fény szabályozás - A zaj és a világítás jelentős tényezők, amelyek befolyásolják az épületben tartózkodók kényelmét. Az IoT-eszközök képesek a zajszintet és a világítási körülményeket valós időben nyomon követni és szabályozni, biztosítva, hogy azok a komfortküszöbértékeken belül maradjanak [17]. Az amszterdami Edge például intelligens LED-es fénypaneleket használ, amelyek a napszak és a természetes fény mennyisége alapján automatikusan beállítják a fényerőt és a színhőmérsékletet, így kényelmes, vizuálisan kellemes környezetet teremtenek.

Levegőminőség-felügyelet és –szabályozás - A levegő minősége kulcsfontosságú szerepet játszik az épületben tartózkodók egészségében és kényelmében. A rossz beltéri levegőminőség kellemetlen érzést és káros egészségügyi hatásokat, például fejfájást, fáradtságot és légzési problémákat okozhat. Az IoT-érzékelők különböző levegőminőségi paramétereket, például a CO₂-szintet, a részecskéket és az illékony szerves vegyületeket (VOC) képesek monitorozni, lehetővé téve a szellőzőrendszerek valós idejű vezérlését az egészséges beltéri levegőminőség fenntartása érdekében. A korábban említett Shanghai Tower remek példa erre a megvalósításra.

Személyre szabott kényelem az IoT-vel - Az IoT nagyobb fokú személyre szabhatóságot tesz lehetővé a lakókomfortban. A hőmérsékletre, fényre és egyéb környezeti paraméterekre vonatkozó egyéni preferenciák nyomon követésével az IoT-rendszerek automatikusan beállíthatják ezeket a tényezőket, hogy megfeleljenek az egyes lakók egyedi kényelmi igényeinek. Ez a funkció a The Edge-ben látható, ahol a lakók egy alkalmazás segítségével személyre szabhatják munkaterületük körülményeit.

Biztonság és védelem

Az IoT az intelligens épületekbe történő integrálása számos lehetőséget kínál a biztonság és a védelem fokozására mind a fizikai, mind a digitális térben. Az épületrendszerek valós idejű felügyeletének, vezérlésének és automatizálásának lehetővé tételével az IoT jelentősen hozzájárulhat az emberek, az eszközök és az adatok védelméhez ezekben az épületekben.

Fizikai biztonság - Az IoT-technológiák jelentősen növelhetik a fizikai biztonságot az intelligens épületekben. Az IoT-alapú felügyeleti rendszerek például átfogó felügyeleti képességeket biztosíthatnak, és a jogosulatlan tevékenység és a potenciális fenyegetések azonnali észlelésével fokozhatják a biztonságot [18]. Hasonlóképpen, az IoT-érzékelők figyelemmel kísérhetik az épületek szerkezeti állapotát, észlelve az olyan rendellenességeket,

amelyek olyan lehetséges veszélyekre utalhatnak, mint a szerkezeti gyengeségek, szivárgások vagy tűzveszély. Az IoT a vészhelyzetekben is hozzájárulhat a biztonsághoz. Tűz esetén például az IoT-rendszerek riasztást indíthatnak, értesíthetik a segélyszolgálatokat, és valós idejű adatokkal segíthetik az evakuálást [19]. A dolgok internete továbbá javíthatja az egészséget és a biztonságot a környezeti paraméterek, például a levegőminőség, a fényviszonyok vagy a hőmérséklet nyomon követésével, biztosítva, hogy azok a kényelmi és biztonsági küszöbértékeken belül maradjanak.

Kiberbiztonság - A kiberbiztonság kulcsfontosságú kérdéssé válik, ahogy az intelligens épületek egyre inkább összekapcsolódnak és adatközpontúvá válnak. Az épület IoT-hálózatának minden egyes csatlakoztatott eszköze potenciális belépési pontot jelent a kibertámadások számára, ami adatszegésekhez, működési zavarokhoz vagy más csatlakoztatott rendszerek veszélyeztetéséhez vezethet [20]. Megfelelő kezelés esetén azonban az IoT a digitális biztonságot is fokozhatja. Például a fejlett titkosítási technológiák, a biztonságos kommunikációs protokollok és a szigorú hozzáférés-ellenőrzési intézkedések megvédhetik az adatokat és megakadályozhatják a jogosulatlan hozzáférést. Emellett a hálózati tevékenység folyamatos nyomon követése lehetővé teszi a potenciális kiberfenyegetések korai észlelését és mérséklését. Ezenkívül a rendszeres szoftverfrissítésekkel orvosolhatók az azonosított sebezhetőségek, és megerősíthető a dolgok internetére épülő rendszerek biztonsága.

KIHÍVÁSOK ÉS LEHETSÉGES MEGOLDÁSOK

Bár az IoT hatalmas lehetőségeket rejt magában az intelligens épületek forradalmasítására, nem mentes a kihívásoktól. Az IoT-technológiák épített környezetbe való integrálása összetett problémákat vet fel, többek között technikai, biztonsági, adatvédelmi és szabályozási kérdéseket. Ez a fejezet részletesen megvizsgálja ezeket a kihívásokat, és megvitatja a problémák kezelésére szolgáló lehetséges megoldásokat. Ezzel összefüggésben az egyes kihívások részletes elemzését mutatjuk be, a jelenlegi tudományos kutatásokra és ipari gyakorlatokra alapozva. Célunk, hogy rávilágítsunk azokra a nehézségekre, amelyeket az IoT az intelligens épületekbe történő integrálása jelent, és feltárjuk az e problémák enyhítésére javasolt vagy megvalósított innovatív megoldásokat.

Adatvédelem és kiberbiztonság

Az intelligens épületekben az IoT-technológiák elterjedése számos lehetőséget és aggályt vet fel, amelyek közül az adatvédelem és a kiberbiztonság a legkiemelkedőbbek. Ezek a kérdések különösen fontosak az intelligens épületekben található IoT-eszközök által gyűjtött, tárolt és feldolgozott érzékeny adatok hatalmas mennyisége miatt.

Adatvédelem - Az intelligens épületek korában az adatvédelem jelentős aggodalomra ad okot. Az IoT-eszközök hatalmas mennyiségű adatot gyűjtenek, a környezeti paraméterektől (hőmérséklet, páratartalom, fényszintek) kezdve az olyan érzékeny adatokig, mint a személyes preferenciák, viselkedési minták és használati ütemtervek. Ha ezeket az adatokat nem kezelik megfelelően, rosszindulatú célokra lehet felhasználni, ami jelentős adatvédelmi kockázatot jelent az épületek lakói számára [21]. E kockázatok mérséklésére számos stratégia alkalmazható. Például a beépített adatvédelem elveinek elfogadása biztosíthatja, hogy az IoT-eszközök teljes életciklusa során figyelembe vegyék az adatvédelmet. Ez magában foglalja az adatok anonimizálását, ahol ez lehetséges, szigorú hozzáférés-ellenőrzéseket,

valamint átláthatóságot az összegyűjtött adatok és azok felhasználásának módja tekintetében.

Kiberbiztonság - Az intelligens épületek az IoT-eszközök összekapcsolt jellege és az általuk tárolt értékes adatok miatt a kibertámadások elsődleges célpontjai. A kibertámadások súlyos következményekkel járhatnak, az adat- és adatvédelmi jogsértésektől kezdve az üzemzavarokon át a fizikai károkozásig. Az ilyen incidensek megelőzése érdekében átfogó kiberbiztonsági intézkedéseket kell végrehajtani. Ezek az intézkedések magukban foglalják a biztonságos kommunikációs protokollokat, a fejlett titkosítási technológiákat és az időben történő szoftverfrissítéseket. Emellett a dolgok internetére épülő eszközöket folyamatosan figyelemmel kell kísérni, hogy a potenciális fenyegetéseket azonnal észleljék és reagáljanak rájuk [20][22].

Világszerte számos intelligens épületben sikeresen hajtottak végre adatvédelmi és kiberbiztonsági intézkedéseket. Az amszterdami The Edge például biztonságos kommunikációs protokollokat és szigorú hozzáférés-ellenőrzést alkalmaz az adatok védelme és az illetéktelen hozzáférés megakadályozása érdekében. Emellett az épület lakóit tájékoztatják arról, hogy milyen adatokat gyűjtenek és hogyan használják fel, ezzel is demonstrálva az átláthatóság és a magánélet védelme iránti elkötelezettséget [8].

Műszaki kihívások

Az IoT-technológiák intelligens épületekbe történő integrálása jelentős technikai nehézségeket jelent, amelyek e rendszerek összekapcsolt jellegéből, valamint az érintett eszközök és technológiák sokféleségéből adódnak.

Interoperabilitás és szabványosítás - Az egyik fő technikai kihívás az IoT-eszközök interoperabilitása. Mivel számos gyártó gyárt különböző kommunikációs protokollokat és adatformátumokat használó eszközöket, az eszközök közötti zökkenőmentes interakció biztosítása nem triviális feladat. Ezt az interoperabilitási problémát súlyosbítja az egyetemes IoT-szabványok hiánya, ami olyan kompatibilitási problémákhoz vezet, amelyek akadályozhatják az IoT-rendszerek integrációját és működését az intelligens épületekben [23]. A lehetséges megoldások közé tartozik a nyílt forráskódú platformok és szabványos kommunikációs protokollok elfogadása, amelyek javíthatják a különböző gyártók eszközei közötti átjárhatóságot. Olyan szervezetek, mint az Open Connectivity Foundation (OCF) és a Zigbee Alliance dolgoznak az IoT-eszközök nyílt szabványainak létrehozásán és népszerűsítésén, amelyek jelentősen hozzájárulhatnak az interoperabilitási problémák megoldásához [24].

Hálózat- és adatkezelés - Egy másik technikai komplexitás a nagy IoT-hálózatok és az általuk generált hatalmas adatmennyiségek kezeléséből adódik. A több száz vagy akár több ezer eszközből álló hálózat megbízható működésének biztosítása az eszközök valós idejű adatainak kezelése mellett megbízható hálózati és adatkezelési rendszereket igényel [18]. A fejlett adatelemző eszközök, a felhőalapú számítástechnika és az edge computing technológiák segíthetnek az IoT-eszközök által generált adatok mennyiségének, sebességének és változatosságának kezelésében. Továbbá az öndiagnosztikára és automatikus konfigurációra képes hálózatkezelési rendszerek növelhetik a nagy IoT-hálózatok megbízhatóságát és hatékonyságát

Teljesítmény- és energiagazdálkodás - A teljesítmény- és energiagazdálkodás egy másik jelentős technikai kihívás. Sok IoT-eszköz akkumulátorral működik, és nehezen hozzáférhető helyeken található, ami miatt a gyakori akkumulátorcseréje nem praktikus. Ezért az energiafelhasználás optimalizálása az akkumulátor élettartamának meghosszabbítása érdekében kulcsfontosságú. Az IoT-eszközök energiaellátására olyan energia-nyerési technológiák alkalmazhatók, mint a napenergia, a rezgési energia vagy a hőenergia kinyerése. Emellett az alacsony fogyasztású kommunikációs protokollok és energiahatékony algoritmusok segíthetnek az energiafogyasztás csökkentésében és az akkumulátor élettartamának meghosszabbításában [25].

Összefoglalva, bár a dolgok internetének az intelligens épületekbe való integrálása jelentős kihívásokat jelent, a folyamatban lévő kutatási és fejlesztési erőfeszítések ígéretes megoldásokat kínálnak. A sikeres integráció és üzemeltetés érdekében azonban elengedhetetlen, hogy ezeket a kihívásokat figyelembe vegyük az intelligens épületek IoT-rendszereinek tervezése és megvalósítása során.

KÖVETKEZTETÉSEK ÉS JÖVŐBELI IRÁNYOK

Kutatásunk az IoT technológiával integrált intelligens épületek jelenlegi globális helyzetének kimerítő feltárását mutatta be. A kutatás elmélyült az IoT-ban és az intelligens épületek újradefiniálásában rejlő mélyreható lehetőségekben. Megvizsgálta a különböző földrajzi régiókban történő kialakítását, és felvázolta az általa kínált előnyöket. Részletes tudományos értekezésen keresztül vizsgáltuk az intelligens épületek jelentését és az IoT szerepét ezen infrastruktúrák fejlesztésében. Megállapításra került a két fogalom közötti sarkalatos metszéspontot, hangsúlyozva, hogy az IoT hogyan segíti elő az intelligens épületek intelligens, autonóm funkcióit, hozzájárulva az energiahatékonyasághoz, a kényelemhez, a biztonsághoz és a védelemhez. A globális gyakorlatok szegmens az IoT intelligens épületekbe történő integrációjának földrajzi vizsgálatát nyújtotta, Európára, Ázsiára és Észak-Amerikára összpontosítva. Kiemeltük az IoT-t különböző célokra használó épületek konkrét példáit, bemutattva, hogy a különböző régiókban milyen egyedi megközelítéseket alkalmaznak az IoT-integrációra, és hogyan kezelik a régióspecifikus kihívásokat.

Ezt követően bemutatásra került az IoT intelligens épületekbe történő integrációjának különböző előnyeit, kiemelve olyan szempontokat, mint az energiahatékonyaság, a lakók kényelmének javítása, a fokozott biztonság és a védelem. Kitértünk az adatvédelem és a kiberbiztonság témájára is, és elmélyedtünk az e téren fennálló összetettségben és árnyalatokban. A kihívások és a lehetséges megoldások kezelése során bemutatásra került az IoT intelligens épületekbe történő integrációjával kapcsolatos technikai összetettséget. Kitértünk az interoperabilitás, a szabványosítás, a hálózat- és adatkezelés, valamint a teljesítmény- és energiagazdálkodás kérdéseire. Minden egyes kihívás esetében potenciális megoldásokat és ígéretes trendeket ajánlottunk fel, amelyek enyhíthetik a problémákat.

Összefoglalva, ez a kutatás felvázolta az intelligens épületek IoT-integrációjának jelenlegi helyzetét, globális perspektívát nyújtva a gyakorlatokról, előnyökről, kihívásokról és lehetséges megoldásokról. Ez egy gyorsan fejlődő terület, amely hatalmas lehetőségeket rejt magában az épített környezetünk, valamint az élet- és munkamódszereink átalakításában. A kutatás előrehaladásával és az innovatív megoldások megjelenésével a teljesen integrált, intelligens és fenntartható intelligens épületek víziója egyre közelebb kerül a valósághoz.

FELHASZNÁLT IRODALOM³

- [1] „AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/844 IRÁNYELVE”. <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A32018L0844> (elérés 2023. május 22.).
- [2] J. Allmendinger, S. Wyatt, R. Veugelers, M. Caball, és R. Burmanjer, „Horizon 2020”. 2013. doi: 10.1037/e503552014-018.
- [3] G. Contributor, „City of London smart city initiative”, *Smart Energy International*, 2020. április 3. <https://www.smart-energy.com/policy-regulation/city-of-london-smart-city-initiative/> (elérés 2023. május 22.).
- [4] L. Schick és C. Gad, „Flexible and inflexible energy engagements—A study of the Danish Smart Grid Strategy”, *Energy Res. Soc. Sci.*, köt. 9, o. 51–59, 2015.
- [5] „MOL Campus”. <https://molcampus.hu/sustainability> (elérés 2023. május 22.).
- [6] C. Gauthier és B. Gilomen, „Business models for sustainability: Energy efficiency in urban districts”, *Organ. Environ.*, köt. 29, sz. 1, o. 124–144, 2016.
- [7] D. Comin, G. Trumbull, és K. Yang, „Fraunhofer: Five Significant Innovations”, *Driv. Compet.*, o. 445–468, 2016.
- [8] A. Jalia és M. Ramage, „The Edge, Amsterdam”.
- [9] A. Harrison, E. Loe, és J. Read, *Intelligent buildings in south East Asia*. Taylor & Francis, 2005.
- [10] F. Chang és D. Das, „Smart nation Singapore: Developing policies for a citizen-oriented smart city initiative”, *Dev. Natl. Urban Policies Ways Forw. Green Smart Cities*, o. 425–440, 2020.
- [11] J. Xia, D. Poon, és D. Mass, „Case Study: Shanghai Tower”, *CTBUH J*, köt. 2010, o. 12–18, 2010.
- [12] R. J. Lea, „Smart cities: An overview of the technology trends driving smart cities”, 2017.
- [13] B. Tranel és H. Ko, „Designing a Data-Driven, Humanistic High-Rise”, *CTBUH J*, sz. 2, o. 12–19, 2016.
- [14] H. H. Yücel Yıldırım, A. B. Gültekin, és H. Tanrıvermiş, „An Examination of the Energy-Efficient High-Rise Building Design”, előadás Proceedings of 3rd International Sustainable Buildings Symposium (ISBS 2017) Volume 2 3, Springer, 2018, o. 158–175.
- [15] D.-M. Han és J.-H. Lim, „Smart home energy management system using IEEE 802.15. 4 and zigbee”, *IEEE Trans. Consum. Electron.*, köt. 56, sz. 3, o. 1403–1410, 2010.
- [16] H. Alwaer és D. Clements-Croome, „Key performance indicators (KPIs) and priority setting in using the multi-attribute approach for assessing sustainable intelligent buildings”, *Build. Environ.*, köt. 45, sz. 4, o. 799–807, 2010.
- [17] D. Clements-Croome, „Sustainable intelligent buildings for people: A review”, *Intell. Build. Int.*, köt. 3, sz. 2, o. 67–86, 2011.
- [18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, és M. Ayyash, „Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, *IEEE Commun. Surv. Tutor.*, köt. 17, sz. 4, o. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

- [19] J. Granjal, E. Monteiro, és J. Sá Silva, „Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, *IEEE Commun. Surv. Tutor.*, köt. 17, sz. 3, o. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.
- [20] B. Sándor és Z. Rajnai, „Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View”, *Interdiscip. Descr. Complex Syst. INDECS*, köt. 21, sz. 2, o. 141–147, 2023.
- [21] R. H. Weber, „Internet of Things–New security and privacy challenges”, *Comput. Law Secur. Rev.*, köt. 26, sz. 1, o. 23–30, 2010.
- [22] R. Roman, J. Zhou, és J. Lopez, „On the features and challenges of security and privacy in distributed internet of things”, *Comput. Netw.*, köt. 57, sz. 10, o. 2266–2279, 2013.
- [23] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, és D. Savio, „Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services”, *IEEE Trans. Serv. Comput.*, köt. 3, sz. 3, o. 223–235, júl. 2010, doi: 10.1109/TSC.2010.3.
- [24] A. Nugur, M. Pipattanasomporn, M. Kuzlu, és S. Rahman, „Design and Development of an IoT Gateway for Smart Building Applications”, *IEEE Internet Things J.*, o. 1–1, 2018, doi: 10.1109/IIOT.2018.2885652.
- [25] A. Le, J. Loo, A. Lasebae, M. Aiash, és Y. Luo, „6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach”, *Int. J. Commun. Syst.*, köt. 25, sz. 9, o. 1189–1212, 2012.

**INFORMATION SECURITY OF
PASSENGER VEHICLES FROM THE
PERSPECTIVE OF INFORMATION
SECURITY EXPERTS****A SZEMÉLYGÉPJÁRMŰVEK
INFORMÁCIÓBIZTONSÁGA AZ
INFORMÁCIÓBIZTONSÁGI SZAKÉRTŐK
SZEMSZÖGÉBŐL**HEGYI Henrietta¹**Abstract**

Internet-connected passenger vehicles face similar risks as mobile phones, but unauthorized access to vehicle systems can pose greater risks to users. Modern passenger vehicles are capable of connecting to the internet and receiving messages that contain various instructions. The aim of this study is to explore the information security challenges related to passenger vehicles and formulate recommendations regarding the practical application of the current regulatory environment. To understand this complex issue, a qualitative research methodology was employed through expert in-depth interviews. The proper state and practical implementation of regulations are key to protecting user data and minimizing the risk of unauthorized access. The recommendations presented in this study support the development of the regulatory environment in the field of automotive manufacturing..

Keywords

IoT, passenger vehicle, information security, security standards, cybersecurity

Absztrakt

Az internetre csatlakozó járművek hasonló veszélyekkel néznek szembe, mint a mobiltelefonok, de előbbieket meghibásodása nagyobb kockázatot jelenthet a felhasználók számára. A modern személygépjárművek képesek kapcsolódni az internethez és üzeneteket fogadni, amelyek különböző utasításokat tartalmaznak. A tanulmány célja a személygépjárművekkel kapcsolatos információbiztonsági kihívások feltárása és a jelenlegi szabályozási környezet gyakorlati alkalmazásával kapcsolatos javaslatok megfogalmazása. Ennek a komplex kérdéskörnek a megértéséhez kvalitatív kutatási módszertant alkalmaztunk, szakértői mélyinterjúk formájában. A szabályok megfelelő állapota és gyakorlati alkalmazása kulcsfontosságú a felhasználói adatok védelmében és az illetéktelen hozzáférés kockázatának minimalizálásában. A tanulmányban bemutatott javaslatok támogatják a szabályozási környezet fejlesztését a gépjárműgyártás terén.

Kulcsszavak

IoT, személygépjármű, szabványok, kiberbiztonság, információbiztonság

¹ hegyi.henrietta@uni-obuda.hu | ORCID: <https://orcid.org/0000-0002-7731-840X> | Doktori hallgató, Óbudai Egyetem | Doktori hallgató, Óbudai Egyetem.

BEVEZETÉS

Az internetkapcsolatra képes személygépjárművek hasonlóan a mobiltelefonokhoz, ki vannak téve az internetről érkező támadásoknak, miközben a személygépjármű rendszereihez való illetéktelen hozzáférés használatának célját tekintve nagyobb veszélyforrást jelenthet annak felhasználója, mint egy mobiltelefon. A modern személygépjárművek a „Dolgok Internetéhez” (Internet of Things, IoT) hasonlóan képesek arra, hogy az internethez kapcsolódjanak és onnan különböző utasításokat tartalmazó üzeneteket fogadjanak. Egyre több gyártó tér át a gépjárművek belső hálózatának kulcsfontosságú elemei, a mikrokontrollerek (ECU – *electronic controller unit*) *firmware*² progjainak (alapszoftver vagy vezérlőprogram) interneten keresztül való frissítésére is. Ezt a gyakorlatot FOTA/OTA szolgáltatásnak (*over-the-air* vagy *firmaware* esetében *firmware-over-the-air*³) nevezzük.

A személygépjárművek ma már a legkülönbözőbb szenzorokkal, adatfeldolgozó egységekkel, rögzítőeszközökkel (pl. kamera) vannak felszerelve, melyek nagy mennyiségű információ összegyűjtésére szolgálhatnak. Az ilyen adatokból a felhasználó vagy egy csoport számos tulajdonságára, szokására lehet következtetni, mely szintén biztonsági kockázatokat rejt magában. Ugyan a gépjárműiparban a mind a gyártóknak, mind pedig a beszállítóknak szigorú biztonsági előírásoknak kell megfelelnie, az informatika gyors fejlődésének hatására ugyanezt a szigorú rendszert az elektronikus információbiztonság kapcsán már sokkal nehezebb működtetni. [1] Bár a legtöbb esetben a támadóknak nem érdekük a járműben tartózkodók életét veszélyeztetni, mégis van ok az aggodalomra, hiszen a rengeteg gyűjtött adatnak köszönhetően magas haszonnal kecsegtethet egy esetleges sikeres behatolás. [2] A megfelelő védelem kialakítása kapcsán problémát jelent, hogy a biztonsági értékelés gyakran szubjektív szempontok alapján történik – minél összetettebb rendszerről van szó, annál nehezebb pontos metrikát alkalmazni a kockázatok elemzésére. [3], [4]

Az információbiztonsági szakértők szubjektív ítéletei fontos szerepet játszanak a kiberfizikai rendszerek fenyegetéseinek értékelése és modellezése során. Például az egyes rendszerelemek sebezhetőségét többféle tényező alapján lehet leírni; ilyenek a bonyolultság, a technológiai érettség és a támadások segítésére rendelkezésre álló eszközök elérhetősége. Ezek az információk hasznosak a támadási kockázat meghatározásában, de nagy részüket nehéz automatikusan begyűjteni. Azonban a legtöbb szakértőben valamilyen mértékű bizonytalanság rejlik az értékelések terén. [5] A meglévő módszerek a fenti okokból kifolyólag nagymértékben függenek az értékelő tapasztalataitól, és a biztonsági mérőszámok általában legjobb esetben belső kockázatelemzési metódusok eredményeiként alakulnak ki. [6]

Jelen tanulmány célja, hogy feltárja a személygépjárművekkel kapcsolatos információbiztonsági kihívásokat és javaslatokat fogalmazzon meg a jelenleg használatban lévő szabványok és szabályozási környezet gyakorlati alkalmazásával kapcsolatban. A tanulmány célja továbbá az is, hogy javaslatokat fogalmazzon meg a szabályozási környezet tar-

² Hardverben - jellemzően csak olvasható memóriában (ROM) vagy programozható csak olvasható memóriában (PROM) - tárolt számítógépes programok és adatok, úgy, hogy a programok és adatok nem írhatók vagy módosíthatók dinamikusan a programok végrehajtása során.

³ A folyamat során a szoftverfrissítés „a levegőn keresztül”, azaz internet kapcsolat segítségével jut el a járműhöz, tehát nincs szükség például pendrive vagy egyéb fizikai eszköz csatlakoztatására.

talmára és alkalmazására vonatkozóan a személygépjárműipar területén, továbbá egy a kibert biztonsági területen kevésbé gyakran alkalmazott módszertani megközelítéssel vizsgálja meg a témát, ezzel hozzájárulva a jövőbeli kutatási irányok meghatározásához.

A cikk kutatási kérdései a következők:

1. A hazai információbiztonsági szakemberek szerint megfelelő-e a jelenlegi információbiztonsági szabályozási környezet hatékonysága a személygépjárműiparban?
2. Milyen változtatásokkal lehetne hatékonyabbá tenni a személygépjárműiparban alkalmazott információbiztonsági szabványokat és szabályozási környezetet, hogy azok megfelelően védjék ne csak a gyártó, de a felhasználó adatait is?

A tanulmány a fenti problémára kvalitatív kutatás segítségével keresi a választ. A szakirodalmi elemzés a főbb információbiztonsági elméleti megközelítéseket, valamint leggyakrabban alkalmazott szabványokat elemzi. A kutatáshoz választott módszertan a mélyinterjú sajátosságait, valamint az átiratok elemzésére alkalmazott tartalomelemzési módszertant ötvözi.

SZAKIRODALMI ELEMZÉS

Az összekapcsolt autókkal kapcsolatos szolgáltatások adatainak feldolgozását szabályozó információbiztonsági irányelvek gyakran lazán meghatározott és/vagy nem összeegyeztethető célokat (pl. kért szolgáltatások nyújtása, biztonságos használat, viselkedésertékelés, valamint üzleti tevékenységek működtetése és bővítése) kapcsolnak össze. [7] Például az eredetileg karbantartási vagy felhasználói élmény fokozásának céljával [8] gyűjtött adatokat az érintettek beleegyező nyilatkozata esetén a biztosítótársaságok felhasználhatják a járművezetői profilok gazdagítására, az egyéni árazás kialakítására, a vezetési magatartáson alapuló biztosítási kötvények kínálására vagy az autóbalesetekben fennálló felelősség kivizsgálására. [9] A főként az ipar 4.0 technológiákat érintő komplexitásból fakadó szabályozási problémákra a COVID-19 időszaka is rámutatott. [10] Megfelelő szabályozási környezetben a közlekedésbiztonsági hatóságok is felhasználhatják ezeket az adatokat a közlekedési szabályok betartatására, például a sebességhatárolások ellenőrzésére. A személyautóhasználatára vonatkozó minden egyes adat, például a vezetési útvonalak és úti célok, az autóra épített kommunikáció vagy az infotainment-szolgáltatások érzékeny információkat tárhatnak fel az adott személy életéről. Az emberek vezetési rutinja és az érdeklődési körükbe tartozó helyek nemcsak az azonosításukat teszik lehetővé [11], hanem – például az általa látogatott helyszínek ismeretében – olyan érzékeny információkra is következtethet az adatfeldolgozó, mint a vallási és politikai kötődések, a szexuális irányultság és az egyéb emberi kapcsolatok. Ezért az összegyűjtött adatok hasznosak az egyének profilalkotásához és megfigyeléséhez, különösen akkor, ha a személyes adatok meglévő (magán- vagy kormányzati) adatbázisaihoz kapcsolódnak vagy például a mobiltelefonjaik által gyűjtött adatokkal kapcsolják össze azokat. [12] Az adatkezelőknek egyértelműen tájékoztatniuk kell az internetre vagy más hálózatra csatlakoztatott autók felhasználóit a helymeghatározási adatok feldolgozásának céljáról. A helymeghatározási adatok érzékeny jellege miatt ezen adatokra az adatvédelmi elvek alapos alkalmazása szükséges, különösen a célhoz kötöttség, az adatok minimalizálása és az adatok tárolása tekintetében. Bár a különböző autóiparban alkalmazott szabványok és jogszabályok ma már magukba foglalják az ellátási lánc védelmét is, amely sok esetben a beszállítóknak a gyártóval egyenértékű szintű szabványoknak

való megfelelést jelenti, [13] az információbiztonsági szabványok általában csak egy keretet határoznak meg és nem adnak konkrét utasításokat a végrehajtással kapcsolatban. Ez bizonyos mértékben szükséges is, hiszen a különböző speciális helyzetek miatt adott fokú rugalmasság kulcsfontosságú.

Széles körben elismert, hogy a mérőszámok fontosak az információbiztonság szempontjából, mivel ezek hiányában nem tudjuk mérni a biztonsági politika, mechanizmusok vagy megvalósítások sikerét. A különböző kockázatelemzési módszerek például hatékony eszközt jelenthetnek az információbiztonsági szakemberek számára, hogy mérjék rendszereik, termékeik, folyamataik biztonsági szintjét, valamint a biztonsági problémák kezelésére való felkészültségüket. A mérőszámok segíthetnek a rendszer sebezhetőségének azonosításában is, útmutatást nyújtva a korrekciós prioritások meghatározásához. Az autógyártóknak érdekük ezenfelül, hogy megfeleljenek a főbb információbiztonsági és IT biztonsági szabványoknak, megvédjék a termékeikben – személygépjárműben – tárolt adatokat és az autók IT infrastruktúráját.

A leggyakrabban használt általános szabvány, melyet különböző vállalatok világszerte széleskörben alkalmaznak, az ISO 27001⁴. Ez a szabvány a személygépjárműiparban is elterjedt és erős kereteket biztosít ugyan az információbiztonság megteremtéséhez, de nem ad iránymutatást arra vonatkozóan, hogyan kell megvalósítani a leírtakat. Amellett, hogy rendkívüli rugalmasságot biztosít ezzel a vállalatok számára, egyúttal a kerülőmegoldások előtt is kaput nyit. Ahogyan a másik népszerű általános szabvány, a NIST 800-53⁵, az ISO 27001 is a folyamatok szemszögéből közelíti meg az információbiztonság problémáját. Bár mindkét szabvány alapján a beszállítók számára is kötelező ugyanazon audit elvégzése, ennek gyakorlati megvalósulása kérdéses lehet, hiszen egy olyan komplex termékben, mint a személygépjármű, számos beszállító és azok alvállalkozói dolgoznak, különböző területekről. Emiatt a betartás nehézségekbe ütközhet például az átláthatatlanság miatt. Az általánosan használt információbiztonsági szabványok között termékorientált szemléletmódot képvisel a Common Criteria⁶, mely így már jobban közelíti azt a célt, hogy a személygépjármű mint végtermék, illetve a vele szerves összeköttetésben álló hálózat és szerverek hardveres és szoftveres rendszerei biztonságos működését biztosítsa. A Common Criteria azonban az ISO 27001-hez és a NIST 800-53-hoz képest sokkal kevésbé elterjedt.

Az elmúlt évek jelentős előrelépésének tekinthető a TISAX és az ISO/SAE 21434⁷ megjelenése, melyek már specifikusan a személygépjárműipar igényeire szabott információbiztonsági szabványok. Az ISO/SAE 21434 egy termékközpontú, autóiipari kibervédelemmel foglalkozó specifikus szabvány, mely meghatározza a közúti járművek elektromos és elektronikus (E/E) rendszereinek - beleértve azok alkatrészeit és kapcsolódási pontjait - koncepciójára, termékfejlesztésére, gyártására, üzemeltetésére, karbantartására és leszerelésére vonatkozó kiberbiztonsági kockázatkezelés műszaki követelményeit. Meghatározásra kerül benne egy keretrendszer, amely a kiberbiztonsági folyamatokra vonatkozó követelményeket és a kiberbiztonsági kockázatok kommunikációjának és kezelésének közös nyelvezetét tartalmazza. A szabvány minden sorozatgyártású közúti jármű E/E-rendszereire alkalmazandó, beleértve azok alkatrészeit és kapcsolódási pontjait, amelyek fejlesztése

⁴ <https://www.iso.org/standard/27001>

⁵ <https://www.nist.gov/privacy-framework/nist-sp-800-53>

⁶ <https://www.commoncriteriaportal.org>

⁷ <https://www.iso.org/standard/70918.html>

vagy módosítása e dokumentum kiadása után kezdődött. Ez ígéretesen hangzik ugyan, azonban a többi szabványhoz hasonlóan, az ISO/SAE 21434 bevezetése sem kötelező, ráadásul mivel egy rendkívül fiatal, 2021-ben kiadott szabványról van szó, időbe telik az is, mire a piac befogadja és így kellő területet tud majd lefedni. A TISAX (Trusted Information Security Assessment Exchange)⁸ egy olyan új biztonsági értékelési keretrendszer, amelyet az autópár szereplői fejlesztettek ki a beszállítók biztonsági kockázatainak kezelése érdekében. Az értékelési rendszer célja, hogy a beszállítók biztonsági szintjét egységes és hatékony módon lehessen értékelni és ellenőrizni, valamint biztosítsa az autópári vállalatok számára, hogy a beszállítók biztonsági szintje megfelelő. A TISAX értékelési keretrendszer alapvetően az ISO/IEC 27001 információbiztonsági szabványra épül, de az autópári beszállítók számára további biztonsági követelményeket is tartalmaz. Az értékelési folyamat során a beszállítók biztonsági szintjét egy harmadik fél értékeli és ellenőrzi, így biztosítva a független értékelést. A TISAX értékelési rendszer használata előnyös lehet a beszállítók számára, mert lehetővé teszi számukra, hogy bizonyítsák biztonsági szintjüket az autópári partnereik számára. Emellett a TISAX értékelési keretrendszer segít a beszállítóknak abban is, hogy felmérjék saját biztonsági kockázataikat és javítsák információbiztonsági folyamataikat. [14]

A fenti szabványokon kívül érdemes még említést tenni az IEC 62443-ról⁹, mely kifejezetten az ipari ellenőrzési rendszerekre vonatkozik, illetve a SAE J3061¹⁰ szabványról, melynek lényege, hogy gyakorlati tapasztalatokat gyűjt egybe és ajánlásokat nyújt a gyártók számára az információbiztonsági folyamatok fejlesztéséhez. Az összegyűjtött jógyakorlatok legfőbb célja, hogy rugalmasak, pragmatikusak és adaptálhatók legyenek a járműiparban, valamint más területeken működő kiberfizikai járműrendszerekre nézve is (pl. kereskedelmi és katonai járművek, teherautók, buszok). Ez az ajánlott gyakorlat azonban szintén magas szintű irányadó elveket állapít meg, tehát a konkrét megvalósításra vonatkozóan nem rögzít elvárásokat.

Ezenkívül az autógyártók az általuk gyártott autókra vonatkozó specifikus szabványokat és irányelveket is alkalmaznak (például ISO/TS 16949, amely az általános, ISO 9001 minőségbiztosítási szabvány autópári leképezése), amelyek lehetnek nemzetközi vagy helyi szintűek. Az Európai Unióban az autókra vonatkozó szabványokat az Európai Bizottság, míg az Egyesült Államokban a Nemzeti Autópálya-biztonsági Hivatal (NHTSA) határozza meg, így attól függően is eltérés tapasztalható a követelmények között, hogy a világ melyik pontját vizsgáljuk. Az Európai Uniót tekintve az elmúlt években egyre nagyobb hangsúlyt kapott a GDPR és ennek hatására más területek is nagyobb hangsúlyt kezdtek fektetni az adatvédelemre. Ennek köszönhetően a felsorolt szabványokban is egyre nagyobb súllyal jelent meg az adatvédelem kérdésköre. Ezzel együtt is elmondható azonban, hogy a szabályozások közül egyedül a GDPR fókuszál kifejezetten a fogyasztók adataira és az adatáramlás átláthatóságára. Jelen tanulmánynak nem célja teljeskörűen bemutatni a GDPR-al kapcsolatos problémákat, de információbiztonsági kontextusban is érdemes kiemelni, hogy a nemzetközi szakirodalom számos olyan példát szolgáltat, melyek alátámasztják, hogy a rendeletet szükséges fejleszteni. [15], [16], [17]

⁸ <https://www.tuvsud.com/en/services/auditing-and-system-certification/tisax>

⁹ <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>

¹⁰ https://www.sae.org/standards/content/j3061_201601

Szintén fontos megjegyezni, hogy a hálózati kommunikáció miatt a tanulmány témájához kapcsolódnak a különböző felhőszolgáltatásokra vonatkozó szabályozások, illetve egy sor ipari eszközökre vonatkozó szabályozás is, ám ezekre jelen kutatás terjedelmi okok miatt szintén nem tér ki.

A SZEMÉLYGÉPJÁRMŰ MINT IOT ESZKÖZ

A Dolgok Internete, azaz az "Internet of Things" (IoT) kifejezést Kevin Ashton alkotta meg 1999-ben, egy előadáson a Procter & Gamble-nél. Ashton az egyik alapítója a Massachusetts Institute of Technology Automatic Recognition Labjának. [18]

Az IoT eszközök fogalmára azóta többféle definíció is elterjedt, melyek közül néhány gyakran alkalmazottat az alábbi táblázatban szemléltetünk:

Forrás	Definíció
NIST SP 1800-16B-C	Eszközök hálózata, amely tartalmazza a hardvert, szoftvert, firmware-t és aktuátorokat, amelyek lehetővé teszik az eszközök kapcsolódását, kölcsönhatását és szabad adat- és információcseré lehetőségét. ¹¹
NIST SP 800-172	A kiadványban használt értelemben olyan felhasználói vagy ipari eszközök, amelyek csatlakoznak az internethez. Az IoT eszközök szenzorokat, vezérlőket és háztartási készülékeket is magukba foglalnak. ¹²
Gartner	Az "Internet of Things" (IoT) a fizikai tárgyak hálózata, amelyek beépített technológiával rendelkeznek, hogy kommunikáljanak, érzékeljenek vagy kölcsönhatásba lépjenek a belső állapottal vagy a külső környezettel. ¹³
Európai Parlament	Az „Internet of Things” (IoT) olyan elosztott hálózatot jelent, amely fizikai tárgyakat köt össze, képesek érzékelni vagy cselekedni a környezetükben, és kommunikálni egymással, más gépekkel vagy számítógépekkel. ¹⁴

1. táblázat - IoT definíciók. (Saját szerkesztés)

A személygépjármű IoT eszközként való értelmezése az elemzett szakirodalmi anyagban nem szerepel ugyan, azonban ha arra gondolunk, hogy a napjainkban használt személygépjárművek szenzorokkal és internetkapcsolattal rendelkeznek, és a telekommunikációs hálózatokon keresztül a szenzorok által rögzített adatokat (vagy azok feldolgozásának eredményét) továbbítják a gyártó vagy harmadik felek szervei felé, akkor az 1. táblázatban felsorolt definícióknak megfelel.

Ez a megfigyelés azért tarthat számot érdeklődésre, mert az IoT eszközök sajátosságait tekintve sokkal közelebb állnak a jelenleg használt személygépjárművekhez, mint a 20-30 évvel ezelőtti, külső hálózati kommunikációt egyáltalán nem használó régi személygépjárművekhez. Ennek okán a rájuk vonatkozó szabályozási környezet alkalmazása

¹¹ https://csrc.nist.gov/glossary/term/internet_of_things

¹² https://csrc.nist.gov/glossary/term/internet_of_things

¹³ <https://www.gartner.com/en/information-technology/glossary/internet-of-things>

¹⁴ [https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI\(2015\)557012_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf)

megoldást jelenthetne a személygépjárművek biztonságának biztosítására. Az IoT eszközök standardizálása azonban mindmáig komoly kihívásokba ütközik, köszönhetően a technológia gyors fejlődésének, az eszközök rövid életciklusának és sokféleségének. [19] Ezek a kihívások szintén megfigyelhetők a személygépjárművek esetén is.

MÓDSZERTAN

A kutatás módszertanaként a téma érzékeny mivoltát és összetettségét figyelembe véve a mélyinterjú választottuk. A mélyinterjú sajátossága, hogy a kutató nem megadott kérdéslista hanem előre definiált témakörök alapján folytat dialógust az interjúalanyokkal azzal a céllal, hogy lehetőséget kapjon olyan kontextuális információk megszerzésére is, melyek az előzetes kutatások alapján nem merültek fel. [20] A mélyinterjú nem alkalmas ugyan arra, hogy a kapott eredmények alapján általánosításokat fogalmazhassunk meg, de lehetőséget biztosít arra, hogy a tématerületet mélyen ismerő szakemberek tapasztalatait és javaslatait megismerjük és összefoglaljuk.

Jelen kutatás lefolytatásához ezért a terepkutatás kategóriájába tartozó féligstruktúrált interjúztatás módszere került kiválasztásra, mint a témához illeszkedő technika. [22] Az empirikus kutatás célja egyrészt annak megismerése, hogy mi a magyar szakértők véleménye a szakirodalomban felvetett információbiztonsági szabályozásokkal kapcsolatos trendekről, érdemes-e IoT eszközként kezelni a személygépjárművet és milyen kihívásokkal szembesülnek az elméletek gyakorlati adaptálása során, másrészt pedig az, hogy a felmerült információbiztonsági problémákkal kapcsolatos megoldási javaslatok összegyűjtésre kerüljenek. Mivel ez a megközelítés mélyebb dialógust igényel és nem oldható meg például egyszerű kérdőíves módszertannal, ezért indokolt a mélyinterjú alkalmazása. [23] Az interjú a kérdésfeltevésén és az arra adott válaszok megvitatásán kívül kötetlen formában zajlott, azaz interaktív beszélgetés keretében, ami megkönnyítette a többletinformációk megszerzését. [22] Az interjú készítése közben fontos szempont volt olyan új információk feltárása, melyek a szakirodalmi elemzés során nem merültek fel, de újabb vizsgálatok alapját képezhetik.

A megfelelő kérdések megállapításához, először a dolgozatban körüljárt témákra alapozva négy dimenzió – személygépjármű mint IoT eszköz, információbiztonsági szabványok hatékonysága és alkalmazása, kihívások a szabványok és jogszabályok gyakorlati alkalmazásában, megoldási javaslatok – elkülönítése történt meg, amelyek sorbarendezésének szempontja az volt, hogy az általánosabb témakörtől tartsanak az egyre specifikusabb felé. Erre azért volt szükség, hogy meghatározható legyen, hogy a kiválasztott szakemberek milyen általános megközelítést alkalmaznak a munkájuk során és milyen specifikumokat fedeznek fel a személygépjárműipari információbiztonsággal kapcsolatban.

Mivel nem minden szakértő rendelkezik ugyanolyan mély tapasztalattal az autóipar kapcsán – de ettől függetlenül lehetnek releváns szakmai észrevételei, melyek az autóiparra is érvényesek – így fontos, hogy az ipárgspecifikus kérdések csak kiegészítő információk gyűjtésére szolgáltak és csak akkor kérdeztünk rájuk, ha az adott interjúalany ténylegesen rendelkezett ilyen jellegű tapasztalattal is.

Narratív elemzés

Ahhoz, hogy az információbiztonsági szabványok alkalmazásának nehézségeit gyakorlati szempontból vizsgálhassuk, olyan technikával volt szükséges elemezni az interjúk

lefolytatása során keletkezett információkat, amely segítségével nem csak egy-egy tény állapítható meg [21] az auditori munkával és a szabványokkal kapcsolatban, hanem azonosíthatók az elmélet és gyakorlat közötti különbségek mélyebben meghúzódó okai, vagy például az eredményeket befolyásoló szubjektív tényezők.

Az interjúleíratok a Krippendorff-féle tartalomelemzési módszertannal kerültek elemzésre, melynek lényege, hogy a kontextus is szerves részét képezi a szövegelemzésnek, így illeszkedik a tanulmányban foglalt komplex témához azáltal, hogy lehetőséget nyújt arra, hogy a kutató induktív módon következtessen a tartalomra. [24]

Mintavétel

A kvalitatív, mélyinterjú kutatás központi alanyai az információbiztonsági szakértők, azaz auditorok, tanácsadók és kutatók. Ahhoz azonban, hogy az elemzés során releváns információkat fedhessünk fel, szükség volt az előzetes, 25 főből álló csoport szűkítésére. A kutatásban résztvevő 10 interjúalany kiválasztása során szűrőfeltétel volt az információbiztonsági szakmák valamelyikében eltöltött minimum 5 év munkatapasztalat, illetve a minimum 5 különböző iparágban vagy területen, iparágban szerzett jártasság. Ezek a kritériumok biztosítják, hogy a szakértők megfelelően széleskörű gyakorlati ismeretekkel rendelkezzenek a kutatott kérdéseket illetően. A személygépjárműiparban szerzett tapasztalat nem volt azonban követelmény, mivel jellegüknél fogva a kutatási kérdések megválaszolásához nem szükséges mély ágazati ismeret, ellenben a minél széleskörűbb rálátás a különböző iparágak szabályozási környezetéről hozzásegít a jó és rossz gyakorlatok felismeréséhez.

Ennek okán került a mintába például olyan szakember, aki főként magyar kis- és középvállalkozásokkal foglalkozik és olyan, aki jelenleg az állami szférában dolgozik, azonban korábbi ügyfelei és munkáltatói közé tartoznak pénzügyintézetek, gyógyszeripari gyárak és élelmiszeripari vállalatok is.

Eredmények

Az interjúalanyok válaszaiból kiderül, hogy három válaszadó dolgozott már valamilyen járműiparral kapcsolatos információbiztonsági projekten, feladatkörben, míg hét személy nem rendelkezik ilyen tapasztalattal. Ennek okán csak az előbbi három személy számára tettünk fel iparág-specifikus, kifejezetten járműipari szabványokra vonatkozó kérdéseket.

1. A személygépjármű mint IoT eszköz

Ennek a kérdésnek a relevanciáját az adja, hogy a személygépjármű, illetve annak alkatrészei hasonlítanak az IoT-ként definiált eszközökre és az ezekre vonatkozó szabályozási környezet jelenleg még szintén igen hézagos – így van létjogosultsága az olyan javaslatoknak, mint például hogy az IoT eszközök esetében megjelenő új szabványokat a személygépjárművek esetében is alkalmazzák az auditorok.

A kutatás során megkérdezett szakértők mindegyike egyöntetűen IoT eszközként tekint a személygépjárműre információbiztonsági szempontból. Ezt javarészt azzal indokolták, hogy a jármű a szenzorok által adatokat rögzít és a külső hálózattal is képes a kommunikációra. Az egyik interjúalany megközelítése a többiekhez képest egyedi volt abban, hogy felvetése szerint nem maga a jármű tekinthető IoT eszköznek, hanem annak alkatrészei. Ezt a megközelítést támasztja alá a személygépjármű, mint kiberfizikai rendszer komplex összetétele és alkatrészeinek sokfélesége.

Azonban ha a személygépjárművet ilyen nézőpontból vizsgáljuk azzal azt kockáztatjuk, hogy egyes alkatrészek kimaradnak az ellenőrzésből. Az egyik interjúalany a korábban bemutatott ISO/SAE 21434 szabvánnyal kapcsolatban kiemelte, hogy bár az jelentős változással kecsegtet a személygépjárművek elektronikai biztonságát tekintve, mivel az egyes elemekre fókuszál a teljes rendszer helyett, ezért nem nyújt teljes megoldást. Amennyiben tehát az IoT eszközökre érvényes szabványokat kívánjuk alkalmazni a személygépjármű egyes részeire, akkor ezt a lefedettséggel összefüggő kockázatot figyelembe kell vennünk.

2. Kockázatelemzés, metrikák, adatbiztonság

A teljes mintából egy szakértő nyilatkozta csupán, hogy szerinte az ISO 27001 (és ISO 27005) alapján végzett kockázatelemzés képes biztosítani a végfelhasználó adatainak biztonságát. Véleményét azzal indokolta, hogy mivel a szabvány kimondja, hogy a szervezetnek a rá vonatkozó szabályoknak meg kell felelnie, így a GDPR-nak való megfelelési kötelezettség az Európai Unió területén biztosítva van. A másik kilenc interjúalany véleménye azonban ettől markánsan eltér, többnyire az elmélet és a gyakorlat között tátongó különbségekre hívják fel a figyelmet, illetve arra, hogy a szabványok betartásának kikényszerítésére nincsenek megfelelő eszközök.

Példaként említik, hogy a beszállítók kibújhatnak a megfelelés alól azzal, ha például azt nyilatkozzák, hogy a szabvány bevezetése már folyamatban van, míg végül a minősítő auditra évek múltán sem kerül sor. A szakértők olyan esetről is beszámoltak, amikor egy szabvány adatbiztonságra irányuló követelményeinek való megfelelést a tanúsítást kérő szereplő egyszerűen egy ügyvédi iroda által kiállított nyilatkozattal oldotta meg.

Akkor sincs biztosítva azonban a megfelelés, ha minden szereplő megfelelő hozzáállással rendelkezik, hiszen a legtöbb kockázatkezelési módszertan nem írja elő, hogy a maradványkockázatokat milyen időtartam alatt kell kiküszöbölni, hanem az erre vonatkozó szabályok és gyakorlatok pontos kidolgozását a szervezetre hagyja.

3. Kihívások és megoldási javaslatok

A kihívások kapcsán több interjúalany is kiemelte a jármű, mint végtermék komplexitását. Két interjúalany is rávilágított arra, hogy egyre nagyobb kihívást fog jelenteni a személygépjárművek szoftverkörnyezetének támogatása. Amennyiben a szoftvertámogatás lejár, akkor onnantól kezdve nem biztosított a megfelelő védelem sem. Az adatbiztonság szempontjából kihívásnak tekinthető az is, hogy a felhasználó nem kap rálátást arra, mi történik pontosan a személyautó informatikai rendszerével és adataival egy szerviz során. Ezt nem csak megfelelő tájékoztatással, de egyes interjúalanyok szerint kifejezetten erre a célra szolgáló archiválóeszközökkel kell biztosítani, azaz lényegében egy az aviatikában is ismert fekete doboz használatára lenne szükség.

Az egyik interjúalany arra világított rá, hogy a Common Criteria szabvány széleskörűbb alkalmazása megoldást jelenthetne a személygépjárművek információbiztonságának termékalapú megközelítésére, azonban ha a szabvány hivatalos weboldalán felsorolt biztosított eszközök listáját megnézzük¹⁵, akkor látható, hogy világviszonylatban csak kevés számú eszköz rendelkezik ezzel a minősítéssel. Ezek nagyrésze pedig valamilyen általános informatikai eszköz például tűzfal.

¹⁵ <https://www.commoncriteriaportal.org/products>

Az ISO/IEC 21434 szabvány esetében már valóban egy iparág-specifikus szabványról beszélhetünk, azonban nem maga a személygépjármű képezi a vizsgálat objektumát, hanem annak egyes elektronikai részei. Ilyenek lehetnek például a fékeket vezérlő elektronikai alkatrészek, de egy *infotainment* rendszer *bluetooth* modulja is. A személygépjármű biztonságának szempontjából problémát jelent, hogy nem is minden alkatrésszel kapcsolatban várható el a tanúsítás, így viszont a gyártó igényeitől függően csak „foltszerűen” érvényesül annak hatása. Ez ráadásul nem csak a menedzsment szemléletéből, hanem a szűkös erőforrásokból is fakad, hiszen a szigorú előírásoknak való megfelelés magas költségekkel járhat.

Az átfogó megoldási javaslatok tekintetében szinte minden szakértő egyetértett abban, hogy szükséges lenne egy egységes európai szintű jogszabályra, mely pontosan előírja azoknak a kontrolloknak az alkalmazását a személygépjárműgyártók és beszállítói számára, amik jelenleg a szabványokban szerepelnek. Ehhez kapcsolódva szükségessé válik egy olyan hatóság létrehozása is, amely betartatja a szabályokat. Az egyik interjúalany kitért arra is, hogy amíg a gazdasági tényezők nem ösztönzik a gyártókat a nagyobb körültekintésre, addig a helyzet változatlan marad.

Végül a tíz interjúalanyból három is megoldási javaslatként hivatkozott a felhasználók tudatosságának növelésére. Az interjúalanyok általános vélekedése szerint ugyanis a felhasználót többnyire magát sem érdeklik az információbiztonsági problémák, csak akkor, ha egy eszköz meghibásodik vagy az adataik valóban veszélybe kerülnek, kiszivárognak. Ezzel kapcsolatban sokszínű megoldási javaslatok születtek az általános iskolai edukációtól (például információbiztonsági előadások az informatika órán) kezdve az átláthatóbb tájékoztatászövegek átadásáig.

Egy olyan vélemény is akadt, melynek lényege egyenesen az volt, hogy a fejlett kényelmi és szolgáltatási célú eszközök, gyakorlatok alkalmazását, mint például az ülésfűtés szolgáltatásként való nyújtását, be kéne tiltani a személygépjárművekkel kapcsolatban. Ennek a gondolatnak a logikai hátterét az adja, hogy az informatika fejlődése ma már olyan méreteket ölt, hogy ennek köszönhetően a biztonsági szakemberek és a szabványok semmiképpen nem tudnak lépést tartani vele.

ÖSSZEGZÉS

Összességében elmondható, hogy a tanulmányban bemutatott szabványok és jogszabályi környezet elsősorban a gyártókat védi, folyamatközpontú és még az olyan célzott szabályok ellenére is, mint a GDPR, kevés hangsúly jut a végfelhasználó adatainak biztonságán. A szabványok nagy része folyamat alapú, a termékközpontú szabványokat pedig a jármű egyes részeire alkalmazzák csak.

A tanulmány első fejezetében bemutattuk a személygépjárművek információbiztonsági szabályozási környezetére vonatkozó szakirodalmi forrásokat, illetve röviden ismertettük a főbb általános és ágazati szabványokat és azok jellemzőit. A második fejezetben röviden vizsgáltuk, hogy az általánosan elterjedt definíciók alapján a személygépjármű tekintetében információbiztonsági szempontból IoT eszköznek, melyet a későbbi interjúelemzés során megerősítettünk. A harmadik fejezetben bemutattuk a kutatás módszertani sajátosságait.

A tanulmányban foglalt kvalitatív kutatás célja az volt, hogy a szakirodalomban fellelhető információk megismerése után hazai, tapasztalt szakemberek egy csoportjának véleményével összevetve azokat, megválaszoljuk a két kutatási kérdést:

1. A hazai információbiztonsági szakemberek szerint megfelelő-e a jelenlegi információbiztonsági szabályozási környezet hatékonysága a személygépjárműiparban?
2. Milyen változtatásokkal lehetne hatékonyabbá tenni a személygépjárműiparban alkalmazott információbiztonsági szabványokat és szabályozási környezetet, hogy azok megfelelően védjék ne csak a gyártót, de a felhasználó adatait is?

A 1 kérdés vizsgálata során azt tapasztalhattuk, hogy az interjúalanyok megerősítették és többféle különböző aspektusból is rávilágítottak arra, hogy a személygépjárművekben keletkezett vagy használt adatok biztonságának szabályozása és a folyamatok megfelelő biztosítása kihívást okoz a szakemberek számára. A szabályozási környezet az információbiztonság területén töredezett, sok esetben túlzottan megengedő és ennek megfelelően nem hatékony.

A 2 kérdés vizsgálata során az elemzést bemutató fejezetből kiderült, hogy a szakértők véleménye meglehetősen sokrétű, többen többféle oldalról közelítik a megoldást. Összességében elmondható azonban, hogy a vélemények többsége kettéoszlik: a szakértők a legnagyobb problémát egyrészt a szabványok gyakorlati betartásában, a megfelelő erővel bíró hatóság hiányában látják, másrészt pedig a felhasználók attitűdjében, tudatosságuk hiányában.

Elmondható, hogy a javasolt megoldások túlmutatnak az információbiztonsági szabályozási intézkedések hatókörén, azonban ettől függetlenül is fontos alapot jelenthetnek mind a további felhasználói attitűdvizsgálatok, mind pedig a szabályok betartásának lehetséges megoldási módjait kereső kutatások számára.

FELHASZNÁLT IRODALOM

- [1] Khan, Shah Khalid; Shiwakoti, Nirajan; Stasinopoulos, Peter; Chen, Yilun. „Cyberattacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. , 148, 105837.,” *Accident Analysis & Prevention*, 2020.
- [2] Weimerskirch, A.; Gaynier, R. „An Overview of Automotive Cybersecurity: Challenges and Solution Approaches,” 2015.
- [3] Koubatis, Andrew; Schonberger, Jorge Yerena. „Risk management of complex critical systems,” *International Journal of Critical Infrastructures*, %1. kötet1(2/3), 2005.
- [4] D. Gardner. *Risk: The Science and Politics of Fear*, New York: Random House, 2009.
- [5] Ellerby, Zack; McCulloch, Josie; Wilson, Melanie; Wagner, Christian. „Exploring How Component Factors and Their Uncertainty Affect Judgements of Risk in Cyber-Security,” *Critical Information Infrastructures Security. Lecture Notes in Computer Science*, 1/11777, 2020.
- [6] Ji, Zuzhen; Yang, Shuang-Hua; Cao, Yi; Wang, Yuchen; Zhou, Chenchen; Yue, Liang; Zhang, Yinqiao. „Harmonizing safety and security risk analysis and prevention in cyber-physical systems,” *Process Safety and Environmental Protection*, %1. kötet148, 2021.

- [7] Ogbuke, Nnamdi Johnson; Yusuf, Yahaya Y.; Dharma, Kovvuri; Mercangoz, Burcu A. „Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society, *Production Planning & Control*,” 2020.
- [8] Hofmann, Martin; Neukart, Florian; Bäck, Thomas. „Artificial Intelligence and Data Science in the Automotive Industry,” 2017.
- [9] M. Marabelli; S. Hansen, S. Newell; C. and Frigerio. „The Light and Dark Side of the Black Box: Sensor-based Technology in the Automotive Industry,” *Communications of the Association for Information Systems*, 40/16, 2017.
- [10] Ivanov, Dimitry; Dolgui, Alexandre. „A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0,” *Production Planning & Control*, %1. kötet7287, 2020.
- [11] Oliver, N.; Pentland, A. P. „Driver Behavior Recognition and Prediction in a Smart-Car,” 2000.
- [12] Peppes, Nikolaos; Alexakis, Theodoros; Adamopoulou, Evgenia; Demestichas, Konstantinos. „Driver Behavior Monitoring Based on Smartphone Sensor Data and Machine Learning Methods,” in 2019 25th Conference of Open Innovations Association (FRUCT), 2019.
- [13] Pereira, Teresa; Barreto, Luis; Amaral, António. „Network and information security challenges within Industry 4.0 paradigm,” *Procedia Manuf.*, 1/13, 2017.
- [14] Haig, Zsolt. „TISAX, az autópár új információbiztonsági követelményrendszere,” *Magyar Minőség*, 1. /június, 2020.
- [15] Machuletz, D.; Böhme, R. „Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR,” *Proceedings on Privacy Enhancing Technologies* 2020.
- [16] Stoica, L. A.; Savu, R. A. C. „RISKS AND EXPLOITS EXPOSED BY GDPR,” *Eurasian Journal of Social Sciences*, 9(1), 2021.
- [17] Gladis, A. ; Hartwich, N. J.; Salge, O. „Weaponizing the GDPR: How Flawed Implementations Turn the Gold Standard for Privacy Laws into Fool's Gold,” in *ICIS 2022*, Koppenhága, 2022.
- [18] Mouha, R. „Internet of Things (IoT),” *Journal of Data Analysis and Information Processing*, 9., 2021.
- [19] Szczepaniuk, H.; Szczepaniuk, E. K. *Standardization of IoT Ecosystems Open Challenges, Current Solutions, and Future Directions*, CRC Press, 2022.
- [20] Kelemen-Erdős, Anikó; Mitev, Ariel. „Holisztikus szolgáltatásélmény-vendég-utazás és kölcsönös értékteremtés dimenziói az art-és romkocsmák példáján,” *Marketing & Menedzsment*, 250(3-4), 2016.
- [21] Babbie, Earl. *A társadalomtudományi kutatás gyakorlata.*, Balassi Kiadó, 2020.
- [22] Kelemen-Erdős, Anikó; Mitev, Ariel. „Tematikus szolgáltatásélmény art-és romkocsmák környezetben,” *Turisztikai és Vidékfejlesztési Tanulmányok*, %1. kötet2(3), 2017.
- [23] Kelemen-Erdős, Anikó; Molnár, Adél. „Cooperation or conflict? The nature of the collaboration of Marketing and Sales organizational units,” *Economics and culture*, %1. kötet16(1), 2019.
- [24] Krippendorff, K. *Content Analysis. An Introduction to Its Methodology*, Thousand Oaks: SAGE, 2018.

**EFFECT OF MICROWAVE
PRETREATMENT ON BIOGAS
PRODUCTION DURING ANAEROBIC
DIGESTION IN A MODEL EXPERIMENT****MIKROHULLÁMÚ ELŐKEZELÉS HATÁSA
A BIOGÁZHozAMRA SZENNYVÍZISZAP
ANAEROB ROTHASZTÁSA SORÁN
MODELLKÍSÉRLETBEN**

BAKOSNÉ DIÓSZEGI Mónika¹ – RÉKÁSI Márk² – SZÉCSY Orsolya³ –
BEZSENYI Anikó⁴ – NAGY-MEZEI Csenge⁵ – PAUKÓ Andrea⁶

Abstract

The use of medicines today shows a continuous increase, which was further stimulated by the COVID-19 pandemic. Dietary supplements, pain and fever relievers, antibiotics, and various hormone preparations flooded from the pharmaceutical industry have been routinely integrated into the lives of the population of welfare states. These enter the sewage from the human body. From the wastewater, they return to our natural waters through the water purification and water treatment plants, thus polluting the flora and fauna.

Keywords

safety of supply, anaerobic fermentation, biogas, drug contamination, health safety

Absztrakt

A lakossági és az egészségügyi gyógyszerfelhasználás mértéke folyamatos növekedést mutat, melyet, a COVID19 világvárvány tovább gerjesztett. A jóléti állapotok lakosságának életébe rutinszerűen épültek be a gyógyszeriparból elárasztott táplálék-kiegészítők, fájdalom és lázcsillapítók, antibiotikumok, valamint különböző hormonokat is jelentős mértékben tartalmazó készítmények. Ezek az emberi szervezetből a szennyvízbe kerülnek. A szennyvízből a víztisztító, vízkezelő üzemeken keresztül visszajutnak a természeti vizeinkbe, szennyezve ezáltal a növény- és állatvilágot.

Kulcsszavak

ellátás biztonsága, anaerob fermentáció, biogáz, gyógyszer-szennyezés, egészség biztonsága

¹ dioszegi.monika@bgk.uni-obuda.hu | ORCID: 0009-0000-3783-5691 | university associate professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi docens, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai mérnöki Kar

² rekasi.mark@atk.hu | ORCID azonosító: 0000-0003-2389-9103 | senior research fellow, Institute for Soil Sciences, Centre for Agricultural Research | tudományos főmunkatárs, Agrártudományi Kutatóközpont Talajtani Intézet

³ szecsy.orsolya@atk.hu | ORCID azonosító: 0009-0003-3811-4898 | research associate, Institute for Soil Sciences, Centre for Agricultural Research | tudományos munkatárs, Agrártudományi Kutatóközpont Talajtani Intézet

⁴ bezsenyia@fcsm.hu | ORCID azonosító: 0000-0002-4981-7869 | Budapest Sewage Works Ltd. Department of Environmental Protection, Biologist | Fővárosi Csatornázási Művek Zrt., Környezetvédelmi Osztály, Laboratórium Csoport, Biológus-mérnök

⁵ pribelszky@fcsm.hu | ORCID azonosító: 0009-0004-3376-2519 | Budapest Sewage Works Ltd., South-pest Wastewater Treatment Department, Technology group, process engineer | Fővárosi Csatornázási Művek Zrt., Dél-pesti Szennyvíztisztító Osztály, Technológiai csoport, technológus mérnök | Magyar Agrár- és Élettudományi Egyetem, Környezettudományi Intézet, Agrárkörnyezettani Tanszék, PhD-hallgató

⁶ andrea.pauko@bgk.uni-obuda.hu | ORCID azonosító: 0009-0004-9189-726X | Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering university assistant professor, | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai mérnöki Kar, egyetemi adjunktus

BEVEZETÉS

A gyógyszerrel és annak maradványaival szennyezett, növény és állatvilág emberi fogyasztásra is alkalmas része által a vegyi anyag visszajut az emberi szervezetbe, így egy körfolyamat alakul ki.

Az oxigénmentes eljárás termékeként energiahordozó is nyerhető, a biogáz. Egyre több víztisztító telep technológiai folyamatába beépül az anaerob rothasztás, mely a szennyvízből leválasztott szerves anyag degradációs lebontását segíti.

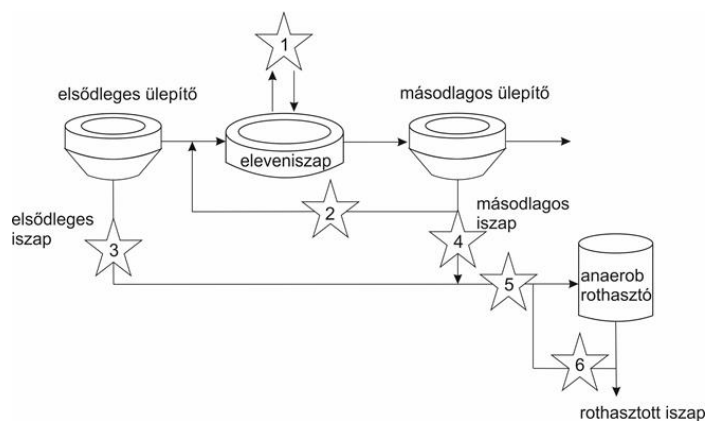
A kutatás célja az volt, hogy megvizsgáljuk, hogy a jelenlegi szennyvíztisztítási technológiába iktatott anaerob fermentáció, valamint az azt megelőző mikrohullámú előkezelés milyen hatást gyakorol a fermentáció során keletkező biogáz mennyiségére, mindamelllett, hogy az energiahordozó előállításának értéke ne változna.

A szennyvíziszap a szennyvíztisztítás mellékterméke. A szennyvíztisztítás során a termék folyékony és szilárd fázisra válik szét [1]. A szennyvíziszap „hulladékot” másodlagos nyersanyagként kell kezelni. A szennyvíziszap tökéletesen illeszkedik a CE koncepcióba, mint elemek, kémiai vegyületek, víz és energia forrása [2] [3]. A népességnövekedés, az új kommunális szennyvíztisztító telepek korszerűsítése és a régi létesítmények korszerűsítése az iszaptermelés növekedését eredményezi. Ezért az EU-ban nagy érdeklődés övezi feldolgozásának lehetőségeit. Az iszaphasznosítás vitathatatlan előnyökkel jár a környezet és a gazdaság számára. Jelentőségéből adódóan fontos folyamatos felügyelet alatt tartani annak szennyezettségi paramétereit.

A szennyvíziszap szennyezettségének vizsgálata alapvető, az újrahasznosítás céljából. A különböző szennyezők koncentrációjának csökkentése hozzásegíthet a szennyvíziszap hasznosíthatóságához. A szennyvíztisztítás technológiai folyamatába iktatva előszeregettel alkalmazzák az iszap anaerob rothasztását. A degradációt segítő művelet során, nem csak a szerves szennyezők távolíthatók el hatékonyan az alapanyagból, hanem a folyamatban részt vevő anaerob baktériumok táplálkozása során értékes zöld energiahordozó, biogáz keletkezik.

A rothasztókban lezajló biológiai folyamatok hatékonysága több tényezőtől is függ. Ilyen befolyásoló tényező lehet a hőmérséklet. A folyamat optimálisan végbe mehet 30–35 °C-os ún. mezofil hőmérsékletű fermentorokban, illetve 50–55 °C-os ún. termofil fermentorokban egyaránt.

Szintén a biogáz képződés serkentését válthatják ki az alapanyagok különböző termikus, vegyi és mechanikus előkezelési eljárásai vagy azok kombinációi. A szennyvíztisztítás technológiai folyamatába illesztett előkezelő eljárásokat a tisztítási folyamat legkülönbözőbb szakaszaiba szokták beépíteni. Erre mutat példát az 1. ábra, ahol a sorszámokkal jelölt csillag elemek utalnak az iszap előkezelési berendezésekre. Az 1. és 2. pontok esetében a levegőztető medencébe és a szekunder iszap recirkulációs ágába elhelyezett beavatkozás, a szennyvíz mennyiségének és hatékonyabb degradációjának céljából történik [4]. A primer, a szekunder és a kettejük kevert iszapjának ágába (5.) is behelyezhető egy-egy anyagfeldolgozó technológia. A 3. számmal jelölt helyen is eredményes a beavatkozás, mert a primer iszap önmagában is könnyen, jól bontható alapanyagként minősül [5].



1. ábra Iszapkezelési technológiák elhelyezkedése a szennyvíztisztítás folyamatában [6] 1. az eleveniszap egyidejű kezelése, 2. egyidejű kezelés az eleveniszap recirkulációs ágában, 3. primer iszap kezelése az anaerob rothasztás előtt, 4. szekunder iszap előkezelése az anaerob rothasztás előtt, 5. kevert iszap előkezelése az anaerob rothasztás előtt, 6. a rothasztóból kapott biotrágya cirkulációs ágában történő előkezelés

A 4. pontba beépített feldolgozást emiatt jobban preferálják, hiszen az itt visszamaradt alapanyag már nehezebben bontható összetételű. A kevert iszap (5. pont) kezelése ugyanakkor nem csak az iszap további rothasztásának hatékonyságát segíti elő, hanem annak ártalmatlanítását is. A fermentlé további fermentálása (6. pont), a rothasztó torony biogáz hozamának mennyiségét, minőségét növelheti. A folyamat ezen pontjában történő beavatkozás célja lehet a szárazanyag tartalom és a patogének további csökkentése. A technológia 1. és 2. pontjánál történő beavatkozás, a tartózkodási idő növelése, extra CO₂ kibocsátása az energiaköltség szempontjából jelentős. A 3., 4., 5., 6., pontnál megjelenő kezelések az anaerob degradáció hatékonyságát segítik elő.

Ezeknek a bomlást fokozó előkezeléseknek a hatását vizsgálták különböző szennyezőanyagok eltávolításának céljából. Nehézfémekkel szennyezett szennyvíziszap anaerob degradációját figyelték meg mikrohullámú előkezelés és vegyi kezelés együttes hatásának következtében. Megállapították, hogy a mikrohullámú savas rothasztás zárt rendszerben lehetővé teszi a minták gyorsabb lebontását, mint a hagyományos mineralizációval. A rothasztás folyamatát a megemelt nyomás és hőmérséklet gyorsítja ugyan, de a reakciórendszer speciális biztonsági berendezéseket igényel, ami a berendezés beszerzési költségeinek növekedésével jár. Másrészt a mikrohullámú mineralizáció kisebb mennyiségű reagenst használ, ami csökkenti a költségeket. Jelentős eredményeket értek el [7] a szennyvíziszap savas és mikrohullámú együttes előkezelést követő anaerob kísérleteivel, melynek szintén nehézfémekre tett hatását vizsgálták.

Antibiotikum rezisztens baktériumok és antibiotikum rezisztens gének sorsát vizsgálták az iszap anaerob lebontása során mikrohullámú-savas (MW-H), mikrohullámú (MW) és mikrohullámú-H₂O₂-lúgos (MW-H₂O₂) előkezeléseket követően. Az eredmények azt mutatták, hogy a kombinált MW-előkezelés, különösen az MW-H előkezelés, hatékonyan csökkentette az antibiotikum rezisztens baktériumok számát. A legtöbb antibiotikum rezisztens gén mennyisége is csökkent az előkezelés során. Az ezt követő anaerob degradáció az antibiotikum rezisztens baktériumok nyilvánvaló eltávolítását mutatta, de a legtöbb antibiotikum rezisztens gén feldúsult az anaerob rothasztás után [8].

Az irodalomkutatás eredményeképpen a mezofil tartományban végbemenő, anaerob rothasztásnak biogáz-hozamra gyakorolt hatását vizsgáltuk diklofenak, 17 β -ösztadiol és ösztron adott koncentrációjával szennyezett fölösiszap (kevert iszap) mikrohullámú előkezelését követően. Célunk a gázkihozatal mértékének megfigyelése az anaerob folyamatban résztvevő változó tényezők függvényében.

SZUBSZTRÁTUMOK MECHANIKUS ELŐKEZEKÉST KÖVETŐ ANAEROB BOMLÁSA

Az anaerob kísérlet alapjai

Az anaerob rothasztás kísérlet során négyféle inkubációs hőmérsékleten (35, 37, 40 és 42 Celsius fok) történő, 9 napig tartó rothasztás során, zárt rendszerben, kontrollált körülmények között vizsgáltuk meg, hogy kimutatható-e változás a keletkező biogáz mennyiségében a mikrohullámú előkezelés következtében. A kísérletek alapanyagainak megválasztásakor (fermentlé, ill. fölösiszap) törekedtünk a valós technológiai folyamatok, lépések követésére.

A mikrohullámú előkezelés során fölösiszapot felülszennyeztük a gyógyszerekkel, majd az így előkészített fölösiszapon alkalmaztunk mikrohullámú előkezelést, 70 °C hőmérséklet eléréseig. A fermentléhez ezt adtuk tápanyagként, és így került a keverék rothasztásra.

A kísérletet 2021. folyamán négy alkalommal végeztük el. Háromhavonta indítottunk új kísérletet, frissen vett alapanyagokkal. A különböző, mezofil hőmérsékletű rothasztásos kísérleteket termosztát szekrényben állítottuk be.

Alapanyag mintavétel, előkészítés és tárolás

A kísérlethez a Bácsvíz Zrt. kecskeméti telephelyéről származó friss fölösiszapot (főként szekunder fölösiszapot tartalmazó kevert iszapot) és fermentlevet (rothasztott iszapot) használtunk. A szárazanyag-tartalom (TS) és szerves szárazanyag tartalom (oTS) méréshez szükséges mennyiségű fermentlevet 2 mm-es szitán átszűrtük, a fölösiszapot gépi keverővel homogenizáltuk. A kísérletet a résztvevő anyagok TS és az oTS mérése után indítottuk. A mintavételi és a kísérletindítási időszakban a fermentlevet 20 °C-on, a fölösiszapot 4 °C-on tároltuk. Az iszapokat kísérletben való felhasználás előtt felrázva homogenizáltuk.

A fölösiszap felülszennyezése gyógyszerekkel

A mikrohullámú előkezelés során a fölösiszapot addicionáltuk gyógyszervegyületekkel, illetve ezen alkalmaztunk mikrohullámú előkezelést. Az addicionált, és a kezeléstől függően mikrohullámú előkezelést kapott fölösiszaphoz kevertük hozzá a fermentlevet. A gyógyszeres törzsoldatok elkészítéséhez 0,1 g diklofenakot, illetve 17 β -ösztadiolt metanollal külön lombikokban 100 ml-re egészítettük ki (1g/l). Az így elkészített metanolos törzsoldatokat további felhasználásig hűtőben tároltuk. A kísérlet indításakor mindkét törzsoldatból csapvízzel 10-szeres hígítást készítettünk. A kísérletek során az alapanyagok addicionálásához ezeket a 100 mg/l-es koncentrációjú munkaoldatokat használtuk fel.

A cél a 100 μ g/l koncentráció elérése volt a rothasztásra kerülő, bekevert anyagok egészében. Összesen 2 l fölösiszapot szennyeztünk egyszerre felül gyógyszerekkel. A TS

és oTS alapján kiszámított fölösiszap térfogathoz kevertük a szükséges térfogatú munkaoldatot. A 2 literbe kísérlet beállításaként eltérő térfogatú, de hozzávetőlegesen 7 ml munkaoldatra volt szükség.

Mérőhengerrel kimértünk 2 liter fölösiszapot, fém vödörbe öntöttük, majd a festékkerő fúrószárral 5 percig kevertük a homogén állapot biztosításához. Ezután további folyamatos keverés mellett hozzáöntöttük a szükséges térfogatú gyógyszeres munkaoldatot. A keverést további 5 percig folytattuk, a homogén addíciónálás eléréshez (2. ábra).



2. ábra A fölösiszap homogenizálása festékkerő fúrószárral, az addíciónálást követően. [saját kép]

A gyógyszerrel felül szennyezett fölösiszap mikrohullámú előkezelése és reaktorok beindítása

A mikrohullámú előkezelés során egy 800 ml-es főzőpohárban 500 ml fölösiszapot 2+2 percig melegítettünk 800 W-on, az első két perc után átkeverve, így értük el a 70°C-os hőmérsékletet.

A megelőző TS és oTS mérések alapján állítottuk be a reaktorüvegekben a fölösiszap és fermentlé egymáshoz viszonyított arányát, a német VDI 4630 (Szerves anyagok fermentálása) [9] ajánlása alapján. A kiszámított térfogatú addíciónált fölösiszaphoz gyógyszermentes fermentlevet adtunk, így egészítettük ki 400 ml térfogatra a reaktorüvegek tartalmát. A rothasztást négy hőmérsékleten (35/37/40/42°C) végeztük (1. táblázat). Az így feltöltött üvegekre szeptumos kupak került, majd 1 percig buborékolattuk nitrogénnel az anaerob körülmények létrehozásához.

Kezelés	Alapanyag	Gyógyszer	Mikrohullámú előkezelés (ME)	Anaerob rothasztás (AR)
kontroll	fölösiszap/ fermentlé	+	-	+
mikrohullámú előkezelés	keveréke	+	+	+

1. táblázat. A kísérlet kezeléseinek vázlata [saját táblázat]

A fermentációs batch eljárás során a szubsztrátumot csak egyszer – a vizsgálat kezdetén – táplálják be a rendszerbe. Emiatt nevezik szakaszos vizsgálatnak.

Az összeállított reaktorokat termosztátban 9 napig a megfelelő hőmérsékleten inkubáltuk. A kísérletek bontására 9 nap múlva került sor. Ekkor következett a pH mérés, a mintavétel analízise, valamint a TS és oTS mérések.

VIZSGÁLATI MÓDSZEREK

TS (szárazanyag tartalom), oTS (szerves szárazanyag tartalom) mérése

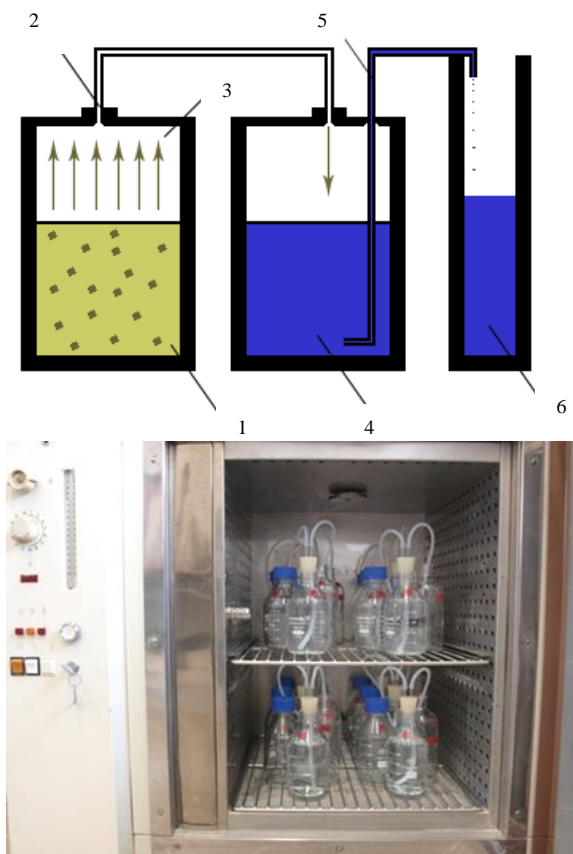
Az alapanyagok szárazanyag tartalmát és szerves szárazanyag tartalmát a standard methods (APHA-AWWAPCF, 1999) ajánlás alapján mértük. A fölösiszap és fermentlé pH-mérését az MSZ 1484-22:2009 szabvány 8.1. szakasza alapján végeztük. A mérésekhez Inolab Multi 9310 készüléket használtunk, a hozzá tartozó SenTix® 980 pH-elektóddal.

Biogáz térfogatának mérése

A keletkező gázok mennyiségét tömegmérés alapján végeztük el. A fejlődő gáz által kiszorított folyadék tömegének növekedését mértük. A mérés a kísérlet elején naponta, majd kétnaponta történt.

A feltöltés után az erjesztőt lezártuk és csak a kísérlet végén kerül kinyitásra. Az eljárás előnye a nagy térfogategységre vetített biogáz hozam, melynek mértéke az időben egyre csökken a további betáplálás hiánya miatt. Tehát a baktériumok lehetőségeik szerint az összes tápanyagot a vizsgálati idő alatt felemésztik. Mikor már nincs gáztermelés – legalábbis nem számottevő –, akkor az elhasználódott anyagot el kell távolítani, és újra feltölteni a rendszert. Az anaerob rothasztást a VDI 4630 Szerves anyagok fermentálása német ajánlás alapján végeztük el.

A batch rendszernek a betáplálás minősége szerint három típusa ismert: folyékony, félszáraz és száraz eljárás. Míg a félszáraz rendszer szárazanyag tartalma 15%, addig a folyékony rendszeré csak 2–8% (szerves szárazanyag-tartalma körülbelül 40–50%), a száraz rendszer szárazanyag-tartalma pedig 25%-nál nagyobb. Az itt leírt kísérletben a szubsztrátumot folyékony eljárásként rothasztottuk.



3. ábra A batch mérés jelképes működési ábrája és fényképe [10]

1. A fermentálni kívánt szubsztrátum, 2. Polipropilén cső, 3. Gáztér, 4. Mérőfolyadék, 5. Szilikon cső, 6. Gázhozam mérő

A 3. ábra alapján, a különböző hőfokon történő fermentáció során fejlődő gáz a gáztérből (3) a polipropilén csövön (2) keresztül a mérőfolyadékkal megtöltött tartály légterébe áramlik. A reaktor üvegekben keletkező biogáz mennyiség változással (térfogat- és nyomásnövekedéssel) egyidejűleg a második tartályban lévő mérőfolyadék (4) a szilikon csövön (5) át a gázhozam mérőhengergebe (6) préselődik. A keletkezett biogáz térfogata megegyezik a kiszorított folyadék térfogatával, a gáz, kompresszállás hiányában, standard nyomáson, 101325 Pa-on képződik.

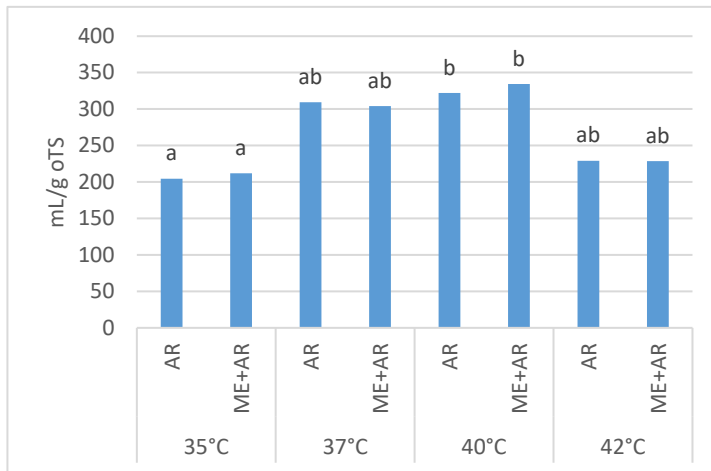
MIKROHULLÁMMAL ELŐKEZELT ALAPANYAG KÍSÉRLETÉNEK EREDMÉNYEI

Biogáz hozam eredmények

A kísérlet során fejlődött biogáz hozam az elvégzett varianciaanalízis alapján szignifikánsan nagyobb lett a 40°C-os kezelések átlagában, mint a 35°C-osban (4. ábra). A diagramon az oszlopok fölött látható a és b betűjelek a varianciaanalízis alapján szignifikáns eltérést jelölnek $p < 0,05$ valószínűségi szinten. A másik két hőmérsékleten (37°C és 42°C)

nem tudunk szignifikáns különbséget kimutatni. Ha csak a hőmérsékletet vesszük figyelembe, a biogáz hozam a következő sorrendben növekedett: 35, 42, 37 és 40°C.

A mikrohullámú előkezelés hatását vizsgálva megállapítható, hogy a biogáz hozamokban a mikrohullámú előkezelés nem okozott érdemi eltérést az előkezelést nem kapott mintákhoz képest. Az előkezelés néhány mL gázhozam növekedést, vagy csökkenést okozott csupán. A változás egyik esetben sem volt szignifikáns.



4. ábra. Biogáz hozamok a mikrohullámú előkezelés kísérletben, az eltérő hőmérsékleteken beállított rothasztások eredményeképpen. AR: anaerob rothasztás, ME: mikrohullámú előkezelés.

A melegítés hatását vizsgáló előkísérletben korábban megállapítottuk, hogy térfogatvesztéséget a mikrohullámú előkezelés következtében nem tudunk kimérni.

ÖSSZEFOGLALÁS

A kapott eredmények és az elvégzett statisztikai elemzések alapján nem lehetett egyértelmű tendenciát kimutatni az anaerob rothasztás hőmérsékletének növekedése és a gázképződés mennyisége között a gyógyszervegyületekkel szennyezett szennyvíziszap rothasztása során. A mikrohullámú előkezelés nem okozott változást a gázkihozatalban egyik vizsgált hőmérsékleten sem. Az anaerob folyamat által biztosított környezeti szennyezés elleni védelem, a gyógyszer összetevők lebomlásának mértéke és az esetleges degradáció viselkedése további vizsgálatok és elemzések után állapítható meg.

FELHASZNÁLT IRODALOM

- [1] Fytli, D.; Zabaniotou, A. Utilization of sewage sludge in EU application of old and new methods—A review. *Renew. Sustain. Energy Rev.* 2008, 12, 116–140.
- [2] Neczaj, E.; Grosser, A. Circular Economy in Wastewater Treatment Plant—Challenges and Barriers. *Proceedings 2018*, 2, 614. [Google Scholar] [CrossRef]
- [3] Healy, M.G.; Clarke, R.; Peyton, D.; Cummins, E.; Moynihan, E.L.; Martins, A.; Béraud, P.; Fenton, O. Resource recovery from sewage sludge. In *Sewage Treatment*

- Plants: Economic Evaluation of Innovative Technologies for Energy Efficiency; Stamatelatou, K., Tsagarakis, K.P., Eds.; IWA Publishers: London, UK, 2015; pp. 139–162. ISBN 9781780405025. [Google Scholar]
- [4] S.I. Perez-Elvira, P.N. Diez; F. Fernandez-Polanco: Sludge minimisation technologies, *REv. Environ. Sci. Bio/Technol.*, 2006., 5(4). pp.: 375–398.
- [5] Ge.e, H.Q., Jensen, P.D. Batstoon, D.J.: Pre-treatment mechanism during thermophilic-mesophilic temperature phased anaerobic digestion of primary sludge. *Water Res.* 44 (2010)., pp.: 123–130.
- [6] H., Carrère; Dumas, C; Battimelli, A; Batstone, D.J.; Delgenés, J.P.; Steyer, J.P.; Ferrer, I.: Pretreatment methods to improve sludge anaerobic degradability: A review, elsevier.com/locate/jhazmat, *Journal of Hazardous Material*, 183 (2010) pp.:1–15.
- [7] E. Veschetti, D. Maresca, D. Cutilli, A. Santarsiero, M. Ottaviani, Optimization of H₂O₂ action in sewage-sludge microwave digestion using Δ pressure vs. temperature and pressure vs. time graphs, *Microchemical Journal*, Volume 67, Issues 1–3, December 2000, Pages 171-179
- [8] Juan Tong, Jibao Liu, Xiang Zheng b, Junya Zhang a, Xiaotang Ni, Meixue Chen, Yuansong Wei, Fate of antibiotic resistance bacteria and genes during enhanced anaerobic digestion of sewage sludge by microwave pretreatment *Bioresource Technology* Volume 217, October 2016, Pages 37-43
- [9] VDI 4630: Fermentation of organic materials – Characterisation of the substrate, sampling, collection of material data, fermentation test, 2006.
- [10] Mónika Bakosné Diószegi, Miklós Horváth Effects of Mechanical Pretreatment on Wheat Straw Fermentation In: Rácz, Pál (szerk.) *IESB 2014: Nemzetközi Gépész és Biztonságttechnikai Szimpózium Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságttechnikai Mérnöki Kar* (2014) pp. 76-88., 13 p. ISBN: 9786155460081

INVESTIGATION OF ABLATION DECONTAMINATION TECHNOLOGY GENERATED BY LASER LIGHT**LÉZERFÉNY ÁLTAL GENERÁLT ABLÁCIÓS DEKONTAMINÁLÁSI TECHNOLÓGIA VIZSGÁLATA**BODOR Károly¹ – ZAGYVAI Péter²**Abstract**

The article describes the operating principle and feasibility of a new decontamination technology. One of the very important parameters for the storage of radioactive waste is its volume. Due to the ablation technology, the surface contamination of solid objects can be eliminated by collecting the particles detached by ablation, thus maximizing the volume / impurity volume ratio of the purified material. Most technologies produce large amounts of secondary contamination, the ablation process is not, inexpensive, fast, and can be deployed almost anywhere. In this article I present the results of our radioactive material decontamination process, during which the contaminated surface was treated three times.

Keywords

Radiation protection, Decontamination, Ablation, Photoraser, Radioactive waste

Absztrakt

A cikk bemutatja egy új dekontaminálási technológia működési elvét, megvalósíthatóságát. A radioaktív hulladékok tárolásának egyik igen fontos paramétere a térfogat. Az ablációs technológia segítségével a szilárd anyagok felületi szennyezettségét meg lehet szüntetni, úgy, hogy a leválasztott részecskéket összegyűjtjük, így maximalizálni lehet a megtisztított anyag térfogata/szennyezés térfogata arányt. A legtöbb technológia nagy mennyiségű másodlagos szennyezést termel, az ablációs eljárás nem, olcsó, gyors, szinte bárhol bevethető. A cikkben bemutatom az általunk elvégzett radioaktív anyag dekontaminálási eljárás eredményeit, mely során háromszori kezelésnek vetettük alá a szennyezett felületet.

Kulcsszavak

Sugárvédelem, Dekontamináció, Abláció, Photoraser, Radioaktív hulladék

¹bodor.karoly@ek-cer.hu | <https://orcid.org/0000-0002-1612-8207> | Radiation protection expert, Centre for Energy Research | Sugárvédelmi szakértő, Energiatudományi Kutatóközpont

²zagyvai.peter@ek-cer.hu | <https://orcid.org/0000-0002-8121-8452> | Radiation protection advisor/Sugárvédelmi tanácsadó, Energiatudományi Kutatóközpont

BEVEZETŐ

A radioaktív anyagok alkalmazása széleskörű, a nukleáris ipar mellett a különféle iparágakban, az oktatás, a kutatás és az egészségügy területén is elterjedt. Radioaktív hulladék legnagyobb mértékben az atomreaktorok működése során keletkezik, de a többi alkalmazásnál sem elhanyagolható ennek mennyisége. A reaktorok kiégett fűtőelemei is ide sorolandók, ha újrafeldolgozásuk nem történik meg. A most működő atomreaktorok többségét le fogják szerelni az elkövetkező 10-20 évben.

A radioaktív hulladékok térfogatának jelentős részét a kis- és közepes aktivitású radioaktív hulladékok adják. (A radioaktív hulladékokat a 2/2022. OAH rendelet 12. melléklete szerint kell besorolni. [5]) A kis- és közepes aktivitású radioaktív hulladék jelentős részét képezik azon szilárd tárgyak, melyek felületén van radioaktív felületi szennyezettség (radiokontamináció). Továbbá egy nukleáris baleset esetén nagy mennyiségben keletkezhetnek felületen szennyezett anyagok a szétterülő radioaktív anyagok hatására, melyek döntő többsége kis- és közepes aktivitású radioaktív hulladéknak fog minősülni. A kis- és közepes aktivitású radioaktív hulladéktárolók kapacitása véges, emiatt nagyon fontos a hulladékok térfogatának csökkentése. A baleseti szituációban keletkező jelentős mennyiségű radioaktív hulladék kimerítheti a tárolási lehetőségeket, ezért fontos ezen felületen szennyezett anyagok megtisztítása, így redukálva a radioaktív hulladékok térfogatát. A végleges tárolók véges kapacitásai miatt a hulladékok temetkezési költségei fokozatosan emelkednek.

A legtöbb dekontaminálási (tisztítási) eljárás során a szennyezett felületről ugyan eltávolítják a szennyezettséget, de nagyobb mennyiségű kisebb aktivitású másodlagos szennyezett anyag keletkezik pl. a magasnyomású mosás során (1. ábra). A felületi szennyezettség nehezen eltávolítható, amennyiben a felülethez erősen kötődik a radioaktív szennyező (fixált szennyezettség), illetve amennyiben a felületi réteg belsejébe vándorol a radioaktív anyag. A megfelelően megtisztított anyagokat inaktívvá lehet nyilvánítani, így azokat továbbra is lehet használni. Az inaktívvá nyilvánítás radiokémiai laboratóriumi anyagok és területek esetén az MSz 62/7:2017 szabvány, általános mentesítés esetén a 2/2022. OAH rendelet, valamint EURATOM-segédanyagok [4] alapján történhet.

A hulladékokat kondicionálják a kisebb térfogat eléréséhez, ez lehet tömörítés, szilárdítás, hamvasztás, égetés. A hulladék feldolgozás előtt célszerű a hulladékokat pihentetni, így a rövidebb felezési idejű izotópok elbomlanak, mely csökkenti a hulladék aktivitását és a hulladék által létrehozott dózisteljesítményt.



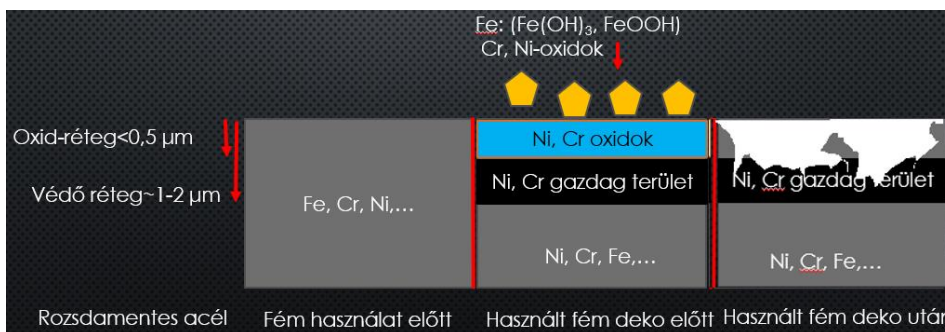
1. ábra: Különböző dekontaminációs eljárások, [3]

LÉZER ABLÁCIÓS DEKONTAMINÁCIÓ

A lézerfényt előállító kompakt berendezések teljesítménye elérheti az 1-2 kW-ot. A lézerfényt a tisztítandó felületre ráfókuszálva lokális felmelegítés érhető el. Elegendően nagy teljesítmény mellett a felületen a hirtelen hőmérsékletváltozás hatására mechanikai feszültség alakul ki az anyag és a felületi szennyezettség között, így elérhető, hogy a felületről leváljanak, lepattogjanak, elpárologjanak a felületi szennyező részecskék. A lézerfényvel történő tisztítást manapság már használják pl. rozsdá, olaj szennyezés eltávolítására az iparban. Radioaktív hulladékok tisztítására a jelenlegi berendezések nem alkalmasak, mivel a felületről a levegőbe kerülő radioaktív anyagok nagyon veszélyesek, beléggzéssel (inhaláció) belső sugárterhelést okoznának. Ahhoz, hogy akár hordozható dekontamináló állomást lehessen kialakítani lézerberendezéssel, a kompakt lézerberendezés mellett a levegőbe kerülő radioaktív részecskék hatékony összegyűjtésére alkalmas technológiát kell a rendszerhez csatlakoztatni. Amennyiben ez megvalósulna, akkor hatékony dekontaminálási alternatíva lehet a lézeres dekontaminálás, mivel a dekontaminálás folyamata a többi technológiához viszonyítva viszonylag gyors, és ellentétben a jelenlegi technológiákkal, ez a rendszer a másodlagos szennyezést (levegőbe került radioaktív részecskék) képes lenne igen kis térfogatba összegyűjteni.

Atomreaktor primervízének kontaminációja

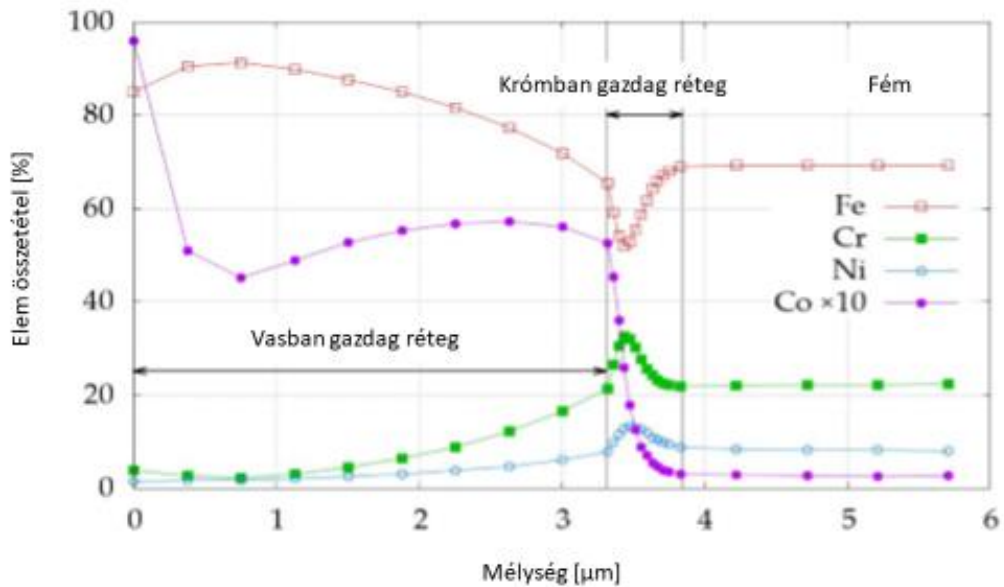
A vízhűtésű atomreaktorok primer vízkörében kioldódás vagy a felületről való leválás miatt megjelennek a fűtőelemek burkolatából, a reaktortartályból és egyéb fémes szerkezeti anyagokból (pl. vízcsövek felületei) származó, úgynevezett korróziós termékek. Ezen anyagok felaktiválódva és a primer víz csőrendszerébe bekerülve bizonyos területeken lerakódhatnak és feldúsulhatnak. A vas a primer vízzel reakcióba lép és vasoxidot hoz létre. A felületből kioldódott vas miatt a felületihez közeli réteg az eredetnél nagyobb arányban tartalmaz krómot és nikkelt [1]. A mintegy 97,5%-ban cirkóniumot tartalmazó fűtőelemek fémfelületén is főleg króm és nikkelt oxidok keletkeznek. Bár a dekontaminálás során ezen oxidok eltávolíthatók, de a sérült felületen újra kialakul az oxid réteg (2. ábra) [1].



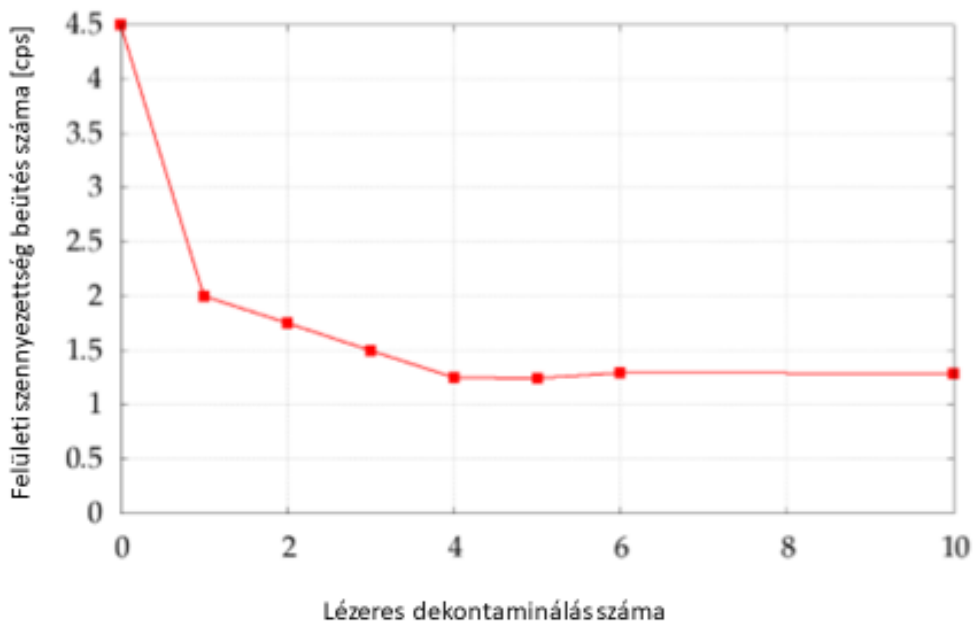
2. ábra: Korróziós folyamatok a primer vízben lévő rozsdamentes acél felületeken, [1]

^{60}Co keletkezik a rozsdamentes acél felületén a kobaltot tartalmazó filmrétegben, a ^{60}Co által emittált gamma fotonok nagy energiájúak (1,17 MeV; 1,33 MeV). A viszonylag nagy aktivációs hatáskeresztmetszet és az 5,27 éves felezési idő miatt az elszennyezett cső dózisteljesítményének döntő többségét a ^{60}Co adja a felaktivált korróziós termékek közül. Amennyiben a felület 0,5-1 μm -ét távolítjuk el, akkor a felületi szennyezettségből származó

dózisteljesítmény drasztikusan csökken. További korróziós termékek nem válnak le, mert a védőréteg nem sérül. Emiatt a lézeres kezelés első pár lépésével jelentősen csökkenthető a felületi szennyezettség és az abból származó dózisteljesítmény értéke (3-4. ábra) [1].



3. ábra: Vas, króm, nikkél és kobalt mélységi eloszlása egy vizsgált rozsdamentes acél felületén [1]

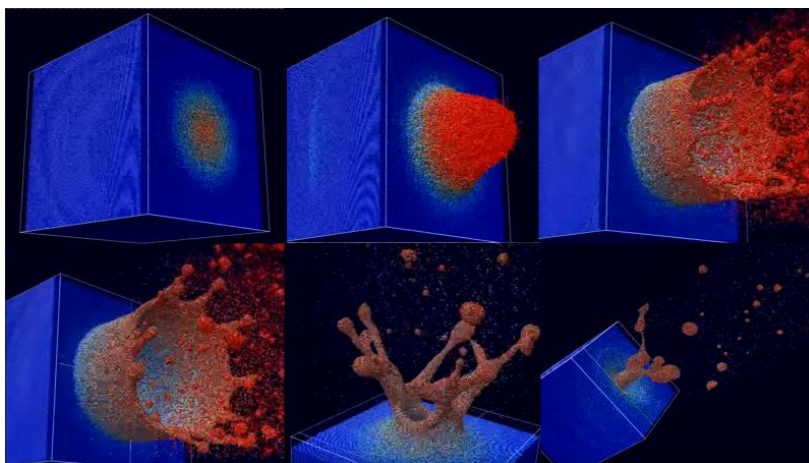


4. ábra: A felületen mérhető szennyezettség által okozott beütésszám csökkenése a lézeres kezelések függvényében, [1]

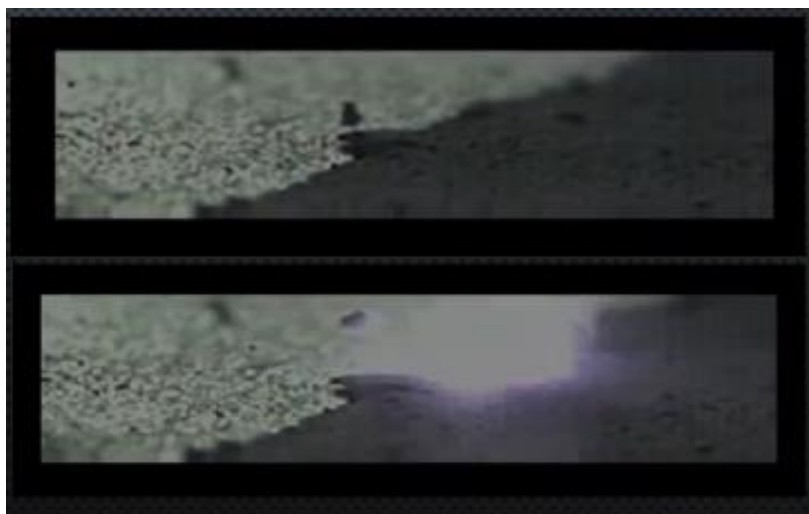
A fűtőelem gyártás során a fűtőelem külső felülete tartalmazhat ^{235}U -tartalmú urán-oxid-szennyezést, a besugárzás hatására hasadó szennyező tovább növelheti a primer víz szennyezettségét. Amennyiben pl. lézeres dekontaminálást alkalmazunk a friss (tehát még nem használt) fűtőelem felületén, akkor a primer víz szennyezése is csökkenthető [1].

Ablációs tisztítás

A lézeres dekontamináció során a fókuszpontban a kialakuló mechanikai feszültség hatására a felületi szennyező részecskék lerobbanhatnak a felületről (5. ábra), mivel a fókuszpontban kialakuló gyors hőmérsékletnövekedés miatt a felület és a felületi szennyező anyag hőtágulása eltérő mértékű. A pulzált módban használt lézer pontról pontra alakítja ki a hőmérsékleti góccokat, így egyfajta felületi rezgés, lökeshullám jön létre, ami szintén elősegíti a szennyező felület leválását (6. ábra) [1].



5. ábra: Felületi anyag kilökődés-robbanás a lézeres kezelés által kialakuló lokális hőmérsékleti gradiens hatására, [1]



6. ábra: Nagy méretű szennyező rész leválása a felületről a lézeres kezelés pillanatában, [saját szerkesztés]

Ablációs küszöb

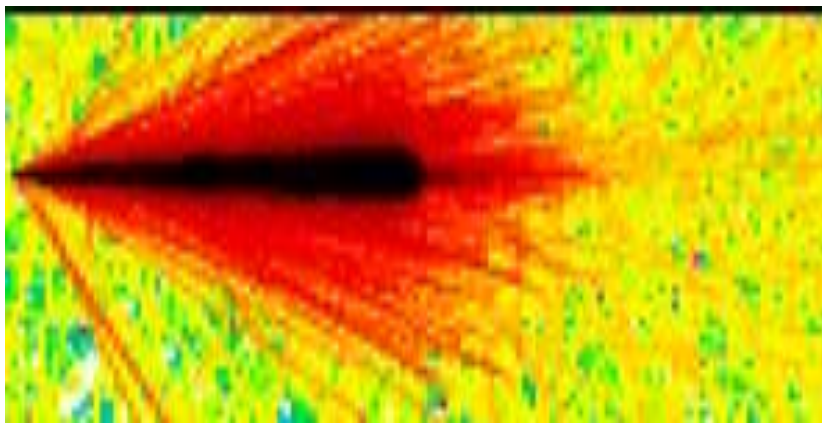
A lézer besugárzás hatására kialakuló hőmérséklet emelkedés hatására a besugárzott terület megolvadhat (termikus abláció). Ezt el lehet kerülni, amennyiben a lézerberendezés képes érzékelni a besugárzott anyag reflektáló képességét, így a berendezés érzékeli, hogy a felületi szennyezés eltávozik a felületről, és tiltja a lézert, ezáltal elkerülhető a felület részleges megolvadása, károsodása [1].

Károsodási küszöb

A lézerkezelt fémtárgy megolvadhat, amennyiben hosszú lézerimpulzust alkalmazunk, illetve nagyteljesítményű a lézerberendezés. A szennyezés módosítja a felület minőségét, a károsodási küszöb növekszik a felület érdességével. A küszöb csökken, amennyiben a besugárzott terület hővezetése alacsony, mivel ez kedvez a lokális hőmérséklet-emelkedésnek. A károsodási küszöböt tovább csökkenti a többszörös besugárzás. Fázisátalakulások jönnek létre a besugárzásokkor, ezek megváltoztatják az anyag reflektáló, hővezető tulajdonságait, és a károsodási küszöböt is [3].

Szennyező filmréteg

Az anyag és szennyező filmréteg határán megváltozik a reflexió, általában csökken, mert az érdesség lecsökken, így a hőmérséklet növekedése megnövekszik. A lézer besugárzás mélysége, penetráló képessége csökken a lézerintenzitás csökkentésével, a nyaláb ún. Molière sugara csökken (7. ábra). Vastag szennyezettség esetén a beérkező lézerimpulzus szóródik, így a hőmérsékletváltozás sem pontszerű. A nagyobb kiterjedésű, de még lokális hőmérséklet emelkedés hatására a vastagabb szennyező filmréteg esetén nagyobb darabok válhatnak le a felületről (8. ábra) [1]. Vékony filmréteg esetén a leváló részecskék méreteloszlása jóval kisebb, ami megnehezíti ezek kiszűrését a levegőből.



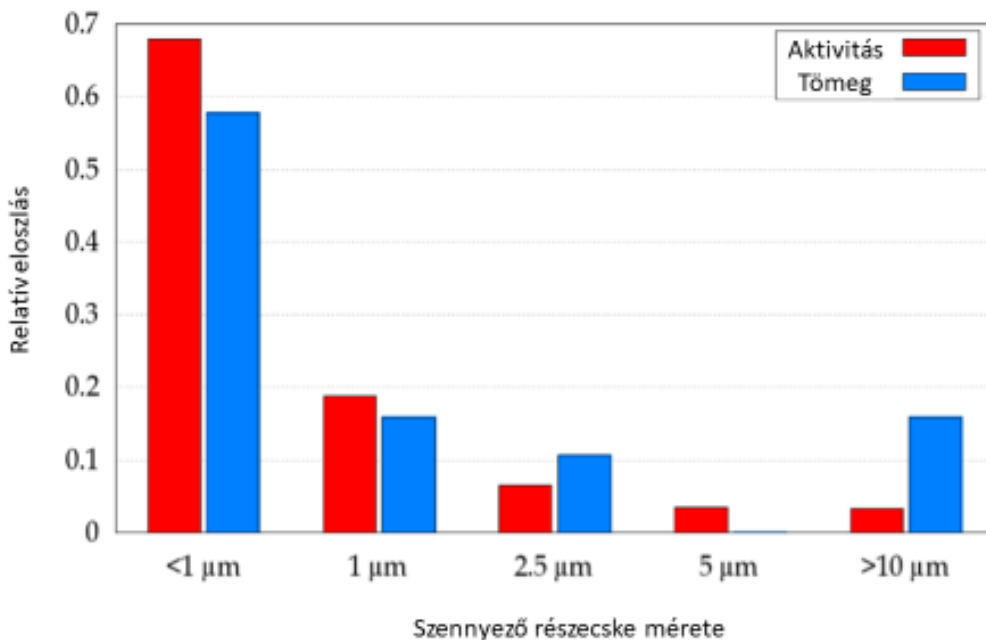
7. ábra: A lézernyaláb fokozatos szóródása-széttartása (Molière sugár), [saját szerkesztés]

Leváló darabok méreteloszlása

A lézeres dekontamináció hatására a felületről lepattanó részecskék méreteloszlása változatos. A leváló részecske darabok döntő többségének a mérete kisebb, mint 1 mikrométer (8. ábra). A mikrométer alatti méret tartományú részecskék adják a felületi szennyezettség jelentős részét. A felületi szennyező filmrétegben mechanikai törések keletkeznek,

amennyiben vastag a felületi lerakódás, ekkor a leváló darabok mérete meghaladhatja a 10 μm -t.

A levegőbe kerülő részecskéket nagyteljesítményű levegő elszívó berendezéssel kell elszívni, a dekontamináló helyiségnek mindig negatív nyomásúnak kell lennie, így elkerülhető, hogy szennyezett levegő a külső térbe kerüljön. A levegő elszívó rendszerbe többszörös szűrési pontokat kell kialakítani, amik képesek a nagyobb és a kisméretű részecskéket is kiszűrni a levegőből, a rendszer kiegészíthető vizes elnyelő rendszerrel is.



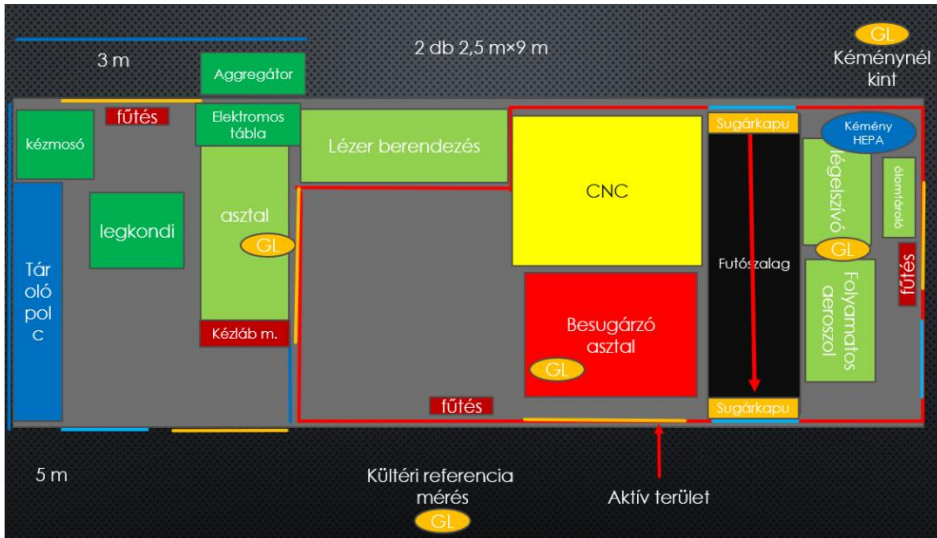
8. ábra: A felületről leváló részecskék relatív eloszlása méret szerint, [1]

AZ ÚJ TÍPUSÚ DEKONTAMINÁLÁSI TECHNIKA MŰKÖDÉSE

A tesztelt hordozható lézerberendezése teljesítménye 1 kW, az ismétlési frekvenciája 15-50 kHz között változtatható. A lézersugár szkennelő üzemmódban végig pásztázza felületet, a lézer besugárzás szélessége állítható 0 – 100 mm szélesség között. A lézerfény fókusz távolsága is beállítható. A besugarazandó felületet felületi szennyezettségméréssel kell megmérni, így ismert a felületi szennyezettség nagysága és kiterjedése, pozíciója a szennyezett tárgyon. A felületi szennyezettség mérése és a lézerfényt kibocsátó pisztoly pozícionálása robotkarral is megoldható. Az egyes lézeres kezeléseket követően újra le kell mérni a felületi szennyezettséget, így újra megállapítható, hogy mennyit csökkent a felületi szennyezettség mértéke, kiterjedése, ebből meghatározható az egyes kezeléseket dekontaminációs hatásfoka. A kezeléseket addig kell végezni, amíg a beavatkozási szint alá nem csökken a felületi szennyezettség értéke.

A lézeres dekontaminálást állandó munkateremként vagy telepíthető állomásként is meg lehet valósítani. Utóbbi több konténerből állhat (iroda, fürdő, tároló részleg) és a fő konténer, amiben a lézerberendezés és a dekontamináló részleg el van helyezve. A konténerrendszer szétszerelve szállítható és adott munkaterületen össze lehet állítani. A tervezett

konténer besugárzási területét légmentesen kell leválasztani, így a levegő elszívás megkísérelése esetén sem tud kijutni szennyezett levegő. A levegő elszívó rendszerbe épített aktivitáskoncentráció mérő eszközök segítségével lehet mérni a konténerből kibocsátott levegő minőségét. Ha egy beállított érték fölötti értéket jelez a rendszer, akkor a lézeres kezelés automatikusan leáll, a levegőszűrő betétek radioaktív hulladékként kezelendők csere esetén (9. ábra).



9. ábra: A lézer elven működő dekontamináló rendszer (Photoraser) tervezett elrendezése, (GI nagyérzékenységű dózisteljesítmény mérő, CNC: programozható szerszámgép), [saját szerkesztés]

A konténer műszaki kialakításának követelményei:

- A konténer szabvány méretű (9*2,5 m), mely bővíthető, mobilis, így bárhová telepíthető a rendszer a megrendelő kérésére, ha a sugárvédelem megfelelőségét az Országos Atomenergia Hivatal elfogadta.
- Két részből áll: aktív zóna, valamint irányító helyiség.
- A konténerrendszert fizikai védelemmel kell felszerelni („C”-szint 190/2011 Korm. r. szerinti [2]), a dekontaminálásra beérkező anyagok aktivitása, izotóp összetétele változatos lehet, a „C” szintű védelem elegendő mozgásteret biztosít a rendszernek, hogy fogadni tudja a különféle radioaktív hulladékokat.
- Audio-vizuálisan kell jeleznie a konténer sugárvédelmi kijelző rendszerének szintemelkedés esetén.
- A sugárkapu bejelzése esetén a rendszer leállítja a már kezelt anyag kiadását.
- A sugárvédelmi mérő rendszerrel a beléptető rendszert össze kell kapcsolni, amennyiben az aktív zónában a személyzet elszennyeződik, akkor a sugárkapu nem enged ki onnan, ebben az esetben a sugárvédelmi szakértő elrendeli a személy dekontaminálását, illetve belső kontamináció vizsgálatát (egésztést számlálás).

- Amennyiben a dekontaminációs eljárás során hiba lép fel, pl. csökken vagy megszűnik a depresszió, valamint ha a kibocsátást ellenőrző berendezés emelkedett értéket mutat, akkor a beépített automatikának azonnal le kell állítani a lézeres kezelést.
- A dekontamináló zónába csak kiegészítő személyi dózismérőt (EPD-t) viselve lehet belépni, a beléptető rendszert össze kell kapcsolni az EPD rendszerrel, így csak EPD összerendeléssel lehetséges a belépés.
- A konténer belső felületeit dekontaminálható felületekkel kell ellátni, sima felületek.
- A kéménybe telepített mintavevő rendszert úgy kell kialakítani, hogy izokinetikus mérés legyen lehetséges a kibocsátás meghatározásához.
- Ólom árnyékolású sugárforrástároló szekrényt kell alkalmazni a használt légszűrők átmeneti tárolására.

AZ ÚJ TECHNOLÓGIA ELŐNYEI, MEGVALÓSÍTHATÓSÁGA

A lézeres dekontamináció főleg szilárd felületek tisztítására alkalmas. Hatékony eljárás, gyors, valamint a másodlagos szennyezés összegyűjtésre kerül, így a másodlagos szennyezés térfogata minimális. A lézeres dekontaminálást korábban kísérleti körülmények között kipróbálták [1], azóta a lézerberendezés fejlődése végett már kompakt, hordozható, kW teljesítményű lézerek is elérhetőek a piacon. Ugyanakkor ezen berendezéseknél csak egyszerű levegő elszívás van, mely a lézerpuska, azaz a kezelést végző személy irányába szívja a levegőt. Ezen berendezések alkalmatlanok a radioaktív anyagok dekontaminálásra (bár a lézer teljesítmény elegendő), mivel nem ilyen célra lettek tervezve. A biztonságos dekontamináláshoz szükséges egy olyan technológiai rendszer kiépítése, mely megfelelően összegyűjti a levegőbe kerülő radioaktív szennyezést és meggátolja a további kontaminációt, inhalációt.

Előnyök:

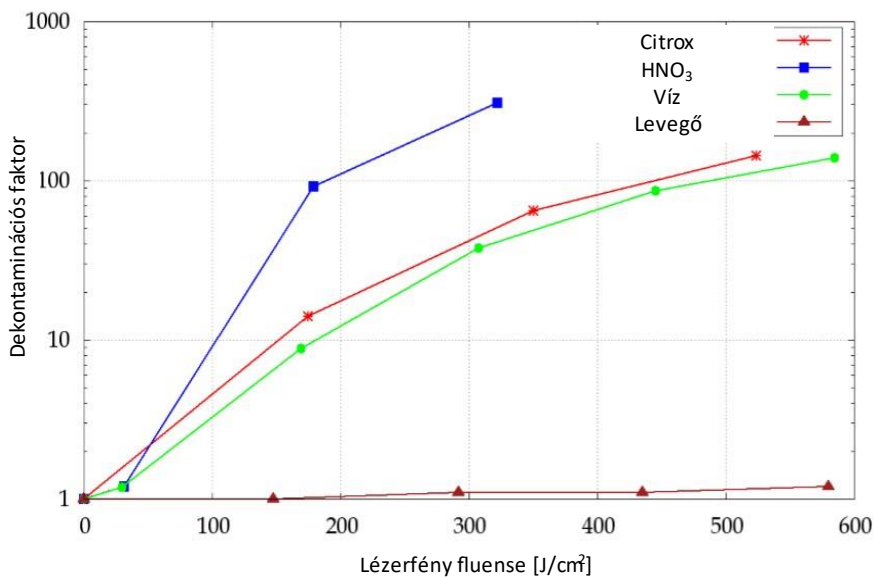
- A dekontaminálás megfelelő robotikai felszereléssel automatizálható.
- Széles körű hasznosíthatóság, radioaktív szennyezők mellett egyéb szennyezettség is tisztítható.
- A radioaktív anyag összegyűjthető, így a kis térfogat miatt ennek temetési költsége nem jelentős.
- A munka végzéséhez legalább bővített sugárvédelmi képzettség szükséges, valamint megfelelő gyakorlat.
- Mobilis kialakíthatóság.
- Kis aktivitású, de nagyméretű hulladékok elhelyezés előtti tisztítására, továbbá radioaktív szennyezettségű munkahely (nukleáris reaktor) leszerelésénél, baleseteknél, piszkos bombatámadásnál a hulladékok térfogatának helyszíni minimalizálására alkalmas a lézeres dekontaminációs technológia.
- A rendszer karbantartási igény csekély.
- A lézer csak a szennyezést távolítja el, az alapfelületet nem károsítja. Bonyolult alakú tárgyak is könnyen kezelhetők (10. ábra).



10. ábra: Különféle felületek lézeres tisztítása, [saját szerkesztés]

- A lézerberendezéssel végzett dekontaminálás hatékony a meglévő eljárásokhoz képest, mivel gyors és a másodlagos szennyezés összegyűjtésre kerül.
- A lézeres dekontaminálás dekontaminációs faktora növelhető, amennyiben hígított (10%) salétromsav vízpermettel kezeljük a felületet (11. ábra) [1].

Dekontaminációs faktor=(Felületi szennyezettség értéke dekontaminálás előtt/felületi szennyezettség értéke dekontaminálás után)*100



11. ábra: A dekontaminációs tényező a lézer fény fluens függvényében, [1]

LÉZERES DEKONTAMINÁLÁS A GYAKORLATBAN

Gyakorlati tesztet hajtottunk végre egy kisebb (200 W) és egy közepes (500 W) teljesítményű lézerberendezéssel. A gyakorlat során használt autóalkatrészeket használtunk. Ezek erősen szennyezettek, rozsdásak voltak, természetesen radioaktivitás nélkül. Az alakjuk változatos volt. A lézerberendezés pisztolyát a felületre kell irányítani, majd szisztematikusan fel-alá szkennelve kell végigmenni a felületen. A ravasz megnyomásával aktiválható a lézer, fontos a megfelelő távolság tartása, így a felület épp a lézerfény fókuszpontjába esik, ekkor maximális a kezelés hatásfoka. A fókusz távolság változtatható 10-50 cm között.

Az első besugárzás során a felületi rozsdá nagy része eltávolításra került, az olajos szennyezés nagy része elpárolgott. A tiszta felület elérésekor a berendezés automatikusan blokkolta a lézerfényt.

A kis teljesítményű lézer főleg az enyhén korrodált felületek megtisztítására alkalmas. Az 500 W-os lézer már képes jelentősebb szennyezést is megszüntetni. A felületi szennyezettség az első kezelés hatására jelentősen csökken (~50 %), mivel a vastagabb rozsdarétegről leváló darabok fajlagos felülete igen nagy, így a leváláskor sok radioaktív részecske is távozhat a felületről (15. ábra).

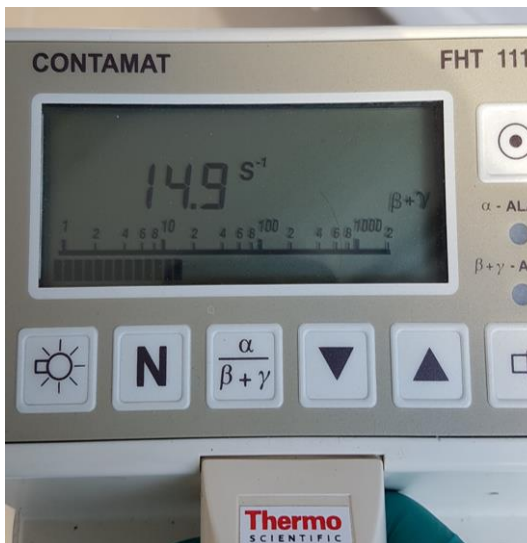


12. ábra: Lézerrel tisztított autóalkatrészek, inaktív minták, [3]



13. ábra: Részben tisztított autóalkatrészek, [saját szerkesztés]

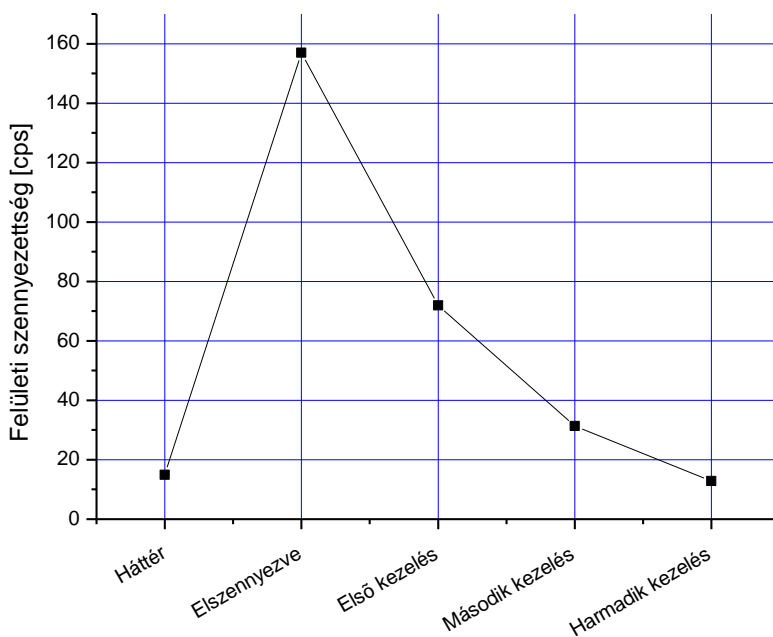
A második kísérletnél izotóplaboratóriumban, levegő elszívás mellett, Tyvek ruhába beöltözve ^{131}I oldatot alkalmaztam, a nehéz rozsdás felületet kisaktivitású, de a háttér felett jól mérhető ^{131}I -t tartalmazó oldattal szennyeztem el. Körülbelül fél óráig vártam, hogy a folyadék megszáradjon a felületen, és egy késsel a folyadékot a felszínén simítottam, hogy mélyen belemenjen a rozsdába. Az FHT111 Contamat felületiszennyezettség-mérővel béta-gamma cps módban mért háttér 15 cps volt (14. ábra). A szennyezés felvitele után a felületi szennyezettség felment a háttér kb. tízszeresére, majd három lézeres kezelést alkalmazva a felületi szennyezettség visszaállt a háttér értékre (15. ábra bal, közép, jobb), 16. ábra, 1. táblázat. (a mért értékek relatív szórása 20 és 5 % között volt, ezeket a táblázat nem tartalmazza).



14. ábra: A megtisztítandó felület felületi szennyezettség értéke elszennyezés előtt és után, [saját szerkesztés]



15. ábra: Az első kezelést követően a felületi szennyezettség a felére, második kezelés után a negyedére csökkent, majd a 3. kezelés után újra háttér értéket lehetett mérni, [saját szerkesztés]



16. ábra: Az elszennyezett alkatrész lézeres dekontaminációjának eredménye, [saját szerkesztés]

	Felületi szennyezettség [cps]
Háttér	14,9
Elszennyezve	157
Első kezelés	71,9
Második kezelés	31,3
Harmadik kezelés	12,8

1.táblázat: Az elszennyezett alkatrész lézeres dekontaminációjának eredménye, [saját szerkesztés]

ÖSSZEFOGLALÓ

A nukleáris létesítmények leszerelése során keletkező radioaktív hulladékok térfogatának jelentős részét adják a szennyezett anyagok és tárgyak. Egy nukleáris baleset során jelentős mennyiségű kis- és közepes aktivitású hulladék keletkezik. A hulladékok térfogatát minimalizálni kell, mivel a tárolók kapacitása véges, és a megfelelően biztonságos elhelyezés költséges. A hulladékok többségében a felületükön szennyezettek. A felületi szennyezettség megszüntetésével, illetve az adott helyen érvényes beavatkozási vagy mentességi szint alá csökkentésével a speciális kezelést, majd elhelyezést igénylő radioaktív hulladékok mennyisége jelentősen csökkenthető, ugyanakkor a legtöbb dekontaminációs eljárás jelentős másodlagos szennyezést generál.

A lézeres dekontaminálás során a másodlagos szennyezés koncentrálható, így annak térfogata minimalizálható, további nagy előnye a hatékony tisztítás mellett a felület folyamatos páasztázása, így a módszer képes a felület alapanyagát és a szennyezést megkülönböztetni. Ezen technika segítségével a lézer csak addig működik, amíg az alapfelületet el nem éri a lézertény, így megkíméli a felület degradációját. Ma már elérhetőek a kW osztályú hordozható lézerberendezések, melyek hatékonyan képesek eltávolítani a felületi szennyezettséget. Az eljárást jól szervezett sugárvédelmi ellenőrzés mellett kell végrehajtani, mivel a dekontamináció során a levegőbe kerül a felületről eltávolított radioaktív részecskék, melyek tovább szennyezhetik a környezetet, valamint inhaláció esetén belső sugárterhelést okozhatnak.

A cikkben bemutatásra került a lézeres dekontaminálási eljárás megvalósíthatósága, a kezdeti kísérletek alapján már 0,5 kW teljesítményű lézer berendezéssel is működik a gyakorlatban a lézer elven működő dekontamináció. A biztonságos működésre vonatkozóan bemutatásra került egy sugárvédelmileg tervezett mobilis dekontamináló állomás.

Supported by the ÚNKP-22-3 New National Excellence program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation fund”

FELHASZNÁLT IRODALOM

- [1] Leontyev, A. (2011): Laser decontamination and cleaning of metal surfaces: modelling and experimental studies. Doktori (PhD) értekezés, UPSud, Párizs
- [2] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről <https://net.jogtar.hu/jogszabaly?docid=a1100190.kor> (Letöltés ideje: 2023.03.06.)
- [3] Badár Fanni: Lézertény által generált ablációs dekontaminálási technológia vizsgálata, MSc. Diplomamunka, Szent István Egyetem, Mezőgazdaság- és Környezettudományi kar, Külső témavezető: Bodor Károly, 2019.
- [4] European Commission Radiation Protection 113 „Recommended radiological protection criteria for the clearance of buildings and building rubble from the dismantling of nuclear installations” (2000)
- [5] 2/2022. (IV. 29.) Korm. rendelet az ionizáló sugárzás elleni védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről, <https://net.jogtar.hu/jogszabaly?docid=A2200002.OAH&txtreferer=00000001.txt> (2022.07.11.)

**DETERMINATION OF THREATS TO THE
WORLD'S ENERGY SUPPLY THROUGH
THE CONCEPT AND OBJECTIVES OF
INFOCOMMUNICATION STRATEGIES****A VILÁG ENERGIAELLÁTÁSA
VESZÉLYEINEK MEGHATÁROZÁSA
INFOKOMMUNIKÁCIÓS STRATÉGIÁK
FOGALMÁN ÉS CÉLJAIN KERESZTÜL**DÉR Attila Tibor¹**Abstract**

An observable phenomenon nowadays is the rise of increasingly complex systems not only in our own lives, but also in our industrial infrastructures. Moreover, for the sake of manageability and comfort, these systems were connected to each other through various channels. This increased their vulnerability, so much so that terrorism moved more and more towards attacking critical infrastructure. Terrorists realized that with relatively few resources and from a distance, how great a blow could be inflicted on a selected country's most important objects. The article highlights the strategies and ideologies of the dominant countries in cyberspace. Furthermore, it provides a comparison of these countries, but with particular attention to the forward-looking regulations between European Union and Hungary. Finally, the courses of action that can be used to reduce the risk factors of the energy supply of European Union and Hungary as a member country are determined at a strategic level.

Keywords

Strategy, cybersecurity, Information security, legal regulation, critical infrastructure

Absztrakt

Napjainkban megfigyelhető jelenség az egyre bonyolultabb rendszerek térhódítása nem csak saját életünk területén, hanem az ipari infrastruktúráinkban is. Sőt irányíthatóság és a kényelem érdekében ezek a rendszerek egymással különféle csatornákon keresztül összeköttetésbe kerültek. Ezzel Sebezhetőségük megnövekedett, olyannyira, hogy a terrorizmus egyre jobban a kritikus infrastruktúrák támadása felé tolódott. Terroristák felismerték, hogy viszonylag kevés forrásból és távolról, milyen nagy csapást lehet mérni egy kiszemelt ország kiemelt fontosságú objektumaira. A cikk kiemeli a kibertérben meghatározó országok stratégiáit és eszmerendszereit. Továbbá összehasonlítást ad ezen országok, de különös tekintettel az Európai Unió és Magyarország közötti jövőbe mutató szabályozásai kapcsán. Végül meghatározásra kerülnek azok a cselekvési irányok, amelyekkel az Unió és tagországaként Magyarország energiaellátásának rizikó faktorai csökkenthetők stratégiai szinten.

Kulcsszavak

Stratégia, kiberbiztonság, információbiztonság, jogi szabályozás, kritikus infrastruktúra

¹ der.attila@uni-obuda.hu | ORCID: 0009-0008-9547-102X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A kiberbiztonság fontosságát a mai fejlet civilizációinkban nem szükséges kifejteni több száz oldalas könyvben, csak egyszerű logikus tapasztalással megérthető, milyen befolyásoló tényezővel rendelkezik a mai fejlett társadalmainkban. Az emberiség történetében már régóta kulcsfontosságú szerepet töltenek be a kritikus infrastruktúrák, mint a szállítás, víz-, olaj-, gáz-, áram-ellátás stb. lehetne még sorolni. Ezek között az infrastruktúrák között ráadásul sokszor szoros kapcsolat van egymástól jelentősen függhetnek, egyi a másik nélkül már elvesztheti eredeti rendeltetését, illetve funkcióját. Ezen kritikus rendszerek között több prioritási csoportosítást is megtalálhatunk a szakirodalomban fontosságuk sorrendjében. Nyilván függ ez az osztályzás, hogy melyik kontinensről vagy országról beszélünk. Az országok társadalmi és technikai adottságai mennyire befolyásolják a kritikus infrastruktúrák kiépítettségét és bonyolultságát. Természetesen rengeteg féle befolyásoló tényezőt még fel lehetne sorakoztatni, de általánosságban kimondható globálisan, hogy az egyik legveszélyeztetettebb infrastruktúra a villamosenergia-ellátást kiszolgáló rendszerek. Erre a megálapításra még ráerősít az elektronikai és az információs technológiai eszközök térhódítása és kölcsönös egymásrautaltsága.

UKRÁN-OROSZ HÁBORÚ ÁRNYÉKÁBAN

A villamosenergia infrastruktúra, mint a legtöbb kritikus szisztéma, egyre nagyobb mértékben összeköttetésben van az internettel. Ezzel sajnos a kiszolgáltatottsága is egyenes arányban növekszik. Ennek következtében a különféle kibertámadások is megnövekedtek, illetve manapság már vannak kifejezetten olyan szakosodott hacher csoportok, akik csak kizárólag ezeket a villamosipari létesítményeket támadják. Nem is kell messzire menni sajnos szomszédunkban Ukrajnában 2022 februárjában elkezdődött fegyveres konfliktus, amelyet nem csak hagyományos fegyverekkel vívnak meg, hanem a kibertérben is egyre komolyabb és szofisztikáltabb támadások jelentek meg mind a két hadviselő félnél. Oroszország már a háború előtt is támadta Ukrajnát, de csak kibertámadás címen. Az első hullámban óriási károkat okozott Oroszország Ukrajnának főként a kritikus infrastruktúrák területén. Nagyon szembeutó volt Oroszország technikai fölénye és Ukrajna védtelensége, felkészületlensége ezekkel a speciális elektronikai rendszereket érintő agresszor ellen. Itt meg kell jegyezni, hogy az ENSZ alapokmánya szerint a kibertámadás önmagában nem váltja ki a háború fogalmát, csak ha háborús konfliktussal van kombinálva. Ennek következtében esetünkben Ukrajna nem számíthatott nemzetközi segítségre, hogy a támadót jogilag megállítsa, illetve megfelelő szankciókkal sújtsa. Felismerve ezt a tényt az ukrán vezetés, úgy határozott, hogy nem tétlenkedik és már a tényleges háború kezdete előtt komoly kibervédelmi stratégiát alakított ki. Megerősítették az ország legsérülékenyebb infokommunikációs rendszereit, kiemelt intézményeit, infrastruktúráit. Az ukrán nemzeti adatvagyon felhőbe rejtették el, különféle zombihálózatokat építettek ki, 2022. 02 26.-án felállították az Ukrán Informatikai Minisztériumot stb. Továbbá nem csak a védelemre rendezkedtek be az ukrán politikai elit, hanem a háború bejelentése óta már tudatos kibertámadások sorozata is napirendre került kiemelt orosz létesítmények ellen, amelyek mai napig folyamatban vannak. Korszakalkotó kezdeményezés volt Ukrajnának, hogy megalapította az Ukrán Kiber hacker közösséget, amely több mint 400 000 fős önkéntes nemzetközi hacker háttérrel rendelkezik.

Sőt állami szinten olyan fontosnak tartják ezt a közösséget, hogy a nemzetközi hacker csapatok szervezése már törvénytervezetben jelent meg és hamarosan elfogadhatja az ukrán kormány, amely első ilyen intézkedés lehet a világon. Az ukrán katonai irányítása alatt működő hacker közösség rendkívüli hatékonyságát jól bemutatja - rendelkezésre álló adatok alapján -, hogy Oroszország képtelen volt megvédeni, illetve ellenállni ennek a félelmetes méretű és szaktudású „Armadának”. Érdekes az a tény is, hogy az a „nagy” orosz kibervédelem, amelyet évtizedek óta nemzetközi szinten propagál az orosz politikai és szakmai elit, viszonylag rövid idő alatt a porba hullott, az ukrán nemzetközi hackerek által megerősített offenzíva alatt. Ezekkel kibertámadásokkal betörték a Kremlbe, a Dumába, a titkosszolgálatok adattáraiba és a legfontosabb állami intézményekbe, valamint átlagos adatszivárgás elérte a 100GB-ot orosz vállaltonként, ide értve majdnem a teljes kritikus infrastruktúrát is.

STRATÉGIÁK ELEMZÉSE

Nem véletlenül emeltem ki az orosz-ukrán háborút, mivel ez napjainkban is hatással van Magyarországra, mint szomszédos államra és természetesen Európára és közvetlenül vagy közvetetten az egész világra is. Stratégiákat az államok már régóta kialakítottak kezdetben inkább katonai jellegűek voltak, majd később már politikai, gazdasági és társadalmi színezetet is kaptak. Napjainkban pedig minden szakterületnek megvan a maga stratégiája, így a nemzeti kibervédelemnek, infokommunikációnak és az energiabiztonságnak is. Természetesen minden állam saját érdekeit veszi alapul és ezeket az érdekeket egyezteteti a nemzetközi érdekekkel vagy teljesen sajátos utat követ. A politikai és gazdasági nagyhatalmak ezen a területeken is éreztetik hatásukat illetve befolyásukat. Nagyon szépen követhető a kisebb országok stratégiai dokumentumaiban ezen országok dominanciája.

Uniós szabályozás

Az Európai Uniónak is van egy stratégiája, melynek keretrendszerét több szervezet is aposztrofálta, úgy, mint ENISA (European Network and Information Security Agency), amely az Unió egyik legfontosabb kiberbiztonsági szervezete. Tanácsadó szervezetként különféle ajánlásokkal, dokumentumokkal segíti a tagállamokat stratégiáik kialakításában. A gyorsan változó nemzetközi környezetre - ukrán-orosz háború - való rugalmas válaszok elengedhetetlenek az Unió szabályozásaiban. Tisztázni kell a határokon átnyúló fenyegetések határait, hol vannak a NATO vagy az Unió és a nemzeti érdekek közös pontjai, illetve saját elkülönített keretrendszeri. Az ENISA jól rámutatott még régebben, hogy a tagállamoknak elemi érdeke, hogy egymás között egyeztessenek a kardinálisabb kifejezéseken és fogalmakon. Mivel egyáltalán nem mindegy, hogy például Lengyelországban kiberbiztonság, mint fogalom mennyiben hasonlít Magyarországi megfelelőjéhez. A szervezet már akkor felismerte, hogy az állam és a piaci szereplők között kiberbiztonsággal összefüggő kapcsolatokat kell kiépíteni a szükséges védelemhez. Fontos információk nyerhetők a piaci alapon működő vállalkozások infokommunikációs tapasztalataiból és természetesen ez kölcsönös az állami szervek oldaláról is.[1]

Itt megemlíteném Magyarországon a Nemzeti Kibervédelmi Intézetet, amely megalakulása óta egyre hatékonyabban ellátja ezt a híd szerepet az állami szféra és a magánvállalkozások között. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv) 2015. évi módosítása során lett létrehozva a Nemzeti Biztonsági Szakszolgálatokon belül. Szakhatósági feladatain kívül eseménykezelési nemzeti

kapcsolattartás Unió határain belül különféle incidensekkel összefüggő adatok elemzése, monitorozása és ezen eredmények megosztása fontosabb Európai incidenskezelő központokkal. Az állami intézményeket és állami tulajdonú vállalatokat kiberbiztonság céljából felügyeli és ajánlásokat küld az illetékes intézmények felé. Fontos, hogy a Nemzeti Kibervédelmi Intézet napra kész információkat oszt meg a honlapján, amelyet bárki elérhet. Sőt incidenseket bárki bejelenthet ezzel segítve a hatóság munkáját. Szolgáltatásai kiterjednek incidensvizsgálásra, eseményészlelésre, sérülékenységvizsgálatra, korai figyelmeztető rendszerre, amelyekkel információs technológiai rendszerek üzemeltetőit nagymértékben támogatják.[2][15]

A NATO Kibervédelmi Kiválósági Központjának kiadott Nemzeti kiberbiztonsági keretrendszer kézikönyve is nagyszerű alapot nyújtott, illetve nyújt a tagok számára, hogy kialakítsák a maguk stratégiáját. A tanulmányban öt kardinális téma kap szerepet, ahol az egyik kritikus infrastruktúra védelme. Érdekes ellentmondás, hogy a veszélyeztetett rendszereket minél jobban korszerűsítik, annál nagyobb sérülékenységet jelentenek egy ország biztonságára. Az sem egy megfelelő gyakorlat főként a villamos iparban, hogy eltérő fejlettségű és típusú eszközöket alkalmaznak. Ezzel az inkompatibilitással és az eltérő biztonsági megoldásokkal kisebb-nagyobb réseket adnak a támadók számára. Nem véletlenül vannak ezekben az ajánlásokban olyan kérdések felvetése, mit például a biztonság vagy versenyképesség legyen a fő mozgatórugó egy adott térségnek illetve országnak. A kérdés egy alapvető megállapításon nyugszik, mint hogy általában információstechnika fejlődése jóval gyorsabb, mint a védelmének fejlődése.[3]

2013-ban született meg az első komolyabb Európai Unió kiberbiztonsági stratégia, amelynek mottója, mint a címben is utalnak rá nyílt megbízható és biztonságos kibertér. Ez a szabályozás megfelelő alapot jelentett a további intézkedéseknek, de a tagállamok még nem tudták abban az időszakban se gyakorlatban se intézményi szinten kivitelezni ezeket az iránymutatásokat. 2016 nyarán jelent meg az újabb biztonsági direktíva a NIS (Network and Information Systems Directive), amelyben az Európai Unió már geopolitikai alapokon határozta meg az együttműködést egyes tagállamok intézményei számára, sőt közös intézményi háttér kialakítását is előírta. [4]

Időrendben tovább haladva 2020. évben készült el egy ráncfelvarrása az előző digitális stratégiáknak továbbfejlesztett Európai Bizottság javaslata. Ebben a javaslatban röviden a főbb újítások a következők: gyors válaszlépések a kibertámadások ellen; katonai missziók felértékelése; korszerű titkosítás megvalósítása; ellátási láncok megerősítése; növekvő kibertámadások elleni immunitás növelése; közös kiberbiztonsági egység kialakítása; biztonsági műveleti központok hálózatának kiépítése az Unió tagállamaiban [5]

Tavaly év végén az Európai Unió Bizottsága kihirdette a NIS2 Irányelvet. Ennek következtében a legfrissebb és egyben a leghaladóbb szemléletű Uniós szabályozás ez év januárjában került hatályba. Fontos vetülete (később tárgyalja a cikk) ennek az irányelvnek, hogy kiterjeszti és kijelöli a kiberbiztonsági kockázatkezeléseket és bejelentési kötelezettségek körét, kritérium-rendszerét és hatályát a kritikus infrastruktúrák területén is. Sajnos a tagállamok csak közel másfél év múlva fogják saját jogrendjükbe áthelyezni a NIS2-es normatívákat.[6]

USA irányelve

Amerikai Egyesült Államok legfrissebb Kiberbiztonsági Stratégiája 2023 március elején jelent meg. Főbb mozgató rugója ennek az elképzelésnek, hogy az informatikával foglalkozó jelentősebb vállalkozásokra alapozza az ország kibertér védelmével kapcsolatban. Ezzel szeretné a kormány kiegészíteni azokat a szegmenseket (civilket, kisvállalkozásokat, közigazgatási szerveket), akik nem férnek hozzá a megfelelő technológiához, nincs elég forrásuk, hogy egy adekvált védelmet kiépítsenek saját rendszereikben. A megfelelő állami koordináció elengedhetetlen záloga a nemzetbiztonság kézben tartására. A dokumentum tartalma 5 fő részből áll. Az első pillér kiemeli az infrastruktúrák védelmét, egy új szemléletű incidenskezelési politika megalkotásával. A második rész a zsarolóvírusok elleni nemzetközi küzdelem összehangolását célozza meg. A harmadik pillér a megbízható szoftvereket gyártó cégeket helyezni előtérbe. A negyedik meghatározó szegmens nem meglepően a képzés és kutatás elősegítése. Az utolsó pillér általánoságban leírja nemzetközi környezetben, milyen helytállásra van szükség, hogy elkerülje az Amerika a nagyobb kibertámadásokat.[7]

A stratégia elkészítését több előzmény is serkentette, ide értve Amerika Nemzetbiztonsági Stratégiáját, ötös és a tízes számú memorandumokat. Ezeknél az eljárási módoknál már megjelenik egy igen fontos fogalom a zéró bizalom, amely még csak felvetődött biztonsági elvként, de már itt a legújabb kiberbiztonsági dokumentumban tovább lett fejlesztve, mint egy sajátos eszmerendszer. Kiemelném a témához szorosan összefüggő 5. nemzetbiztonsági dokumentumot, ahol kifejezetten a kritikus infrastruktúrák vezérléseinek biztonsági réseinek javításával foglalkozik. Sőt felmerültek lehetőségek, hogy a fontosabb vezérlő rendszereknél kvantumszámítógépek csatasorba állításával jelentősen csökkenthetők a sérülékenységek. A stratégia hangsúlyozza, hogy az állam feladata megvédeni az állampolgárait a kiberbűnözőktől vagy olyan országoktól, amelyek nem tartják be a nemzetközi jog normáit. Számon kérné azon országokat, amelyek a kiberbűnözőket támogatják akár pénzzel, akár technikai eszközökkel. Továbbá rávilágít a különféle kibertámadások okozta károokra, amelyek egyre komolyabbá is válhatnak, ha nincs megfelelő cselekvési terv. A digitális technológiák egyre jobban rátelepednek mindennapi életünkre. Személy adatainkra egyre jobban kell vigyázni, mivel olyan láthatatlan térben vannak ahol sokszor már követni sem lehet.

A stratégia kifejti, hogy egykor jól meghatározott keretek között csak néhány ország volt képes kibertámadások kifejtésére, illetve ehhez szükséges eszközök előállítására. Ma-napság viszont, már széles körben elérhető a különféle kémprogramok, hacheléshez használt adatok, eszközök és szolgáltatások. Ezeknek az eszközöknek a birtokában - általában jóval alacsonyabb költséggel rendelkeznek, mint a hagyományos fegyverek - már olyan országok is vannak, akik messze nem közelítik meg a fejlett országok kibernetikáját. Kiemeli név szerint megemlítve Kínát, Oroszországot, Iránt, Észak-Koreát, ahol agresszíven használnak fejlett kiberképességeket, olyan célok elérésére, amelyek ellentétesek a nemzetközi normákkal és értékekkel. Ezek közül a felsorolt országok között is az amerikai vezetés a Kínai Népköztársaságot tartja a legveszélyesebbnek, amelynek gazdasága, katonai ereje lassan eléri az Egyesült Államokét. Ebben nagy szerepet játszott az elmúlt évtizedekben történt ipari kémkedés, amelyet a kommunista rezsím kifinomult információtechnoló-

giai eszközparkkal véghezvitt USA-ban és más fejlett országokban. A stratégia figyelmeztet, hogy Kína nem csak „importál” kritikus információkat, hanem „exportálja” saját ideológiáját, hogy ezzel átalakítsa a világ demokratikus képét.[8]

Kína startégiája

Nyilván Amerikai szemüvegen nézve teljesen más képet kapunk Kínáról, mint amikor saját dokumentumait kutatjuk. Nem véletlenül ezzel a résszel folytattam a cikkemet, közvetlenül az amerikai álláspont befejezése után. Így jobban érzékelhető az olvasó számára, hogy milyen a két legbefolyásosabb hatalom (Oroszországot még ide lehetne sorolni, de véleményem szerint már leszakadó félben van helyzetével kapcsolatosan) egymás közötti interakciója. Mivel a kínai pártvezetés már több éve megfigyeli állampolgárait totális megfigyelő rendszerein keresztül, ezért óriási információ halmazt gyűjtött össze. Nem is beszélve az infokommunikációs területeket érintő nagyvállalatairól, akik világszínvonalú termékeket és szolgáltatásokat bocsátanak ki szerte a világban. Ezzel Kína úgymond versenyelőnyre tett szert a versenytársakkal szemben. Jellemző a kommunista rezsimre, hogy az ENSZ alapokmányának szabályozásába is beleszólt, sőt beadott egy viselkedési kódexet a következő szövegrészlettel szemben, amely így szól „nem alkalmaznak információs és kommunikációs technológiákat, valamint információs és hírközlési hálózatokat abból a célból, hogy megzavarják más ország belső ügyeit vagy, hogy aláássák annak politikai, gazdasági és társadalmi stabilitását.” (United Nations 2015) „, 2003. év óta a Kínai nagy Tűzfal néven felállított megfigyelőrendszerrel totális kontrollt gyakorolnak az állampolgárok felett. Ha azt vesszük, hogy Kínában nagyjából egy milliárd internetes felhasználó van, akkor érzékelhető, hogy megkora tapasztalatot képesek begyűjteni ennyi felhasználóról.[9]

A kínai rendszer folyamatosan szoros együttműködésben van az internet szolgáltató vállalatokkal. Ezzel próbálja megelőzni, hogy bárki is a kormány ellen szervezkedjen vagy agitáljon. Rendszeresen monitorozza az internetet és, ha valami gyanús tartalom kerül előtérbe azt rögtön blokkolásra kerül. Kína kiberbiztonsági stratégiájára teljes mértékben rányomja a bélyegét az előző bekezdések megállapításai és tényei, amelyek természetesen szoros összefüggésben vannak a rezsim ideológiájával is. Stratégiájában jól körvonalazható a katonai szemlélet, amely nem titkolva az Egyesült Államok technikai fölényének legyőzésére is nagymértékben törekszik.

EURÓPAI SZINTŰ SZABÁLYOZÁS LÉTFONTOSÁGÚ RENDSZEREKKEL KAPCSOLATOSAN

2005. zöld könyv CIP (Critical infrastructure Protection) irányelvek 2008-as és 2020-as átdolgozása, majd következett a 2020 NIS 2.0 javaslata a CIP továbbfejlesztése. A létfontosságú infrastruktúrák védelmére vonatkozó európai program 2020-as markáns jellegzetesége, hogy bevezette az immunitás képességének korszerűsítését, a bekövetkező problémák gyors és szakszerű kezelését szakítva a korábbi gyakorlattal, miszerint materiális síkon kellene megvédeni a különféle infrastruktúrális elektronikai rendszereket. Kiemeli a kockázatelemzés fontosságát, kritikus elemek azonosítása, entitások hatósági felügyeletét stb. A kritikus entitások ellenálló képességéről szóló irányelv CER (Critical Entity Resilience)-ben egyre jobban bővül az ágazati paletta az évek előrehaladtával például tavaly is

bekerült digitális infrastruktúra, agrárium és a közigazgatás. A dokumentum kifejezett szándéka, hogy a többi rendelkezéssel vagy jogi aktusokkal, ne kerüljön ellentmondásba, ne lehessen kijátszani és ne legyen egy konkrét szabályozás több helyen.[10]

A hálózati és információs rendszerek biztonsága (NIS 2) Uniós szintű szabályozását az Európa tanács elfogadta, de még a tagállamok nem ratifikálták saját jogrendükben. Ebben a tervezetben az Unión belüli országoknak egy hatóságot kellene felállítani kapcsolattartó ponttal és egy eseménykezelő központtal egyetemben. Részletezi a kritikus szervezetek bejelentési és kapcsolattartási kötelezettségét a jövőbeni hatóság felé, ahol a mostani gyakorlatot (több hatóság) felváltja egykapus rendszer. Így egy hatóság járna el az adatszivárgások kivizsgálásánál, helyszíni ellenőrzéseknél, iratok és adatok átvilágításánál. Fontos felvetése a NIS 2 –nek, hogy az Unióban jelentkező szakemberhiányt, azt valahogyan pótolni kell, úgy hogy a jogilag kiszervezhető szolgáltatásokat még az eddigi szabályozásoknál is markánsabban kellene támogatni. Viszont még ettől is fontosabb, hogy ezeket a külső „alvállalkozókat” legalizálni kellene az új irányelv szerinti. Ugyanis nem mindegy, hogy ezeket a szentitív adatokkal kapcsolatos munkákat kire illetve kikre bízzák. Továbbá az Unió jogalkotás még keményebben fellépne, ezen jogi normák megsértőivel szemben. Azok a szervezetek, amelyek az ENISA-nál szerepelnek és 72 órán belül nem jelentik a hatóság felé biztonsági incidensüket, azokat jelentős bírsággal lehetne súlytani.

Magyarországi szabályozás

Magyarországon a Nemzeti Infokommunikációs Stratégia 2014-2020 közötti időszakot ölelte fel. Majd az Európai Unió által szerkesztett iránymutatás digitális iránytű címmel 2030-ig kijelölte az európai tagállamok digitális stratégiáját. Egy újabb szemléletet vezetett be a - régebbi iránymutatásokkal összhangban - digitális készségek fejlesztése, vállalkozások és az infrastruktúrák teljes digitalizációja területén. Ennek a digitális „forradalomnak” magyarországi leképezése a Nemzeti Digitalizációs Stratégia (2022-2030), amely újabb lendületet adhat a hazai digitális gazdaságnak. A Nemzeti Digitális Stratégia inkább általánosságokat fogalmaz meg, mint a szupergyors internet kiépültségének hatása a társadalomra, a digitális ökoszisztéma területén megfogalmazott kezdeményezéseket, stratégiákat, azok fejlesztési irányait, jövőképét, digitális kompetenciákat, SWOT elemzést, eszközrendszereket és átfogó jövőképet.[11]

Az Európai Unió szabályrendszerével összefüggésben 2012. évi CLXVI. törvény (létfonosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről)

majd energia ágazati iránymutatása kiegészült 374/2020 kormányrendelettel. Itt körvonalazódik, hogy a villamosenergia rendszernek magyarországi hatósága a Magyar Energetikai és Közmű-szabályozási Hivatal. Azonosítási jelentés küldése a Magyar Energetikai és Közmű-szabályozási Hivatal részére. Üzemeltetői biztonsági tervnél nevesítette a jogalkotó a rendkívüli eseményeket, sőt a kiemelt ágazatok üzemeltetőinek meg kell adniuk, hogy milyen eljárásrend szerint oldják meg ezeket az incidenseket. A rendkívüli intézkedések részleteit is meghatározta ez a törvény. Megfelelő részletességgel az Európai Unió normáknak megtartásával segítik ezen előírások a jogalkalmazókat. Itt kiemelném, hogy a létfonosságú ágazatoknak és természetesen az államnak is elemi érdeke, hogy felkészítsék létesítményeiket és vezetőiket a rendkívüli eseményekkel szemben. Ennek érdekében az Országos Katasztrófavédelmi Igazgatóság bevonásával – kötelező gyakorlatot el-

rendelheti, mint hatóság - vagy nélküle tesztelési gyakorlatokat kell elvégezni. A fiktív támadási teszt meglátásom szerint nagyon fontos eleme a védekezésnek, mivel nem éles helyzetben kell kapkodni és a hiányosságokat feltárni, amikor közvetlen vagy közvetett formában emberi illetve anyagi kárt szenved az ország. Továbbá kötelező tartalmi elme lett a biztonsági tervnek a kockázatelemzés, amelynek összhangban kell lennie a törvény mellékletében lévő védelmi intézkedések szintjével és elvárásaival. Ezekhez a táblázatok, tervek kitöltéséhez segítséget nyújtanak a Vármegyei Katasztrófavédelmi Igazgatóságok. A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság éves jelentése is hasznos szakmai alapot adhat a kockázatelemzés szakszerű leírásával kapcsolatosan. [12][14][16]

2013. évi L. tv. Ibtv az állami és önkormányzati szervek elektronikus információbiztonságáról. Ahol a kritikus infrastruktúrák rendszereit és intézményeit törvény által nevesített osztályok szerint kell nyilvántartani. Kötelező ezen szervezetek mindegyikéhez egy-egy kiberbiztonsági felelős szakértőt kijelölni. Leírja a hatóságok szerepét és ellenőrzését államilag fontos intézményeknél.[15]

ÖSSZEFOGLALÁS

A jelen írás megvizsgálta a világ kiberterében meghatározó országainak stratégiáit. Így görcső alá vettem Amerikát különös tekintettel a legújabb kiberbiztonsági dokumentumait, majd Kína, mint vetélytárs követte a sorban. Továbbá Magyarország geopolitikájából kiindulva átrágtam magam az Európai Unió stratégiai elvein, illetve tervezetein és ezzel összefüggésben hazánk szabályozásait és infokommunikációhoz köthető irányelveit is átnéztem.

Ezekből a vizsgálatokból levonható következtetés, hogy még mindig nincs kiberteret érintő garanciális alapokon nyugvó egységes szabályozás a teljes globális világra nézve. Ha van is, mint például ENSZ határozat, akkor sem mindegyik állam ratifikálja. Sőt Kína még saját dokumentumot is benyújtott, hogy saját nézőpontja szerint legyen az ENSZ határozat megváltoztatva. Megjegyezném, hogy ha minden ország a világon aláírna egy ilyen kiberbiztonsági egyezményt, akkor sem biztos, hogy az be is tartanák az aláírók. Sajnos volt már rá példa, hogy egyes országok hacher kalózokat bízott meg titokban, hogy más államok biztonságát és szuverenitását veszélyeztesse. A nagyhatalmakhoz képest az Uniónak van még lemaradása stratégiai szinten, habár a NIS 2 tervezetben már jól körvonalazódnak azok a tendenciák, amelyek már képesek lesznek majd egy fejlett struktúra kialakítására. A hazai szabályozásban is kivehető, hogy az Európai intézmények és a tagországok között nincs az a kohézió, amellyel az elméleti iránymutatásokat megfelelő hatékonysággal át lehetne ültetni a gyakorlatba. Az Amerikai gyakorlatban – nyilván a politikai berendezkedés miatt – nem probléma az államok közötti munkamegosztás és bizonyos központosítás. Megállapítható, hogy a jelenlegi ukrán háborús politikai helyzet, amely jól reprezentálta és reprezentálja a hibrid hadviselés elemeit, igen csak komoly gondokat okozott az Európai Unió tagországok belbiztonsága szempontjából. Gondolok itt például a nem régen történt ír kórházak elleni kibertámadásra.

Kritikus infrastruktúra szerepe nem kérdőjelezhető meg egy ország életében sem, ezért is fokozott figyelmet kell fordítani rá, mint Unió keretszinten és tagállamok „sajátos” szintjén egyaránt. Viszont az Európai Unió nehézkes jogalkotási rendszere nem teszi lehetővé a gyors stratégiai szabályozást és így a védekezés mindig hátrányban lesz a támadók

képességeivel szemben, főként tagállami szinten (lásd NIS 2-es szabályozás 2024 őszén lesz csak a tagállamok jogrendjébe ültetve).

A cikk elemzéseiből levont következtetésem, hogy az Európai Uniónak, így hazánknak is magáncégeket kellene bevonni a kritikus infrastruktúrák védelme szempontjából. Mivel a kormányzati szektoroknak jelenleg nincs akkora anyagi és emberi erőforrása, illetve technikai kompetenciája, hogy egyedül megbirkózzon ezzel a speciális és késlekedést nem tűrő speciális feladattal. Egyébként a digitális magáncégeknek épp úgy érdeke az együttműködés, mint az állami intézményeknek, hiszen egy kívülről jövő agresszív kibertámadás az adott célszág teljes nemzetbiztonságát fogja veszélyeztetni. Ehhez kellene erősíteni a felderítést és a védekezést. Nagyobb hangsúlyt kellene fektetni az oktatásra kiberbiztonsági szakemberek képzésére, kvantumszámítógépek és a mesterséges intelligencia fejlesztésére. Kormányzati és magáncégek összefogásával kellene létrehozni egy egységes védelmi rendszert és egy tartalékszolgálatot is, amelyet éles helyzetben vethetnének be a veszély semlegesítésére.

FELHASZNÁLT IRODALOM

- [1] Kovács László, *Kiberbiztonság és –stratégia*. Budapest: Dialóg Campusz Kiadó, 2018, pp. 32-44.
- [2] <https://nki.gov.hu/intezet/tartalom/magunkrol>. 2023.05.12.
- [3] B Müller Tamás, *Kiberhadviselés és katonai védelem*. infójegyzet 2019. november 15.
https://www.parlament.hu/documents/10181/1789217/Infojegyzet_2019_49_Kiberhadviseles.pdf
- [4] Bihaly Barbara: *A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában*, Hadtudományi Szemle 2021 XIV. évfolyam 3. szám 45- 55. doi 10.32563 /hsz.2021.3.4
- [5] EU Tanácsa: *Kiberbiztonság: a Tanács következtetéseket fogadott el az uniós kiberbiztonsági stratégiáról*. Sajtóközlemény 2021. március 22. <https://www.consilium.europa.eu/hu/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/>
- [6] EU Tanácsa: *A kiberbiztonság és -reziliencia megerősítése az EU egész területén – Ideiglenes megállapodás a Tanács és az Európai Parlament között*. Sajtóközlemény 2022. május 13. <https://www.consilium.europa.eu/hu/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-ac-cord-provisoire-du-conseil-et-du-parlement-europeen/>
- [7] The White House: *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*, 2023.03.02. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>
- [8] The White House: *Amerikai Egyesült Államok Nemzeti Kibervédelmi Stratégiája* 2023. március. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
- [9] Kovács László, *Kiberbiztonság és –stratégia*. Budapest: Dialóg Campusz Kiadó, 2018, pp. 104-105.

- [10] SeConSys együttműködés keretében: *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve*, Nemzeti Kibervédelmi Intézet, 2022, pp. 42-44.
<http://www.seconsys.eu/>
- [11] Miniszterelnöki Kabinetiroda: Nemzeti Digitalizációs Stratégia, 2022.12.05,
<https://kormany.hu/dokumentumtar/nemzeti-digitalizacios-strategia-2022-2030>
- [12] <https://www.securinfo.hu/szabalyozasok/jogszabalyok/12033-jogszabalyvaltozasok-kritikus-infrastruktura-vedelemben.html>

FELHASZNÁLT JOGSZABÁLYOK

- [13] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- [14] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- [15] 2013. évi L. tv. Ibtv az állami és önkormányzati szervek elektronikus információbiztonságáról.
- [16] 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

**TERMINOLOGY OF EMERGENCY
MASS MOVEMENTS****A VÉSZHELYZETI TÖMEGMOZGÁSOK
TERMINOLÓGIÁJA**EDELMANN Dóra¹**Abstract**

With the spread of urbanization, the safety of mass populations has gained increasing emphasis. The field of crowd dynamics, which studies human movement, is based on classical scientific disciplines. Physics, mathematics, engineering, sociology, psychology, and medicine are just a few of the disciplines whose findings contribute to this field. However, crowd dynamics has become an independent field of study in the 21st century. As is often the case with emerging sciences, the consolidation of relevant knowledge is an ongoing process, and the necessary specialized terminology is not yet available either domestically or internationally. This study proposes a method for naming and categorizing distinct motion phenomena in crowd dynamics. It is based on the recognized physical phenomena in motion processes, the temporality of events, the characteristics of resulting accidents, and scientometric indicators.

Keywords

crowd movement, crowd dynamics, terminology, emergency, crowd, security, scientometrics

Absztrakt

Az urbanizációval az embertömegek biztonsága egyre nagyobb hangsúlyt kap. Az emberek mozgását kutató tömegdinamika klasszikus tudományterületek alapjain áll. A fizika, a matematika, a mérnöki tudományok, a szociológia, a pszichológia, az orvostudomány csak néhány azon diszciplínák közül, melyek felismerései megjelennek ezen területen. Önálló tudományággá ugyanakkor a XXI. században vált. Mint a fiatal tudományok esetében gyakran tapasztalható, a vonatkozó ismeretanyag egységgé formálódása folyamatos, a szükséges szakszókincs ugyanakkor sem hazai, sem pedig nemzetközi vonatkozásban még nem áll rendelkezésre. A tanulmány a tömegdinamikában jellegzetesen elkülöníthető mozgásjelenségek megnevezésére és csoportosításának módzatára tesz javaslatot. Alapul a mozgásfolyamatokban felismert fizikai jelenségek, az események időbelisége, a bekövetkező balesetek jellemzői és szcientometriai mutatók szolgálnak.

Kulcsszavak

tömegmozgás, tömegdinamika, terminológia, vészhelyzet, embertömeg, biztonság, szcientometria

¹ edelmann.dora@phd.uni-obuda.hu | ORCID: 0009-0005-9882-3500 | PhD student at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

ELŐZMÉNYEK

Az egyes vészhelyzeti mozgások megkülönböztetése és feltárása, a történések, a mozgásjellemzők, a bekövetkezett balesetek szempontjából történő megközelítés korunk aktuális kutatási feladata. [1] Haghani a tömegdinamika önálló tudományterületét analizálta Chen publikációjában [2] között szcientometriai módszerek szerint. A tanulmányában feltárt kutatási területek közül a gyalogos menekülés („pedestrian evacuation”) témacsoport bizonyult a legnagyobbaknak, a gyalogos dinamika („pedestrian dynamics”) a második helyen szerepelt. [3] A múltbéli felismerések implementálását, az új irányvonalak kijelölését egyaránt nagymértékben nehezíti, hogy mind a hazai, mind pedig a nemzetközi szakmai szókincsből hiányoznak a folyamatokat megfelelően leíró fogalmak. A megfelelő kifejezések hiányát, a közös nyelvezet szükségességét jól szemlélteti, hogy még az alapvető fogalmakra is (példaként „tömeg”, vagy „gyalogos”) egyelőre körülírások, ajánlások születtek. [4] A meglévő, angol nyelvű megnevezések közül régebben használtak pontatlanságára, a sajtóban megjelenő kifejezések helytelenségére való figyelemfelhívás a nemzetközi szakirodalom visszatérő eleme napjainkban, hazai szókincsünk pedig rendkívül hiányos a területen. Felismerésre került, hogy új kifejezésekre és a tömegben előforduló balesetek tudományos magyarázatainak terjesztésére van szükség. [5]

MÓDSZEREK

A vészhelyzeti tömegmozgások alapvető csoportosítási rendszerének és terminológiájának meghatározása a következő három módszer együttesével történt:

- 1) Szcientometriai megközelítés: A Web of Science Core Collection (WoS) adatbázisában szereplő, első 500-1500 releváns publikáció címében megjelenő tematikus kifejezések és az idézések mezo-szintű témabesorolásai szerint kigyűjtött adatok CiteSpace szoftver 6.2.R2 verziójával történő elemzése. A véleménybányászatra alkalmazott program [6] az egyes publikációkat tematikus csoportokba (klaszterekbe) rendszerezi, három algoritmus alapján:
 - látens szemantikai indexelés (LSI, „latent semantic indexing”) [7];
 - logaritmus valószínűségi arány (LLR, „log-likelihood ratio”) [8];
 - kölcsönös információ (MI, „mutual information”) [9].
- 2) Szakirodalom szisztematikus feltárása.
- 3) Empirikus megközelítés: A megtörtént esetekről készült videófelvevételek, fényképek, leírások tanulmányozása.

NORMÁL ÉS VÉSZHELYZETI TÖMEGMOZGÁSOK

Az embertömeg-mozgások jellegzetességeit tekintve elkülöníthetőek a normál helyzeti gyalogosmozgások és a vészhelyzeti tömegmozgások. [10] A WoS adatbázisában szereplő publikációk címében megjelenő kifejezések és az idézetek témabesorolásai közelebbi képet mutatnak a két fogalom eltéréséről. (1. Táblázat) Megállapítható, hogy a hivatkozott tanulmányok minden keresett kifejezés esetén igen nagy arányban a „közlekedés” valamilyen témájában íródtak. A vészhelyzeti mozgások körébe sorolható kereső kifejezéseknél azonban minden esetben megjelennek az egészségügy témakörei is a hivatkozási területek között.

idézési téma	kifejezések a címben						
	gyalogos mozgás ^{*1} N=3263	tömegdinamika gyalogos ^{*2} N=1629	tömeg vészhelyzet ^{*3} N=2863	gyalogos vészhelyzet ^{*4} N=1657	tömeg biztonság ^{*5} N=2440	menekítés tét ^{*6} N=31643	tömegdinamika vészhelyzet ^{*7} N=521
közlekedés	1. (30%)	1. (78%)	2. (30%)	1. (61%)	1. (33%)	1. (32%)	1. (80%)
automatizálási és vezérlőrendszerek		3. (1%)					
telekommunikáció	3. (12%)			3. (5%)			
számítógépes látás és grafika	2. (29%)	2. (4%)			2. (11%)		3. (2%)
egészségügyi ellátás			1. (33%)		3. (7%)		2. (5%)
baleseti sebészet			3. (3%)	2. (7%)		2. (5%)	
égés						3. (4%)	

1. Táblázat, WoS adatbázisában szereplő publikációk címében megjelenő kifejezések és az idézések mezo-szintű témabesorolásai, az adott kifejezéscsoport esetében az előfordulási rangsor első három tagjának a teljes hivatkozási területen mért százalékának megadásával, vizsgálat ideje: 2023.05.18., (*1: „pedestrian motion”, *2: „crowd dynamic pedestrian”, *3 „crowd emergency”, *4: „pedestrian emergency”, *5 : „crowd safety”, *6, „evacuation space”, *7 : „crowd dynamic emergency”)

A mozgásfolyamatok és a balesetek bekövetkeztének leírására hivatott angolnyelvű szakirodalomban használt kifejezésekre való keresés esetén már kevésbé egyértelmű kép rajzolódik ki. A vizsgálat során az alábbi szavak az „embertömeg” („crowd”) kifejezés párosításával képezték a publikációk címében való keresés tárgyát: (2. Táblázat)

- „stampede”: bélyegzés, fejvesztett menekülés, mely gyakran a tömegben előforduló mindennemű balesettel összefüggésben használt;
- „crush”: összetörés, zúzás értelmezésű, szintén a tömegben előforduló minden baleseti formára alkalmazott;
- „walk”: séta, gyaloglás;
- „flow”: folyam, áramlás;
- „panic”: pánik, riadalom, gyakran a tömegben előforduló minden baleseti formára alkalmazott kifejezés;
- „surge”: hullámozás;
- „injuries”: sérülések.

idézési téma	kifejezések a címben						
	(„crowd stampede”) N=223	(„crowd crush”) N=91	(„crowd walk”) N=1408	(„crowd flow”) N=4320	(„crowd panic”) N=395	(„crowd surge”) N=215	(„crowd injuries”) N=521
közlekedés	1. (57%)	1. (55%)	1. (38%)	1. (38%)	1. (60%)		1. (19%)
neuroscanning					3. (2%)		
numerikus módszerek			3. (4%)				
egészségügyi ellátás						1. (13%)	3. (5%)

idézési téma	kifejezések a címben						
	(„crowd stampede”) N=223	(„crowd crush”) N=91	(„crowd walk”) N=1408	(„crowd flow”) N=4320	(„crowd panic”) N=395	(„crowd surge”) N=215	(„crowd injuries”) N=521
baleseti sebészet	3. (4 %)	2. (9 %)		3. (5 %)		3. (9 %)	2. (15%)
számítógépes látás és grafika	2. (19 %)	3. (9 %)	2. (6 %)	2. (13%)	2. (7 %)		
megosztott és valós idejű számítás						2. (11%)	

2. Táblázat, A WoS adatbázisában szereplő publikációk címében megjelenő, az angolnyelvű szakirodalomban gyakran tömegmozgással és balesetekkel összefüggésben használt kifejezések és az idézetek mezo-szintű téma-besorolásai, az adott kifejezéspár esetében az előfordulási rangsor első három tagjának a teljes hivatkozási területen mért százalékának megadásával, vizsgálat ideje: 2023.05.14.

A nemzetközi szakirodalmi áttekintéséből megállapítható, hogy a veszély és a tömegmozgás fogalmainak tematikus velejárója az egészségügyi ellátás szükségessége, azaz a baleset. Elengedhetetlenül szükséges tehát a megfelelő fogalmak megtalálásánál, az egyes mozgásfolyamatok rendszerezésénél ezen negatív történés figyelembevétele, az események folyamatának alaposabb megismerése.

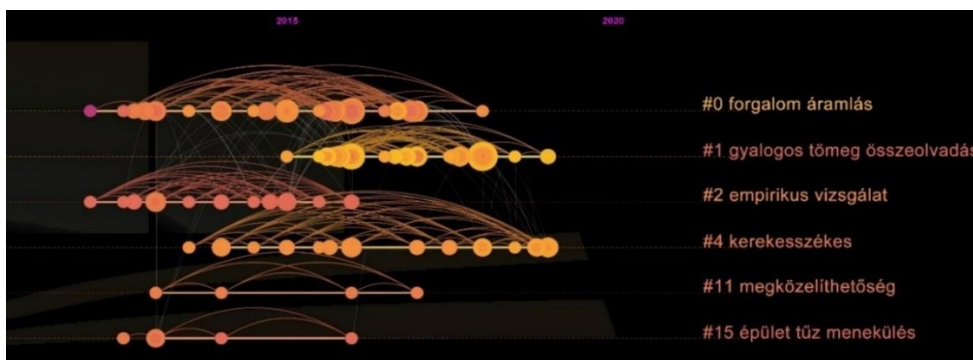
A „vészhelyzet és mozgás” („emergency, movement”) kifejezések a WoS adatbázisban szereplő 7100 publikáció címében találhatóak meg. Az 1500 releváns publikáció összesen hat nagy klasztert alkot. Ezek sorszám / méret / LSI / LLR / MI felsorolás szerint rendre a következők:

- #0 / 40 / építészeti tervezés / forgalom áramlat / gyalogos mozgás dinamika
- #1 / 34 / sokemeletes épület vészkiürítési viselkedése / forgalom áramlat / gyalogos tömeg összeolvadás
- #2 / 19 / embertömeg / empirikus vizsgálat / hozzáférhetőség
- #4 / 16 / kerekesszékes / kerekesszékes / gyalogos mozgás
- #11 / 9 / fogyatékkal élők sürgősségi menekítése: gyakorlatok, szimulációk és hozzáférhetőség felmérése / hozzáférhetőség / hozzáférhetőség
- #15 / 7 / elrettentő kijárat jelzések / épület tűz kiürítés / személyhajó

A két legnagyobb, vészhelyzethez és mozgáshoz kötődő klaszter tehát az épített környezettel, és a tömegdinamikával együttesen foglalkozik. Velük együtt alkotja a terület magját az empirikus vizsgálatok területe. Tőlük távolabb a kerekesszéket használók mozgása és a fogyatékkal élők sürgősségi menekítése. A hatodik legnagyobb klaszterben pedig a meneküléssel kapcsolatos jelzések témaköre szerepel, az épületek és hajók tüzesetével is összefüggésben. (1. ábra) (2. ábra)



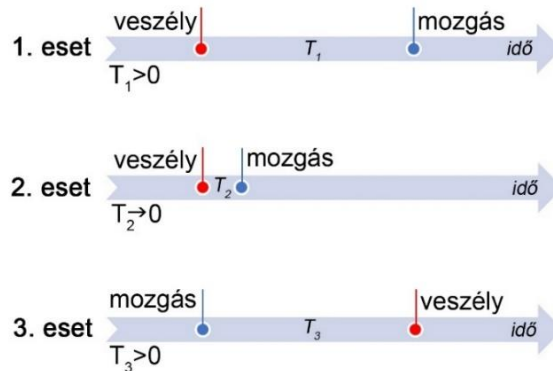
1. ábra, vészhelyzet és mozgás („emergency movement”) kifejezések címszavakban való előfordulása szerint listázott első 1500 releváns publikáció hivatkozási és tudományos klaszter rendszere



2. ábra, vészhelyzet és mozgás („emergency movement”) kifejezések címszavakban való előfordulása szerint listázott első 1500 releváns publikáció hivatkozási és tudományos klaszter rendszere időrendben

A VÉSZHELYZETI MOZGÁSOK IDŐBENI ELTÉRÉSEI

A vészhelyzeti tömegmozgások általános jellemzője a mozgás fő motivációja, miszerint az egyének valamilyen vélt, vagy valós veszélyforrás elől biztonságos helyzetbe szeretnének kerülni, vagy éppen elszenvető alanyai a kialakult veszélyhelyzetnek. Az egyes folyamatok ok-okozati összefüggéseinek keresésénél a történések időbelisége kulcsfontosságú. Eszerint a mozgás követheti a vészhelyzetet, kialakulhat azzal közel egyidőben, de akár oka is lehet annak. (3. ábra)



3. ábra, veszélyforrás és vészhelyzeti mozgások időbeni megjelenése

Az első esetre jellemző példa a kiürítés, menekülés folyamata. A második eset jellegzetességeit a tömegben fellépő hirtelen reakciómozgások mutatják. A harmadik esetre az előzetes külső fizikai vészhelyzettel nem rendelkező események szolgáltatnak példát.

A MENEKÜLÉS

A tűzvédelem területén a vészhelyzeti tömegmozgás jellemzően a menekülés folyamata, mely a hazai és nemzetközi gyakorlatban egyaránt az észlelési idő, a kiürítés előtti időtartam és a kiürítés időtartamának hármásából áll. A kiürítés előtti időtartam a riasztási idő, az érzékelési idő, az értelmezési idő és a döntésmeghozatali idő egymásutánjaként írható le, mely folyamatok együttese akár percekig is eltarthat. [11] [12] A meneküléshez szükséges idő (RSET, TNE) tehát meghatározható, ahogyan a menekülésre alkalmas körülmények fennállásának határáig tartó menekülésre rendelkezésre álló idő (ASET, TAE) is. A veszélyforrás keletkezése tehát megelőzi az egészséget veszélyeztető tényező bekövetkezését idejéig. (3. ábra, 1. eset) értéke pedig ASET, TAE. [13] A tűzvédelem területén belül használt „evacuation” (kiürítés, menekülés) kifejezés a veszélyhelyzet bekövetkezése után történő haladási folyamat megnevezésére releváns, a szakirodalomban elterjedt.

A REAKCIÓ-MOZGÁS

A vészhelyzeti tömegmozgások csoportján belül fentiekől eltérő jellegzetességekkel rendelkeznek azon események, melyeknél az életveszélyes helyzet hosszabb előzmény nélkül alakul ki, a menekülés folyamata pedig ezen esemény után, hirtelen reakcióként történik. (3. ábra, 2. eset) Példaként ide sorolhatóak a tömegben történt terrortámadások, közvetlen fegyveres fenyegetések, szerkezeti elemek gyors tönkremenetele, vagy természeti csapások után bekövetkező mozgásfolyamatok. További jellegzetességként nevezhető meg, hogy a tűzvédelmi menekülés folyamatában a kiürítés előtti idő értékének egyénienkénti változatossága, valamint a gyakran térkapcsolatokon áthaladó, egyénileg változó úthosszakat eredményező jellegzetességei a torlódások kockázatát csökkenthetik, ugyanakkor a hirtelen reakcióként jellemzett tömegmozgásokban az egyének közel azonos sebességgel és időben, gyakran azonos térből egyszerre reagálnak. Ezen események baleseti és fizikai, ket-

tős szemléleti megközelítésű kutatását nagyban nehezíti, hogy a részletes hatósági, orvosszakértői, vagy igazságügyi vélemények rendelkezésre állása nélkül nehezen különíthető el a balesetek közül, melyik a közvetlen kiváltó ok, és melyik az esemény után kialakuló tömegmozgás következménye. A jelenséget ugyanakkor minden esetben a történés környezetében lévő emberek gyors és kollektív reagálása jellemzi. Ennek megfelelően a vészhelyzeti reakció-mozgás kifejezés használata javasolható együttes leírásukra.

ÖNGERJESZTŐ FOLYAMATOK

A vészhelyzeti tömegmozgás folyamatok között önálló jellegzetességekkel bírnak azon események, melyeknél a tömeg mozgása, vagy a tömeg több tagjának egyéni, illetve kollektív viselkedése maga a potenciális veszélyforrás. (3. ábra, 3. eset) Ezen esetekben jellemzően nem határozható meg életveszélyesnek ítélt előzetes külső fizikai jelenség, [14] a történések az embertömeg egyfajta öngerjesztő folyamatoként következnek be. Ezen csoportba sorolhatóak:

- a tömeget alkotó egyének nagyon magas számánál jelen lévő, erős motiváció hatására kialakuló, aszimmetrikus mozgásfolyamatok;
- extrém zenei eseményeken előforduló testi aktivitások; [15][16][17]
- a tömeg igen nagy létszámsűrűségére visszavezethető jelenségek; [18]
- a reakció-mozgások vélt veszélyforrású módosulatai (pl. tömeg hirtelen szétnyílása, dinamikus tömegáramlás).

Az öngerjesztő tömegmozgás folyamatok és a reakció-mozgások közötti legnagyobb eltérés ezen megközelítés szerint tehát egyértelműen a valóságos és észlelt életveszélyes helyzet fizikai megléte, vagy annak hiánya. Ugyanakkor a tömeg mozgása nem írható le megfelelően a kollektív viselkedés területén elért szociológiai és pszichológiai felismerések [19] [20], az aktuális társadalmi fenyegetettségérzet [21] figyelembevételével. A tömeg egészének, egyes csoportoknak, vagy az egyéneknek a társadalomtudományok területén megfogalmazott jellemzőinek nemcsak a mozgás folyamatára, de akár – különösen az öngerjesztő folyamatok csoportján belül – a veszély keletkezésére is igen nagy hatásuk lehet. Adott mozgásfolyamat valós külső fizikai ok nélkül is végbe mehet a reakció-mozgásokkal nagymértékben egyező módon, példaként vélt veszélyforrás esetén. Ugyanakkor a fizikai és baleseti kettős megközelítés esetén az öngerjesztő folyamatok elkülönítése a fizikai külső tényezők kizárásával a történések pontosabb feltárására adhat lehetőséget, mely különösen a kevés hiteles dokumentációval rendelkező esetek megértésében nyújthat segítséget.

Aszimmetrikus öngerjesztő mozgásfolyamatok

Curtis és munkatársai [22] a gyalogosmozgások hitelesebb szimulációja okán javasolják a tolokodás figyelembevételét, melyet aszimmetrikus egyéni interakcióként jellemeznek. Munkájukban két domináns eseményt jelöltek meg a jelenség folyamatoként, így a metróperonon már várakozó emberek és a későn jövő, tolokodó emberek mozgásjelenségét, továbbá a Tawaf iszlám zarándoklati rituálét. A látványosságok, nagy érdeklődésre számot tartó pontok (PoI, Point of Interest) körül csoportosuló tömeg jellegzetességei a gyalogosmozgások vonatkozásában szintén meghatározóak. [23] Martinez-Perdiguero [24] a PoI-k

környezetében elhelyezkedő emberek és a fermionoknál felismert Fermi-Dirac eloszlás közötti illeszkedést írta le, egy szabadtéri koncert színpad körül csoportosuló tömeg és egy bevásárlóközpont parkolójában álló autók mintáján. [24] Egy öt főből álló sor hátulról érkező lökés hatására történő elmozdulását vizsgálták elméleti és kísérleti megközelítéssel Wang és munkatársai. [25] Eredményeik szerint a sor hátulról érkező lökés hatására dominóként viselkedik, az impulzus azonban nem egyenletesen terjed. Feldmann és Adrian [26] hasonló kísérleti beállításokkal végzett megfigyelései szerint a sorban hátul álló egyént meglökve az ütés továbbadásának módja függ a lökés erősségétől, és a személyek távolságától. Elméletük szerint az egy sorban álló emberek esetén a lökés terjedése nem dominóként, hanem fordított ingaként modellezhető. Song és munkatársai [27] tanulmányukban a hátulról érkező lökés nagysága, a személyek távolsága és száma közötti összefüggéseknek megfelelő, módosított szociális-erő modellt javasoltak, hat elemből álló dominósr hatását vizsgálva.

Megtörtént esetek vizsgálatából megállapítható, hogy a fenti elvekhez hasonlatos mozgások a tömegben különösen veszélyesek lehetnek, akár kisebb résztvevőlétszám esetén is halálos kimenetelű baleseteket okozhatnak. A tömegben lévő motiváció erőssége ugyanis nemcsak a tömeg leghátsó sorát, hanem egy egész hátsó mezőt, vagy akár az egész tömeget elmozdulásra készítheti. A jelenség a mozgásvonalak irányultsága alapján elkülöníthető vonalmenti és koncentrikus formákra.

A vonalmenti aszimmetrikus mozgásoknál a tolóerő a tömeg szélesebb tartományában, párhuzamosan jelenik meg. A jelenség megfigyelhető a 25 sérültet eredményező 2019. augusztus 31-i Seattle's Bumbershoot fesztivál Jai Wolf koncertjén történt kordon összeomlás előtt. A rendezvényen 3000 résztvevő sorakozott fel a legalább 20 méter széles színpad előtt, becsült létszámsűrűségük helyenként elérte a 6 fő/m^2 értéket. (4. ábra) A nézők közel sík, füves területen álltak. A színpad előtt 120 cm magas kordon állt. A koncert kezdetekor a hátul állók nagy számban és egyidőben léptek közelebb a színpad felé, az első sorokban állók előre zuhanását okozva. (videó 1., 0:49-0:57)



4. ábra, 2019. augusztus 31-i Seattle's Bumbershoot fesztivál Jai Wolf koncert, forrás: komonews.com

Az aszimmetrikus mozgások koncentrikus módozatában a tömeg szélességi méretéhez képest pontszerű irányultsággal rendelkeznek. (5. ábra)(6. ábra) Ezen igen magas érdeklődési értékkel rendelkező terület (javasolt megnevezés: HPOI, High Point of Interest) irányában történő kollektív elmozdulás az üvegyak („bottle neck”) hatáshoz igen hasonló

mozgásformákkal jellemezhető. Különbség azonban ezen esetben a kijárat hiánya, vagy nagymértékben korlátozott volta.



5. ábra, adományosztás, Pakisztán,
forrás: awazthevoice.in



6. ábra, Black Friday akció, Washington,
forrás: der-postillon.com

Az aszimmetrikus öngerjesztő vészhelyzeti tömegmozgások esetében a tömeg teljes egészére jellemző nagyon erős motiváció már kisebb létszámú embercsoport esetén is halálos kimenetelű baleseteket okozhat. A motiváció lehet:

- tárgyak megszerzése (pl. adományosztások², vagy kereskedelmi akciók³);
- eseményekre való bejutás⁴;
- személyekkel való kontaktus⁵;
- társadalmilag előnyös feltételek megszerzésének lehetősége.⁶

Ezen külső kiváltó életveszélyes fizikai ok nélküli, de életveszélyessé váló erős tömegmotivációval jellemezhető események társadalmi oka feltételezhetően a szociológia és pszichológia területein felismert szűkösség („scarcity”) [28], a lemaradástól való félelem („FoMO, Fear of Missing out”), a versengő magatartás és a tömeg érzelmfokozó hatásának együttesével magyarázható.

Extrém zenei eseményeken előforduló testi aktivitások („mosh”)

A rock, metal és punk koncertek nézői között gyakran előforduló, a tömeg többi tagjával való egyéni vagy csoportos, szándékos dinamikus fizikai kontaktusok („moshing”) sorolhatóak ezen mozgásfolyamatok körébe. (2. videó) A „moshing” mozgás egyfajta ritualizált tánc, mely a fizikai agressziót az érzelmek kollektív megjelenítésével ötvözi. [29] A „mosh pit”, „circle pit”, „wall of death” fogalmak (angol nyelvű megnevezésükkel terjedtek el a magyar koncertlátogatók körében, ritkán magyarul: körgödör, halál fala) a sűrű tömegben agresszív, lökdösődő körkörös táncként, illetve a tömegből kiváló két csoport szándékos egymásnak rohanásaként írhatóak le. Silberberg és munkatársai [15] kutatásukban a

² 2023. április 20., Jemen, Sannaa, 85 halálos áldozat; 2023. március., Pakisztán, 16 halálos áldozat

³ 2008. november 30., Black Friday akció, New York, USA 1 halálos áldozat; 2004. szeptember 2., IKEA nyitás, Jeddah, Szaúd-Arábia; 3 halálos áldozat

⁴ 2010. október 24., Nyayo Nemzeti Stadion, Nairobi, Kenya, 7 halálos áldozat

⁵ 2011. február 22., Modibo Keita Stadion, Bamakó, Mali, vallási rendezvény, 36 halálos áldozat

⁶ 2020. október 21., Jalabad, Afganisztán, vízumkérelmek beadása, 15 halálos áldozat

„mosh pit” jelenségét rendezetlen gázszerű állapotként, míg a körgödör („circle pit”) folyamatát rendezett örvényszerű állapotként határozták meg. Milsten és munkatársai [30] nyolc koncert látogatói között történt balesetekről készített tanulmányából megállapítható, hogy a „mosh pit”-ekből származó, tízezer koncert-résztevőre jutó balesetek száma (PPTT) legalább átlagosan 26 volt. Hasonló eredményre (25,1) jutottak Janchar és munkatársai [16]. Az esetek legnagyobb részét (64%) fejsérülések tették ki.

Létszámsűrűségből adódó mozgásfolyamatok

A résztvevők túlzott létszámsűrűségére visszavezethető tragédiák közül a 21 halálos áldozatot és 652 sérülést követelő, 2010. július 24-én Duisburgban történt Love Parade fesztivál tragédiája (3. videó, 4. videó) a sűrű tömegben fellépő balesetek vonatkozásában az elmúlt évtized legtöbbet hivatkozott eseményei közé tartozik. A történéseket rögzítő, nagyszámú térfigyelő kamera jó minőségű felvételeinek nyilvánossá tétele nagymértékben segítette a vonatkozó kutatásokat. Az eredmények hatalmas mérföldkövet jelentettek az álló, nagyon sűrű tömegben bekövetkező vészhelyzeti mozgásfolyamatok megismerésében. Tanulmányok születtek a sebességmezők detektálására [31], a fellépő turbulens áramlások és az erőterjedés sebesség-ingadozás előidézőjeként tartott, gyalogosok közötti érintkezés összefüggésére. A tömegben bekövetkező ún. tömegrengés („crowd-quakes”) jelenségét a létszámsűrűség és a sebesség együttes következményeként állapították meg. Rekonstruáltak egy nagyobb áramlási mezőt, mely a folyadékokra jellemző örvények jellegzetességeit mutatta [32]. Felismerésre került, hogy egyéb, sűrű tömegekben jellemző folyamatokhoz képest a duisburgi tragédiában rövidebb, többirányú és szabálytalan áramlásvektorok voltak detektálhatóak, a tömegben belüli kéttengelyű mozgás helyett pedig csak előre-hátra való mozgás volt lehetséges. [33] Tanulmányozásra került a nagylétszámú tömegben fellépő összetartó mozgásokra összpontosítva a sebességentrópia értékek és a torlódások összefüggése. [34] Egyéb kutatások szerint ugyanakkor a sűrű tömegre jellemző, feltárt turbulens áramlás és a meg-megálló („stop-and-go”) folyamatok nem feltétlenül a földrengésszerű "nyomásfelszabadulás" eredményei, a hirtelen sebességváltozásokból ugyanakkor elesések keletkezhetnek. Az ilyen típusú baleseteket helytelenül taposásnak és elsodrásnak („trampling” és stampede”) nevezték meg, holott az orvosszakértői vélemények kevesebb százalékban ismerik fel ezen sérüléseket elesés következményének, sokkal inkább fulladásnak. A turbulens áramlások kiváltó okaiként a tömegben haladók és állók, illetve a haladók miatt haladásra kényszerülő állók jelensége egyfajta vezető-követő mechanizmusként is leírásra került, kiemelve az egyének között fellépő különböző érintkezéseket. [35] Vizsgálat készült továbbá a negatív érzelmek tömegben való terjedéséről. [36] Összefoglalták a sérültekről és kezelésükről rendelkezésre álló adatokat, melyhez hasonló részletességű statisztikákat tartalmazó szakirodalom tömegkatasztrófáról még nem született. [37].

A megtörtént esetek sorában a duisburgi fesztivál tragédiája kiemelkedően jól dokumentált. Ennek ellenére a vonatkozó kutatások között nem található meg egyértelműen, a helyszínen pontosan hol és milyen okból következtek be balesetek. A nyilvánossá tett, elemzett videók felvételei az első haláleset bekövetkezése előtt 20 perccel befejeződnek, így az elemzések a balesetek előtti veszjósló mozgásokról tanulságos képet adnak, a hasonló esetek megelőzéséhez elengedhetetlenül szükségesek, a történések és okozati összefüggések felismerése azonban még mindig hiányos. Megfigyelhető továbbá, hogy az esetet leíró

szakirodalomban a résztvevők magas létszámsűrűsége a tragédia legfontosabb kiváltó jellemzőjeként ismertetett, ezen jellemző pontos értékeinek megadása, változásának folyamata mégsem képezte a vizsgálatok tárgyát.

A duisburgi tragédiát még számtalan, a résztvevők nagy létszámsűrűségére visszavezethető hasonló eset követte. Valószínűsíthető, hogy két, teljesen eltérő jelenség okozza a statikus tömeg létszámsűrűségére visszavezethető halálos baleseteket. A tömegben jelenlévő, mellkasra ható oldalirányú erő álló helyzetben lévő résztvevőknél is halálos kimenetelű kompressziós fulladást (asphyxia) okozhat. [38] A jelenség a nyomásértékek heterogenitása okán egy nagyobb terület (pl. szektor) eltérő pontjain is felléphet, mint az megfigyelhető volt az Astroworld Fesztivál⁷ esetében is. (5. videó) Eltérő folyamat a nagy létszámsűrűségben előforduló csoportos stabilitásvesztés jelensége. Hatására akár 3-4 sorban egymáson heverő áldozatok százai kerülnek életveszélyes, fulladást okozó helyzetbe. (6. videó) A tragikus folyamat igen nagyszámú áldozattal jár.⁸⁹ Elnevezésére a tömegomlás kifejezés lehet megfelelő.

ÖSSZEGLÉS

A tanulmány szcientometriai mutatók, a vonatkozó szakirodalom és megtörtént esetek vizsgálata alapján javaslatot tesz a normál és vészhelyzeti tömegmozgások elkülönítésére, a mozgásfolyamatok és a bekövetkezett balesetek eltérősége okán. A vészhelyzeti tömegmozgásokon belül a történések időbelisége szerint a „menekülés” a „reakció-mozgások” és az „öngerjesztő folyamatok” megkülönböztetését ajánlja. Az öngerjesztő folyamatokon belül az aszimmetrikus öngerjesztő, az extrém zenei eseményeken előforduló testi aktivitások és a létszámsűrűségből adódó mozgásfolyamatok eltérő vizsgálatát javasolja.

VIDEÓ HIVATKOZÁSOK

sz.	helyszín, dátum	videó
1	Seattle's Bumbershoot fesztivál, 2019. 08 31.	https://www.youtube.com/watch?v=IfO9_njAOYQ
2	Körgödör és halál fala jelenségek, 2014.	https://www.youtube.com/watch?v=9LvE8jp77b8
3	Love Parade, Duisburg, kamera 15 (alagút), 2010.07.24.	https://www.youtube.com/watch?v=osLQIVR--fU
4	Love Parade, Duisburg, kamera 13 (rampa), 2010. 07.24.	https://www.youtube.com/watch?v=QpzISdBE3dA

⁷ 2021. november 5., Travis Scott koncert, Astroworld, Houston, USA, 8 halálos áldozat

⁸ 2010. november 22., Lámpásfesztivál, Phnom Pen, Kambodzsza, 375 halálos áldozat

⁹ 2022. október 29., Halloween party, Szöul, Dél-Korea, 159 halálos áldozat

sz.	helyszín, dátum	videó
5	Travis Scott koncert, Astroworld, Houston, USA, 2021.11.5.	https://www.youtube.com/watch?v=LGXwJn-ZSikQ a videó a nyugalom megzavarására alkalmas jeleneteket tartalmaz!
6	Phnom Pen, Kambodzsa, 2010.11.22.	https://www.youtube.com/watch?v=t8Upo-QmN7uI a videó a nyugalom megzavarására alkalmas jeleneteket tartalmaz!
7	Halloween party, Szöul, Dél-Korea, 2022.10.29.	https://www.youtube.com/watch?v=DJ4e2tSeKB0 a videó a nyugalom megzavarására alkalmas jeleneteket tartalmaz!

FELHASZNÁLT IRODALOM

- [1] W. Weng, J. Wang, L. Shen, and Y. Song, 'Review of analyses on crowd-gathering risk and its evaluation methods', *Journal of Safety Science and Resilience*, vol. 4, no. 1, pp. 93–107, 2023, doi: <https://doi.org/10.1016/j.jnlssr.2022.10.004>.
- [2] C. Chen, 'Searching for intellectual turning points: Progressive knowledge domain visualization', *Proceedings of the National Academy of Sciences*, vol. 101, no. suppl_1, pp. 5303–5310, 2004, doi: 10.1073/pnas.0307513100.
- [3] M. Haghani, 'The knowledge domain of crowd dynamics: Anatomy of the field, pioneering studies, temporal trends, influential entities and outside-domain impact', *Physica A: Statistical Mechanics and its Applications*, vol. 580, 2021, doi: 10.1016/j.physa.2021.126145.
- [4] J. Adrian *et al.*, 'A Glossary for Research on Human Crowd Dynamics', *Collect Dyn*, vol. 4, 2019, doi: 10.17815/cd.2019.19.
- [5] H. Lügering, D. Tepeli, and A. Sieben, 'It's (not) just a matter of terminology: Everyday understanding of "mass panic" and alternative terms', *Saf Sci*, vol. 163, p. 106123, 2023, doi: <https://doi.org/10.1016/j.ssci.2023.106123>.
- [6] Y. Zhu, M. C. Kim, and C. Chen, 'An investigation of the intellectual structure of opinion mining research', *Information Research*, vol. 22, no. 1, 2017.
- [7] S. Deerwester, S. T. Dumais, G. W. Furnas, T. K. Landauer, and R. Harshman, 'Indexing by latent semantic analysis', *Journal of the American Society for Information Science*, vol. 41, no. 6, 1990, doi: 10.1002/(SICI)1097-4571(199009)41:6<391::AID-ASII>3.0.CO;2-9.
- [8] T. Dunning, 'Accurate methods for the Statistics of Surprise and Coincidence', *Computational Linguistics*, vol. 19, no. 1, 1993.
- [9] L. Zheng, 'Using mutual information as a cocitation similarity measure', *Scientometrics*, vol. 119, no. 3, 2019, doi: 10.1007/s11192-019-03098-9.
- [10] J. Liu, Y. Chen, and Y. Chen, 'Emergency and disaster management-crowd evacuation research', *J Ind Inf Integr*, vol. 21, 2021, doi: 10.1016/j.jii.2020.100191.

- [11] M. Forsberg, J. Kjellström, H. Frantzich, A. Mossberg, and D. Nilsson, 'The Variation of Pre-movement Time in Building Evacuation', *Fire Technol*, vol. 55, no. 6, pp. 2491–2513, Nov. 2019, doi: 10.1007/s10694-019-00881-1.
- [12] M. Kobes, I. Helsloot, B. de Vries, and J. Post, 'Exit choice, (pre-)movement time and (pre-)evacuation behaviour in hotel fire evacuation — Behavioural analysis and validation of the use of serious gaming in experimental research', *Procedia Eng*, vol. 3, pp. 37–51, 2010, doi: <https://doi.org/10.1016/j.proeng.2010.07.006>.
- [13] L. László *et al.*, 'Tűzvédelmi Műszaki Irányelv (TvMI), Kiürítés, 2.5:2022.06.13.' Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság, pp. 5–7, 2022.
- [14] L. Sun and N. I. Badler, 'Exploring the consequences of crowd compression through physics-based simulation', *Sensors (Switzerland)*, vol. 18, no. 12, 2018, doi: 10.3390/s18124149.
- [15] J. L. Silverberg, M. Bierbaum, J. P. Sethna, and I. Cohen, 'Collective motion of humans in mosh and circle pits at heavy metal concerts', *Phys Rev Lett*, vol. 110, no. 22, 2013, doi: 10.1103/PhysRevLett.110.228701.
- [16] T. Janchar, C. Samaddar, and D. Milzman, 'The mosh pit experience: Emergency medical care for concert injuries', *American Journal of Emergency Medicine*, vol. 18, no. 1, 2000, doi: 10.1016/S0735-6757(00)90051-2.
- [17] T. Janchar, R. Samaddar, and D. Milzman, 'The impact of "mosh pits" on medical incidents at mass gatherings', *Ann Emerg Med*, vol. 34, no. 4, 1999, doi: 10.1016/s0196-0644(99)80340-0.
- [18] R. S. C. Lee and R. L. Hughes, 'Exploring trampling and crushing in a crowd', *J Transp Eng*, vol. 131, no. 8, 2005, doi: 10.1061/(ASCE)0733-947X(2005)131:8(575).
- [19] J. Drury, 'Recent developments in the psychology of crowds and collective behaviour This review comes from a themed issue on Social change (rallies, riots and revolutions) (2020) Crowds and conflict', *Curr Opin Psychol*, vol. 2020, 2020.
- [20] A. Templeton, J. Drury, and A. Philippides, 'From mindless masses to small groups: Conceptualizing collective behavior in crowd modeling', *Review of General Psychology*, vol. 19, no. 3, 2015, doi: 10.1037/gpr0000032.
- [21] A. B. Pál, 'Az elrettentés művészete A hadiipar szerepe a fegyverkezési versenyben', *Biztonságtudományi Szemle*, vol. 4, no. 3, pp. 27–28, 2022.
- [22] S. Curtis, B. Zafar, A. Gutub, and D. Manocha, 'Right of way', *Vis Comput*, vol. 29, no. 12, pp. 1277–1292, 2013, doi: 10.1007/s00371-012-0769-x.
- [23] J. Was and R. Lubaś, 'Towards realistic and effective Agent-based models of crowd dynamics', *Neurocomputing*, vol. 146, 2014, doi: 10.1016/j.neucom.2014.04.057.
- [24] J. Martinez-Perdiguero, 'Fermion-like behavior of elements/agents in their spatial distribution around points of interest', *Physica A: Statistical Mechanics and its Applications*, vol. 557, 2020, doi: 10.1016/j.physa.2020.124905.
- [25] C. Wang, S. Ni, and W. Weng, 'Modeling human domino process based on interactions among individuals for understanding crowd disasters', *Physica A: Statistical Mechanics and its Applications*, vol. 531, 2019, doi: 10.1016/j.physa.2019.121781.
- [26] S. Feldmann and J. Adrian, 'Forward propagation of a push through a row of people', *Saf Sci*, vol. 164, p. 106173, 2023, doi: <https://doi.org/10.1016/j.ssci.2023.106173>.

- [27] Y. Song, X. Hu, L. C. Shen, and W. Weng, 'Modeling Domino Effect Along the Queue Using an Improved Social Force Model', *SSRN Electronic Journal*, 2023, doi: 10.2139/ssrn.4357736.
- [28] J. Zhao and B. M. Tomm, 'Psychological Responses to Scarcity', in *Oxford Research Encyclopedia of Psychology*, 2018. doi: 10.1093/acrefore/9780190236557.013.41.
- [29] G. Riches, 'Embracing the Chaos: Mosh Pits, Extreme Metal Music and Liminality', *Journal for Cultural Research*, vol. 15, no. 3, 2011, doi: 10.1080/14797585.2011.594588.
- [30] A. M. Milsten, J. Tennyson, and S. Weisberg, 'Retrospective Analysis of Mosh-Pit-Related Injuries', *Prehosp Disaster Med*, vol. 32, no. 6, 2017, doi: 10.1017/S1049023X17006689.
- [31] B. Krausz and C. Bauckhage, 'Loveparade 2010: Automatic video analysis of a crowd disaster', *Computer Vision and Image Understanding*, vol. 116, no. 3, 2012, doi: 10.1016/j.cviu.2011.08.006.
- [32] J. Ma, W. G. Song, S. M. Lo, and Z. M. Fang, 'New insights into turbulent pedestrian movement pattern in crowd-quakes', *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2013, no. 2, 2013, doi: 10.1088/1742-5468/2013/02/P02028.
- [33] J. Wang, W. Weng, and X. Zhang, 'Comparison of turbulent pedestrian behaviors between Mina and Love Parade', in *Procedia Engineering*, 2014. doi: 10.1016/j.proeng.2014.10.477.
- [34] L. Huang, T. Chen, Y. Wang, and H. Yuan, 'Congestion detection of pedestrians using the velocity entropy: A case study of Love Parade 2010 disaster', *Physica A: Statistical Mechanics and its Applications*, vol. 440, 2015, doi: 10.1016/j.physa.2015.08.013.
- [35] J. Ma, W. Song, and S. Lo, 'Simulation of crowd-quakes with heterogeneous contact model', in *Traffic and Granular Flow, 2013*, 2015. doi: 10.1007/978-3-319-10629-8_12.
- [36] T. Xu, D. Shi, J. Chen, T. Li, P. Lin, and J. Ma, 'Dynamics of emotional contagion in dense pedestrian crowds', *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 384, no. 3, 2020, doi: 10.1016/j.physleta.2019.126080.
- [37] O. Ackermann *et al.*, 'Patient care at the 2010 Love Parade in Duisburg, Germany: clinical experiences.', *Dtsch Arztebl Int*, vol. 108, no. 28–29, 2011.
- [38] J. P. Nolan *et al.*, 'Compression asphyxia and other clinicopathological findings from the Hillsborough Stadium disaster', *Emergency Medicine Journal*, vol. 38, no. 10, 2021. doi: 10.1136/emered-2020-209627.

**RISK ANALYSIS OF THE RESERVOIR OF A
MINING WASTE MANAGEMENT
FACILITY****BÁNYÁSZATI HULLADÉKKEZELŐ
LÉTESÍTMÉNY TÁROZÓJÁNAK
KOCKÁZATELEMZÉSE**ELEK Barbara¹ - BODNÁR László² - HORVÁTH-KÁLMÁN Eszter³**Abstract**

Mining waste management facilities can be referred to as the largest engineering structures in the world. Their serious accidents draw attention to the fact that these facilities have a potentially increasing danger through climate change and structural aging. Therefore, it is a very important task for the engineers of our time to explore the human, environmental and social risk of these facilities. In this article, we present a risk analysis method that can provide quick and effective help for the evaluation of the reservoirs of mining waste management facilities from a disaster prevention point of view, for determining the risk, and for planning external and internal defenses in the event of a potential accident.

Keywords

mining waste management facility, reservoir, risk analysis method

Absztrakt

A bányászati hulladékkezelő létesítmények a legnagyobb mérnöki szerkezetek közé sorolhatók a világon. Súlyos baleseteik felhívják a figyelmet arra, hogy ezek a létesítmények a klímaváltozás, valamint szerkezeti elöregedésük révén potenciálisan egyre növekvő veszélyt hordoznak magukban. Emiatt a jelen kor mérnökei számára kiemelten fontos feladat ezen létesítmények humán, környezeti, valamint társadalmi kockázatának feltárása. Tanulmányunkban egy olyan kockázatelemzési módszert mutatunk be, mely gyors és hatékony segítséget nyújthat a bányászati hulladékkezelő létesítmények tározóinak katasztrófavédelmi szempontú értékeléséhez, a kockázat meghatározáshoz, illetve a külső és belső védekezés megtervezéséhez egy potenciálisan bekövetkező baleset esetén.

Kulcsszavak

bányászati hulladékkezelő létesítmény, tározó, kockázatelemzési módszer

¹ elek.barbara@bgk.uni-obuda.hu | ORCID: 0000-0001-7515-6374 | associate professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Institute of Safety Science and Cybersecurity | egyetemi docens Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Biztonságtudományi és Kibervédelmi Intézet

² bodnar.laszlo@uni-nke.hu | ORCID: 0000-0001-9196-8030 | assistant lecturer, University of Public Service, Department of Fire Protection Engineering | tanársegéd, Nemzeti Közszerológiai Egyetem, Tűzvédelmi Mérnöki Tanszék

³ kalman.eszter@ybl.uni-obuda.hu | ORCID: 0009-0003-5199-3751 | associate professor, Óbuda University, Ybl Miklós Faculty of Architecture and Civil Engineering, Department of Infrastructure Development, | egyetemi docens, Óbudai Egyetem, Ybl Miklós Építéstudományi Kar, Infrastruktúra-fejlesztési és üzemeltetési tanszék

BEVEZETÉS

A bányászati hulladékkezelő létesítmények (pl. zagytározók, meddőhányók) nagy mennyiségű hulladék befogadására kialakított depónia terek, amelyeket a feldolgozó létesítmény közelében alakítanak ki, megfelelő telepítési előírások alapján. A telepítési előírások mindig az adott korszak tudományos - technológiai szintjét, környezeti hatásokra vonatkozó ismereteit tükrözik. Emiatt egy több évtizede létesített tározó lehet, hogy az adott korban korszerűnek számított, de a jelenlegi mérnöki tapasztalatok, tervezési, valamint kivitelezési műszaki előírások alapján valószínűleg már korszerűtlennek minősülhet. Egy évtizedek óta üzemelő, illetve egy már felhagyott tározó elhelyezésének, kialakításának utólagos bírálatakor fontos ezt szem előtt tartani. Továbbá szem előtt kell tartani, hogy egy feltöltött tározó mai kor követelményeit kielégítő biztonsági szempontok szerinti átépítése igen nehezen kivitelezhető, rendkívül költséges folyamat lenne. Ugyanakkor a bányászati hulladékkezelő létesítmények tározói ásványvagyon gazdálkodási szempontból akár igen jelentős másodnyersanyag (pl. vas, titán, réz, ezüst, arany, szén stb.) források is lehetnek. A bányászati hulladékkezelő létesítmények a legnagyobb mérnöki szerkezetek közé sorolhatók a világon. Súlyos baleseteik azonban felhívják a figyelmet arra, hogy ezek a létesítmények a klímaváltozás, valamint szerkezeti eloregedésük révén potenciálisan egyre növekvő veszélyt hordoznak magukban.

Munkánk során egy olyan új kockázatelemzési módszert alkalmaztunk, mely lehetővé teszi, hogy adott bányászati hulladékkezelő létesítmény tározójának kockázatát viszonylag rövid idő alatt hatékonyan meghatározzuk.

SZAKIRODALMI ÁTTEKINTÉS

Az elmúlt 50 esztendőben közel 60 db jelentős zagytározó baleset következett be világszerte [1]. 1990 óta a súlyos társadalmi és környezeti következményekkel járó balesetek száma növekvő tendenciát mutat [2]. A katasztrófák egyike volt a 2010. október 4-én hazánkban bekövetkezett vörösiszap katasztrófa. A WISE Uranium projekt [3] becslései szerint 1961 és 2019 között legalább 2375 ember vesztette életét a zagytározó katasztrófák következtében világszerte.

A zagytározók épsége a jó tervezéstől és helyes üzemeltetéstől kiemelkedő mértékben függ. Általános tapasztalat, hogy a legtöbb súlyos balesetet már az esemény bekövetkezése előtt hetekkel, napokkal arra utaló jelenségek előzik meg. Ezért a megfelelő üzemeltetésnek létfontosságú eleme kell hogy legyen egy hatékony monitoring rendszer [4].

A hazai helyzetet tekintve az Európai Bizottság már 2006/21/EK irányelvében (bányászati hulladék irányelv) [5] előírta a tagállamok részére azt, hogy nyilvántartásba kell venniük azokat a már bezárt és elhagyott bányászati hulladékkezelő létesítményeket, amelyek közép- és rövidtávon komoly humán, környezeti és társadalmi kockázatot jelentenek környezetükre.

Az EU MWD (Mine Waste Directive) munkacsoportja 2010-ben elkészített egy úgynevezett kockázat alapú előszűrés útmutatót [6]. A második lépésnek tekinthető kockázati rangsorolásra (szűrésre) nem készült egységes útmutató, így a rangsorolást az EU tagállamok saját hatáskörben végzik.

A bányafelügyeltől a Szabályozott Tevékenységek Felügyeleti Hatósága vette át a bezárt bányászati hulladékkezelő létesítmények nyilvántartásba vételének, a környezeti

kockázati kiértékelésének és a rangsorolásának feladatát 2022. január 31-től a bányászati hulladékok kezeléséről szóló 13/2022. (I. 28.) SZTFH rendelet [7] alapján. A rendelet értelmében „hulladékkezelő létesítmény: a szilárd vagy folyékony halmazállapotú, oldatban vagy szuszpenzióban lévő bányászati hulladéknak az a)-d) pontban meghatározott időtartamon túl történő gyűjtésére vagy elhelyezésére szolgáló, a bányafelügyelet által engedélyezett kijelölt terület. Ezek a létesítmények magukban foglalnak bármely gátat vagy egyéb, tárolásra, visszatartásra, elkülönítésre szolgáló, illetve a létesítményt egyéb módon szolgáló építményt, továbbá - bár nem kizárólagosan - a meddőhányókat és tározókat, de nem beleértve a bányatérsegeket, amelyekbe a hulladékot az ásvány kitermelését követően rehabilitációs és építési célból visszatöltik” [7].

Az Eötvös Lóránd Geofizikai Intézet (ELGI) elvégezte a bányászati hulladékkezelési irányelvnek megfelelő szűrést és 2020. évi jelentésében [8] részletesen bemutatta azt a két lépcsős vizsgálatot, mely a bezárt bányászati hulladékkezelő létesítmények tározójának kockázati besorolását tette lehetővé hazánkban. Az első lépcsőben az előszűrés (kockázati szűrés), a második lépcsőben a szűrés (kockázati rangsorolás) történt meg. A szűrés paraméterek alapján végzett rangsorolás a rekultivációs paraméterek, az objektum mérete és a térszín dőlése alapján végzett rangsorolást jelentette. A kockázati előszűrést 1046 létesítmény esetében végezték el. Az előszűrés eredményeként 170 létesítmény esetében találták úgy, hogy nincs szükség további vizsgálatra. 876 létesítmény esetén további vizsgálatok váltak szükségessé. A következő lépésben végzett szűrés (kockázati rangsorolás) eredményeként hazánk területén 4 db zagyatározó és 5 db érces meddőhányó esetén határoztak meg magas kockázatot [8].

Fenti kétlépcsős kockázat besorolási vizsgálat is azt mutatja, hogy még jelenleg is található hazánk területén környezeti és társadalmi kockázattal bíró bányászati hulladékkezelő létesítmények. A fennmaradó létesítmények esetében számos további rendelkezik közepes és alacsony kockázattal, tehát nem azonosítható kockázatmentes tározóként. Mindez arra hívja fel a figyelmet, hogy nem tétlenkedhetünk, mindent meg kell tennünk annak érdekében, hogy még egyszer ne történjen meg az ajkai vörösiszap tározó gátszakadásához hasonló katasztrófa.

MÓDSZERTAN

Tanulmányunkban egy hipotetikus bányászati hulladékkezelő létesítmény tározójának - esetünkben zagyatározó – kockázatelemzését végeztük el.

Kockázatelemzés lépései

Az általunk alkalmazott kockázatelemzés lépései az alábbiak voltak:

- Első lépésben azonosítottuk azokat az ún. csúcseseményeket (főeseményeket), amelyek bekövetkezése súlyos balesetet válthat ki.
- Következő lépésként hibafa-elemzéssel feltártuk az egyes csúcsesemények kialakulásához vezető okokat, közbülső és alapeseményeket, majd meghatároztuk a csúcsesemény bekövetkezési valószínűségét (gyakoriságát).
- Harmadik lépésben árvízi következmény számítást végeztünk.
- Utolsó lépésként az egyes csúcsesemények kockázatát kockázatértékelési mátrix segítségével értékeltük. Ennek során a hibafa - elemzés, az árvízi következmény számítás eredményeit, továbbá a potenciális árvízi kármutatót vettük figyelembe.

Hibafa-elemzési módszer

A hibafa elemzés egy olyan minőségi elemző módszer, mely a csúcsesemény (főesemény) okait tárja fel. A hibafa eseményekből és olyan logikai kapukból épül fel, amelyek összekapcsolják az eseményeket annak érdekében, hogy a legfelső nemkívánatos csúcsesemény okai azonosíthatók legyenek. A hibafa egy felülről lefelé építkező fastruktúrájú gráf.

Li Xi-Ling et al. [9] 2001-ben, majd Shu Yongbao et al. [10] 2010-ben alkalmazta a hibafa elemzési módszert zagyatározók baleseteinek vizsgálatánál. 2004-ben Hartford és Baecher [11] gátak biztonsági kérdéseinek vizsgálata során végzett hibafa-elemzést.

Árvízi következmények számítása a súlyosság megítéléshez

A világban bekövetkező zagyatározó balesetek alapján könnyen belátható, hogy a legsúlyosabb környezeti és társadalmi következményei a későbbiekben részletesen vizsgált ún. „Gátsérülés” csúcseseménynek van. Ezért a gát részleges vagy teljes tönkremenetelből eredő árvízi következmények számítása, valamint az elárasztási térképek megszerkesztése rendkívül fontos lehet katasztrófavédelmi szempontból. A legkritikusabb esemény a gát valamely pontján teljes vagy részleges keresztmetszeti törés bekövetkezése, hiszen ekkor a gát mögött lévő folyékony, kvázi folyékony anyag a résen keresztül a gát alatti területeket (szabad térszín feletti területeket) elárasztja. Az árvízi következmények számítását, az elárasztási térképeket ezeknek az eseményeknek a modellezése alapján lehet elkészíteni. A számítási eredmények alapján megmondható, hogy mely területek kerülhetnek veszélybe, illetve hol kell a lakosság riasztására és mentésére kidolgozni a külső védelmi terveket.

A gátsérüléshez, mint csúcseseményhez kapcsolódó közvetett jelenségek közül csak néhány határozható meg mennyiségileg. A tározó gátszakadásának mennyiségileg meghatározható jellemzőit mutatja az 1. táblázat különböző szerzők munkái alapján.

Számítási jellemző	Megjegyzés	Szerzők
A gátszakadás folyamata		
1. gátszakadás nyílásszélessége		
$B_{avg} = 3 \cdot H_w$		U. S. Bureau of Reclamation [12]
2. az átszakadás eróziós törmelékmenyisége		
$V_{er} = 0,0348 \cdot (V_w \cdot H_w)^{0,852}$	beton-, kőgátnál	MacDonald és Langridge-Monopolis [13]
3. kiömlési csúcs hozam		
$Q_p = 0,607 \cdot (V_w^{0,295} \cdot H_w^{1,24})$		Froehlich [14]
4. az átszakadás időtartama	Q_p kialakulási ideje	
$t_f = 30 \text{ sec (0,5 min)} \dots 720 \text{ sec (12 min)}$; a konstrukció függvényében	beton-, kőgátnál	Environment Agency [15]
5. a tározó kiürülési időtartama		Environment Agency [15]
$t_e = 2 \cdot V_w / Q_p$		Environment Agency [15]
Alvízi jelenségek		
1. az alvízi elöntés vízmélysége		
$h = [Q_p / \{(1,49/n) \cdot (B) \cdot \sqrt{(S)}\}]^{0,6}$		FERC [16]

Számítási jellemző	Megjegyzés	Szerzők
$h = [Qp / \{1,49 \cdot (B)^* \cdot \sqrt{(S)}\}]^{0,6};$ $1/n = 1,0$		
2. az árvíz áramlási középsebessége		
$u = (1/n)^* \sqrt{(S)^*} \cdot \sqrt{(B * d) / (B * 2 * d)}$ $u = \sqrt{(S)^*} \cdot \sqrt{(B * d) / (B * 2 * d)}; 1/n =$ $1,0$		FERC [16]
3. az árhullám sebessége		
$c = (5/3)^* u$; Kinematikus sebesség, $c > u$		FERC [16]
4. az alvizi adott pontjának árvízi elérési ideje		
$tt = X/c$		FERC [16]
5. árvízi életvesztés becslése		
$N = 0,5 * Npar$; $TA < 0,25$ h $N = (Npar)^{0,6}$; $0,25 < TA < 1,5$ h $N = 0,002 * Npar$; $TA > 1,5$ h $D = u * h$		Jonkman et al. [17]; RESCDAM [18], Reiter [19]

1.táblázat: A gátszakadás mennyiségileg meghatározható jellemzői különböző szerzők alapján (saját szerkesztés)

A táblázatban a különböző külföldi szerzők által megalkotott empirikus formulák szerepelnek. A számítások során alkalmazott jelölések a 2. táblázatban láthatók.

Változó	Mértékegység	Leírása
Bavg	m	A gátszakadás kifolyási szélessége. Itt ömlik ki a betározott anyag, folyadék
Ver	m ³	A kitört (errodált) és elsodort gátszakasz térfogata
Qp	m ³ /sec	A maximális- csúcs hozam, amely a szakadáson kiömlik
tf	sec	A szakadási folyamat kialakulási időtartama, amíg kialakul Qp
te	sec	A csúcs hozam utáni kiürülési (lecsengési) időtartam
Vw	m ³	A tározóban lévő folyadék térfogata
Hw	m	A tározó maximális gátmagassága
h	m	Az alvizi elöntés vízmélysége
B	m	Az alvizi elöntés „mederszélessége”
S	m/m	Az alvizi meder lejtése
u	m/s	Az árvíz áramlási középsebessége
n	sec/m ^{1/3}	Manning-féle érdességi tényező. Szakadásnál: $n \approx 0,1$; $1/n = 1,0$
c	m/m	Az árhullám kinematikus mozgási sebessége.

Változó	Mértékegység	Leírása
tt	óra	Az árhullám adott távolságú pontjának (X) elérési ideje
X	m	Távolság a gátszakadástól mérve
N	fő	Az árvíz okozta elhalálozások száma
N _{par}	fő	Az árvízzel szorosan érintett lakosok száma N _{par} <N _{település}
TA	óra	Az árvízi riasztás (az előrejelzés) ideje.
D	m ² /s	Árvízi kármutató (veszélymutató)

2.táblázat: A gátszakadás számításánál alkalmazott jelölések (saját szerkesztés)

Potenciális árvízi kármutató

A különböző szerzők nagyon sokféle árvíz-elöntési indikátort határoznak meg. Vizsgálataink során az adott csúcsesemény által okozott károk súlyosságának megítélése során a 3. táblázatban részletezett D potenciális árvízi kármutatót alkalmaztuk.

Érintettek	Potenciális árvízi kármutató [D= u*h (m ² /s)]		
	Alacsony	Közepes	Magas
Gyerekek	D<0,1	0,1<D<0,25	D>0,25
Felnőttek	D<0,3	0,3<D<0,7	D>0,7
Személygépkocsik	D<0,9	0,9<D<1,5	D>1,5
Könnyűszerkezetes épületek	D≤1,3	1,3<D<2,5	D>2,5
Szilárd építmények	D<3,0 (u>2,0 m/s)	3,0<D<7,0 (u>2,0 m/s)	D>7,0

3. táblázat: Potenciális árvízi kármutató[18],[19].

Kockázatértékelési mátrix

A bányászati hulladékkezelő létesítmények tározójának kockázatértékelését mátrix [20] segítségével végeztük el. A kockázatértékelési mátrix egy kvalitatív kockázatértékelési eszköz, melynek előnye, hogy a módszeres mérnöki munkát megfelelően támogatja.

Ennek érdekében a kockázatértékeléséhez egy olyan mátrixot (4. táblázat) alkalmaztunk, mely 1-től 5 –ig tartalmazza az esemény hatását jellemző súlyosság értékeket és szintén 1-től 5-ig tartalmazza a bekövetkezési valószínűséget jellemző értékeket.

Az elemzés során minden egyes súlyos, illetve kevésbé súlyos tározó balesetet kiváltó eseményhez hozzárendelhetünk egy súlyossági értéket (6. táblázat) és egy bekövetkezési valószínűség értéket (7. táblázat).

A mátrixban a kockázat értékét (nagyságrendjét) az aktuális súlyossági és bekövetkezési valószínűség értékek szorzata adja.

Például, ha egy súlyos hatással bíró esemény bekövetkezési gyakorisága valószínű, akkor a mátrix adott cellájának pontértéke 4×4 , azaz 16. A mátrix elemeinek pontértéke 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20 és 25 lehet. A kockázati mátrix cellái a kockázat elfogadhatóságát mutatják.

Csúcsesemény be- következési valószí- nőség értéke	Súlyosság érték				
	1	2	3	4	5
5	(5) EE*	(10) NK	(15) NK	(20) NE	(25) NE
4	(4) EE	(8) EE	(12) NK	(16) NE	(20) NE
3	(3) E	(6) EE	(9) EE	(12) NK	(15) NK
2	(2) E	(4) EE	(6) EE	(8) EE	(10) NK
1	(1) E	(2) E	(3) E	(4) EE	(5) EE

4. táblázat: Tározó kockázatértékelési mátrixa [20]

*Kockázat mértékének, illetve elfogadhatóságának jelölése a táblázatban:

E: Elfogadható (zöld szín); EE: elfogadható ellenőrzéssel (sárga szín); NK: nem kívánatos (narancssárga szín); NE: nem fogadható el (piros szín).

Az alábbi 4. táblázat a kockázatértékelési mátrix által kapott kockázat elfogadhatóságát ismerteti, amely alapján javaslatot ad intézkedésekre is.

Kockázat		Javasolt intézkedések
értéke	elfogadhatósága	
1-3	elfogadható (E)	Nincs szükség intézkedésre.
4-9	elfogadható ellenőrzéssel (EE)	Nincs szükség újabb intézkedésre a folyamatos ellenőrzés mellett.
10-15	nem kívánatos (NK)	Sürgős intézkedés kell a kockázat csökkentésére.
16-25	nem fogadható el (NE)	A kockázatot azonnal meg kell szüntetni.

5. táblázat: Kockázat elfogadhatósága és javasolt intézkedések [20]

Az 6. táblázatban részletesen ismertetjük az esetlegesen bekövetkező súlyos esemény hatását jellemző súlyosság értékeket, illetve az azokat meghatározó jellemzőket (pl. személyi sérülés, anyagi veszteség, stb.).

Súlyosság értéke	Súlyossági szint	Hatás jellemzése			
		Személyi sérülés	Anyagi veszteség (Ft)	Állási idő	Környezeti hatás
1	Jelentéktelen	Nincs sérülés/betegség	< 1 millió Ft	< 1 nap	Nincs környezeti kár
2	Alacsony	Kisebb sérülés/betegség	1 – 50 millió	1 nap – 1 hét	Kisebb, visszafordítható és/vagy helyreállítható környezeti kár (<1 hónap)
3	Mérsékelt	Közepes sérülés/betegség	50 -250 millió	1 hét – 1 hónap	Rövidtávú környezeti hatások (1 hónap-1év)
4	Súlyos	Súlyos sérülés/betegség	250 millió – 1 milliárd	1 hónap – 1 év	Középtávú környezeti hatások (1–5 év)
5	Nagyon súlyos	Elhalálozás	1 milliárd <	1 év <	Hosszútávú környezeti hatások (5 év <)

6. táblázat: Súlyossági értékek és jellemzőik (saját szerkesztés)

A csúcsesemények bekövetkezési valószínűség értékét, leírását mutatja az alábbi 7. táblázat.

Bekövetkezési valószínűségi érték	Csúcsesemény bekövetkezési valószínűségének leírása	Valószínűség számított értéke
5	Nagy valószínűséggel bekövetkezik.	>0,5; 0,5-1,0
4	Valószínű, hogy bekövetkezik.	0,1-0,5
3	Mérsékeltlen valószínű a bekövetkezés.	0,001-0,1
2	Nagyon kicsi az esélye a bekövetkezésnek.	0,0001-0,001

Bekövetkezési valószínűségi érték	Csúcsesemény bekövetkezési valószínűségének leírása	Valószínűség számított értéke
1	Valószínűtlen. Szinte biztos, hogy nem következik be.	<0,0001

7. táblázat: A tározó bekövetkezési valószínűség értékei és jellemzésük (saját szerkesztés)

VIZSGÁLATI EREDMÉNYEK

A vizsgált zagytározó bemutatása

A vizsgált fiktív zagytározó egy közepesen lakott településtől nem messze, 2 km-es távolságra (település széle, ahol már lakóépületek találhatóak) helyezkedik el kisvízfolyás völgyében. A tározóban iszapot helyeztek el. A tározó nem rendelkezik aljzatszigetelő rendszerrel.

A tározó alapadatai az alábbiak:

- A tározótó alsó szintje az aktuális (közel sík) terepszinten található, ez a 0,00 szint.
- A tározó geometriai méretei:
tározó alapterülete: 450 m x 450 m = 202 500 m², azaz 20, 25 ha a töltet és a víz magassága: 18,0 m (3,0 m víz és 15,0 m iszap)
- A tározó geotechnikai adatai:
a gát anyaga: pernye (beton)/salak
a gát talpszélessége: 50 m
a gát magassága: 22 m
a gát koronaszélesség: 10 m
a gáttest keresztmetszete: 660 m²
- Környezeti adatok:
az érintett lakosság száma: 1 500 fő (kistelepülés)
előre láthatólag közvetlen hatással érintettek száma: 200 fő

Hibafa elemzés eredményei

A hibafa elemzést több lépésben végeztük el. Az első lépésben meghatároztuk azokat a Csúcseseményeket, melyek bekövetkezte már önmagában súlyos balesetnek tekinthetők. Ezek az alábbiak lehetnek a zagytározó esetében:

- 1. csúcsesemény: „Felszín alatti közegbe jut a csurgalékvíz”,
- 2. csúcsesemény: „Gát alatt jön ki az iszap”,
- 3. csúcsesemény: „Gát kontúrszivárgás”,
- 4. csúcsesemény: „Zagy anyaga a gát tetején átbukik”,
- 5. csúcsesemény: „Gátsérülés (részleges vagy teljes tönkremenetel)”,
- 6. csúcsesemény: „Zagytározó felszínérő porterjedés a környezetbe”.

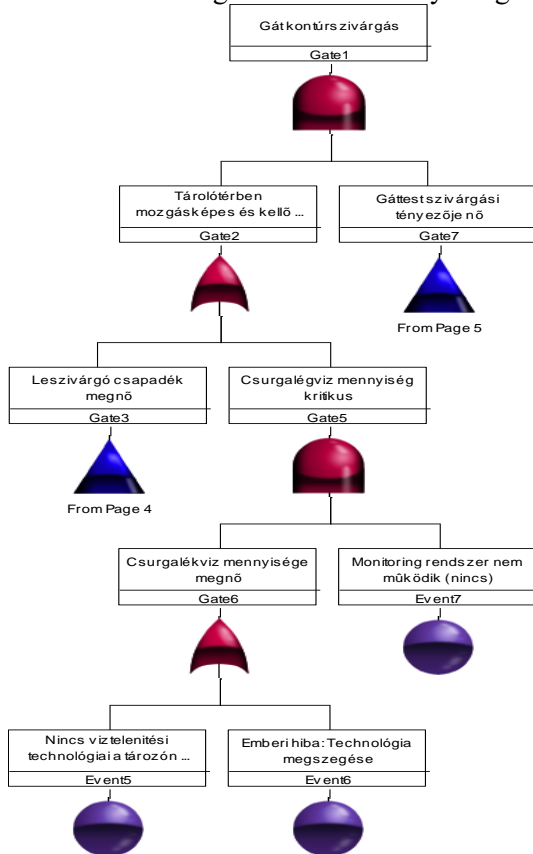
A vizsgált csúcsesemények esetében a hibafa elemzést Relax 7.7 programmal hajtottuk végre, meghatározva az adott csúcsesemény bekövetkezési valószínűségét.

Az alábbiakban részletesen bemutatjuk a „Gát kontúrszivárgás” csúcsesemény hibafa-elemzését. A hibafa elemzést valamennyi csúcsesemény estében elvégeztük.

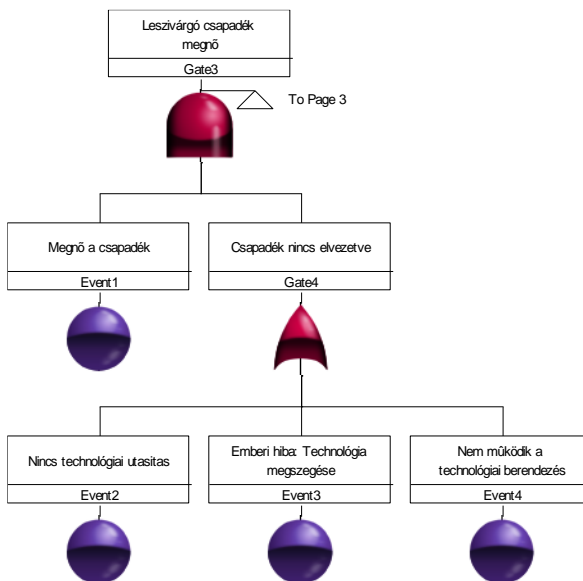
A „Gát kontúrszivárgás” csúcsesemény esetében a tározóteret körülvevő gáttest anyagán keresztül lép ki a tározóterben lévő folyékony vagy ahhoz hasonló tulajdonságú anyag. Az anyagkilépés a gáttesten keresztül a következő jelenségek hatására következik be:

- a tározóterben víz (csapadék- és konszolidációs víz) halmozódik fel;
- a tározóterben lévő folyadéktest nyomása megnő;
- külső dinamikus hatás (szél vagy földrengés) lép fel.

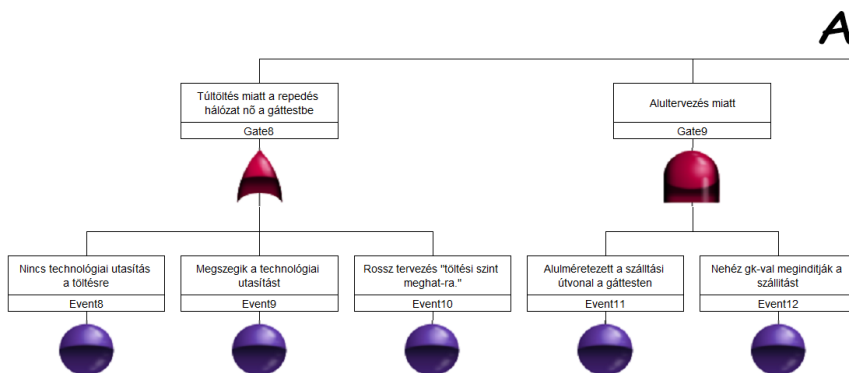
A hibafa-elemzés (1. -3. ábra) során meghatározásra került az összes olyan közbülső és alapesemény, amelyek önálló vagy együttes bekövetkezése „Gát kontúrszivárgás” csúcsesemény bekövetkezéséhez vezet. Az elemzés által egyértelművé vált, hogy az átszivárgást kiváltó jelenségek elsődlegesen emberi (tervezési-kivitelezési vagy technológia megszegési) hibára, valamint a technológiai előírások hiányosságára vezethetők vissza.



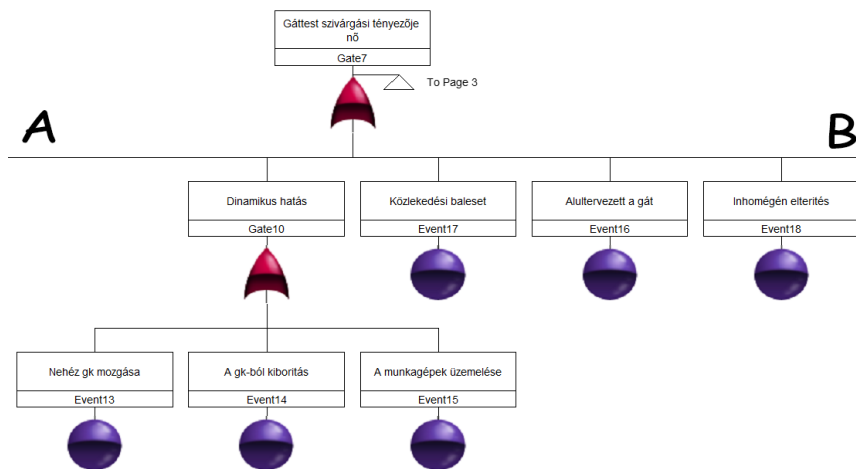
1.ábra: Hibafa elemzés „Gát kontúrszivárgás” csúcsesemény esetén, első rész (saját szerkesztés)



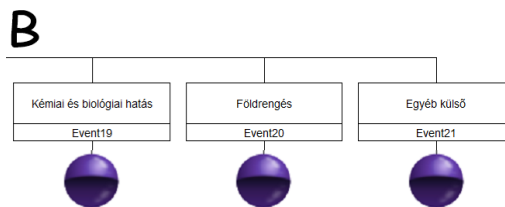
2.ábra: Hibafa elemzés „Gát kontúrszivárgás” csúcsesemény esetén, második rész (saját szerkesztés)



3.ábra: Hibafa elemzés „Gát kontúrszivárgás” csúcsesemény esetén, harmadik rész első rész (saját szerkesztés)



4.ábra: Hibafa elemzés „Gát kontúrszivárgás” csúcsesemény esetén, harmadik rész második része (saját szerkesztés)



5.ábra: Hibafa elemzés „Gát kontúrszivárgás” csúcsesemény esetén, harmadik rész harmadik része (saját szerkesztés)

A hibafa elemzés eredményeként a „Gát kontúrszivárgás” csúcsesemény bekövetkezési valószínűsége 0,19 értéknek adódott, azaz a valószínű kategóriába tartozott.

Elemzésünk rávilágított arra, hogy a „Gát kontúrszivárgás” csúcsesemény elsősorban a pontos technológiai utasítások (Event3) be nem tartása, illetve a tervezési szakaszban különböző típusú terhelésekre alulméretezett gát tervezésére (Event1, Event2, Event11, Event16, Event18) vezethető vissza.

A hibafa elemzés eredményeként a „Gátsérülés (tönkremenetel)” csúcsesemény bekövetkezési valószínűsége 0,0063 értéknek adódott, tehát a mérsékelt valószínű kategóriába tartozott.

A gátsérülésből adódó árvízi következmények

A „Gátsérülés” csúcsesemény bekövetkezése esetén az 1. táblázat alapján elvégzett számításaink alapján elmondható, hogy a 2 km-re lévő települést az árvíz 1,32 óra alatt éri el. Az árvízi életvesztés becslült száma: maximum 24 fő. A potenciális árvízi kármutató (D) értéke 0,625 m²/s adódott számításaink eredményeként. A 3. táblázat alapján az árvízi elöntés által okozott károk minősítése: gépkocsikra, építményekre alacsony, felnőttekre közepes, míg a gyerekekre magas.

A „Gát kontúrszivárgás” csúcsesemény esetén nem kell számolni árvízi következményekkel. Elhalálozás nem várható, anyagi kár alacsony, leállási idő rövid, valamint környezeti károkozás még nincs.

Megállapítható az is, hogy a szimulációs modellezéshez képest ez az egyszerű számítási módszer viszonylag gyors, megfelelő pontosságú és költségkímélő megoldást adhat egy tározó katasztrófavédelmi szempontú biztonságossági elemzéséhez. Fontos szerepet tölthet be az balesetet megelőző intézkedések rendkívül gyors meghozatalában, illetve a polgári védelmi feladatok megszervezésben.

Kockázat megadása kockázatértékelési mátrix alapján

A kockázatértékelés mátrix alapján a tározó kockázatát az alábbiakban adhatjuk meg:

A „Gát kontúrszivárgás” csúcsesemény tekintetében a tározó kockázata elfogadható ellenőrzéssel (EE), mivel a súlyossági érték: 2 (elhalálozás nem várható, anyagi kár alacsony, leállási idő rövid, környezeti károkozás még nincs) és a bekövetkezési valószínűség értéke: 4 (bekövetkezési valószínűség számított értéke: 0,19, tehát valószínű az esemény bekövetkezése). Tehát ebben az esetben nincs szükség újabb intézkedésre (5. táblázat) a folyamatos ellenőrzés betartása mellett.

A „Gátsérülés” csúcsesemény vonatkozásában a tározó kockázata nem kívánatos (NK), mivel a súlyossági érték: 5 (elhalálozás maximálisan 24 fő, ha 54 m hosszon átszakad a gát) és a bekövetkezési valószínűség értéke: 3 (bekövetkezési valószínűség számított értéke: 0,0063, tehát mérsékelten valószínű az esemény bekövetkezése). Az 5. táblázat értelmében sürgős intézkedés javasolt a kockázat csökkentésére.

A konzervatív megközelítés elvét alkalmazva, a tározó kockázatát adja a „Gátsérülés” csúcsesemény mint legsúlyosabb baleset, mivel ehhez kapcsolódik a legtragikusabb következmény (maximálisan 24 fő elhalálozása), így a tározó kockázata összességében egyértelműen a nem kívánatos (NK) kategóriába sorolható.

KÖVETKEZETÉSEK, JAVASLATOK

A zagytározó kockázatelemzésének eredménye alapján elmondható, hogy a kockázatsökkentésre szükség van, mely alapvetően két területre összpontosítva lehetséges:

- az események bekövetkezési valószínűségének csökkentésével,
- illetve a következmények súlyosságának mérséklésével.

A „Gát kontúrszivárgás” és a „Gátsérülés” csúcseseményeket, mint lehetséges tározó baleseteket figyelembe véve az alábbi kockázatsökkentő megoldások bevezetését javasoljuk.

A csúcsesemények bekövetkezési valószínűsége csökkenthető rendszeres ellenőrzések bevezetésével, amelyek egyrészt a töltet lerakására (a technológiai utasításban foglaltak ne kerüljenek megszegésre), másrészt a csapadékvíz elvezetésére vonatkoznak (műszaki és humán feltételrendszer folyamatos ellenőrzése). Harmadrészt célirányosan a gátszerkezeti változások, illetve az azokat előidéző okok - vizsgálatára (pl. rezgésellenőrzés, geodéziai ellenőrzés, vízszivárgások mértékének ellenőrzése, inklinométeres mérések végrehajtása, stb.) terjednek ki.

Ezek a különböző kockázatsökkentő intézkedések nem csak a zagytározók, hanem katasztrófavédelmi szempontból kiemelt fontosságú egyéb épületek és létesítmények esetében is igen nagy jelentőséggel bírnak [21], [22].

ÖSSZEFOGLALÁS

Tanulmányunkban egy olyan kockázatelemzési módszert mutattunk be, mely gyors és hatékony segítséget nyújthat a bányászati hulladékkezelő létesítmények tározóinak katasztrófavédelmi szempontú értékeléséhez, a kockázat meghatározáshoz, illetve a külső és belső védekezés megtervezéséhez egy potenciálisan bekövetkező baleset esetén.

Az általunk alkalmazott kockázatelemzési módszer során számításokat, vizsgálatokat végeztük el, mely során:

- Azonosítottuk azokat az ún. csúcseseményeket (főeseményeket), amelyek bekövetkezése súlyos balesetet válthat ki.
- Hibafa-elemzéssel feltártuk az egyes csúcsesemények kialakulásához vezető okokat, közbülső és alapeseményeket, majd meghatároztuk a csúcsesemény bekövetkezési valószínűségét (gyakoriságát).
- Elvégeztük az árvízi következmény számítást, meghatároztuk a potenciális árvízi kármutató értékét.
- Értékeljük az egyes csúcsesemények kockázatát kockázatértékelési mátrix segítségével. A konzervatív megközelítés elvét szem előtt tartva meghatároztuk a zagytározó kockázatát környezetére nézve.

Ezt követően olyan kockázatsökkentő javaslatokat fogalmaztunk meg, mely által csökkenthető a veszély, amelyet a tározó jelent mesterséges és természetes környezetére.

FELHASZNÁLT IRODALOM

- [1] R. Liu, J. Liu, Z. Zhang, A. Borthwick, K. Zhang *Accidental water pollution risk analysis of mine tailings ponds in Guanting reservoir Watershed, Zhangjiakou city, China* Int. J. Environ. Res. Public Health, 2015, pp. 15269-15284.
- [2] L.N. Bowker, D.M. Chambers. *The risk, public liability, and economics of tailings storage facility failures*. The Public Interest: Stonington, Maine, Bowker Associates Science and Research, 2015. Available at: <https://files.dnr.state.mn.us/input/environmentalreview/polymet/request/exhibit3.pdf>, Accessed: 18th May 2023.
- [3] World Information Service on Energy, *WISE-Uranium Project, Chronology of Major Tailings Dam Failures.*, 2019. Available: <https://www.wise-uranium.org/mdaf.html>, Accessed: 4th May 2023.
- [4] Martin, T.E., Davies, M.P., *Trends in the stewardship of tailings dams*. In: Proceedings of Tailings and Mine Waste'00, Fort Collins, January, Balkema Publishers, 2000, pp. 393–407.
- [5] 2006/21/EK irányelv (bányászati hulladék irányelv)
- [6] Stanley, G., Jordán, Gy., Hámor T., Sponar M. *Útmutató a „Bezárt bányászati hulladékkezelő létesítmények felmérésének kockázat alapú előminősítési rendszeréhez a 2006/21/EK Irányelv 20-as cikke alapján*, Kézirat, 2011. MBFH Adattár
- [7] 13/2022. (I. 28.) SZTFH rendelet a bányászati hulladékok kezeléséről
- [8] Kiss, J., Jordán, Gy. (szerk.), *Bezárt bányászati hulladékkezelő létesítmények nyilvántartása és kockázati besorolása*. Magyar Bányászati és Földtani Szolgálat, 2020. Elérhető: https://mbfsz.gov.hu/sites/default/files/file/2020/03/03/mwf2012_1.pdf, Letöltve: 2023. május 12.

- [9] Xi-bing, L., Wei-dong, J. and Fu-jun, Z., *Fault tree analysis of tailings dam break during flood season. Journal of Safety and Environment.* 2001, 1 (5) pp. 45-48.
- [10] Shu Yongbao, Li Zhongxue. *Fault tree analysis of tailings dam break. Journal of Safety and Environment.* Gold, 2010, 31 (6). pp. 54-56.
- [11] Hartford, D. and Baecher, G. B. *Risk and uncertainty in dam safety.* Thomas Telford Ltd., London. 2004.
- [12] U. S. Bureau of Reclamation. *Downstream hazard classification guidelines.* ACER technical memorandum No. 11. Assistant commissioner - engineering and research. Denver, Colorado. 1988.
- [13] MacDonald, T.C. and Langridge- Monopolis, J. *Breaching Characteristics of Dam Failures.* Journal of Hydraulic Engineering, 1984, Vol. 110, No. 5., p. 567-586.
- [14] Froehlich, D. C. *Embankment Dam Breach Parameters Revisited.* Water Resources Engineering, Proceedings of the 1995 ASCE Conference on Water Resources Engineering, San Antonio, Texas, August 14-18, 1995, pp. 887-891.
- [15] Environment Agency. *Reservoir Flood Maps (RFM) Guide.* Explanatory Note on Reservoir Flood Maps for Local Resilience Forums – Version 3 – November 2014.
- [16] FERC (*Federal Energy Regulatory Commission*) Engineering Guidelines for the Evaluation of Hydropower Projects, Chapter 2. *Selecting and Accommodating Inflow Design Floods for Dams.* Federal Energy Regulatory Commission. 1993.
- [17] Jonkman, S. N., Vrijling, J. K. and Vrouwenvelder, A. *Methods for the estimation of loss of life due to floods: a literature review and a proposal for a new method.* Natural Hazards, 2008. 46. pp. 353–389.
- [18] RESCDAM. *The Use of Physical Models in Dam-Break Flood Analysis: Rescue Actions Based on Dam-Break Flood Analysis;* Final Report of Helsinki University of Technology; Helsinki University of Technology: Helsinki, Finland, 2000.
- [19] Reiter, P. *International methods of risk analysis, Damage evaluation and social impact studies concerning Dam-break accidents.* EU-Project RESCDAM. PR Water Consulting Helsinki. 2000.
- [20] Elek, B. és Kovács, G.: *Ipari tározók a katasztrófavédelmi szempontú vizsgálata.* In: Restás Ágoston, Urbán Anett (szerk.) Tűzoltó Szakmai nap, Budapest. BM OKF kiadvány, 2016. pp. 82-92.
- [21] Ambrusz, J. és Érces, G. *Természeti csapásoknak ellenálló épületek.* In: Bodnár, László; Heizler, György (szerk.) Konferenciakiadvány: Természeti Katasztrófák Csökkentésének Világnapja Nemzetközi Tudományos Konferencia. Budapest, Magyarország: Rádiós Segélyhívó és Infokommunikációs Országos Egyesület, 2021. 369 p. pp. 208-214.
- [22] Komlai, K., Restás, Á., Kerekes, Zs. *Fire resistance thermodynamic test of self-supporting double skin metal faced sandwich panels.* In: Bodnár, László; Heizler, György (szerk.) Book of abstracts : Fire Engineering & Disaster Management Prerecorded International Scientific Conference. Budapest, Magyarország, Nemzeti Közszolgálati Egyetem, 2021. 119 p. pp. 44-45.

**FIRE SAFETY ISSUES OF
THERMOFORMING TECHNOLOGY****MELEGALAKÍTÁSI TECHNOLÓGIA
TŰZBIZTONSÁGI KÉRDÉSEI**HORVÁTH-KÁLMÁN Eszter¹ –ELEK Barbara²– KOVÁCS-SZELECZKI Xénia³**Abstract**

Thermoforming technologies are gaining more and more space in the automotive industry. The materials to be processed are usually heated to 850-950 °C in the process and then cooled during pressing. The leakage of the hydraulic oil of the press, which is an integral part of the technology, is a common phenomenon, which can increase the probability of a fire occurring in a given plant. In our study we investigate in a laboratory test whether the flammability of the press machine's hydraulic oil is affected by changes in the quality of the oil. After that, we analyze the consequences of oil ignition in a fictitious plant only partially equipped with fire protection equipment, and the spread of fire and smoke. We will then propose a technical solution to reduce the risk of fire at plant, primarily keeping in mind the aspects of life protection, supplemented by compliance with property protection requirements.

Keywords

thermoforming technology, hydraulic oil, press machine, fire safety, spread of fire and smoke

Absztrakt

Az autóiparban egyre nagyobb teret nyernek a melegalakítási technológiák. A megmunkálandó anyagokat általában 850-950 °C-ra hevítik az eljárásban, majd préselés közben hűtik. A technológia szerves részét képező présgép hidraulika olajának elfolyása gyakori jelenség, mely növelheti tűz kialakulásának valószínűségét adott üzemben. Tanulmányunkban laborvizsgálat során vizsgáljuk, hogy a présgép hidraulikai olajának éghetőségét befolyásolják-e az olaj minőségében bekövetkező változások. Ezt követően elemezzük tűzvédelmi berendezésekkel csak részben ellátott fiktív üzemben az olaj meggyulladásának következményeit, a tűz- és füstterjedést. Majd műszaki megoldási javaslatokat teszünk az üzemi tűzkockázat csökkentésére elsődlegesen az életvédelmi szempontokat szem előtt tartva, kiegészítve a vagyónvédelmi elvárásoknak való megfeleléssel.

Kulcsszavak

melegalakítási technológia, hidraulika olaj, présgép, tűzbiztonság, tűz- és füstterjedés

¹ kalman.eszter@ybl.uni-obuda.hu | ORCID: 0009-0003-5199-3751 | PhD, associate professor, Department of Infrastructure Development, Ybl Miklós Faculty of Architecture and Civil Engineering, University of Óbuda | PhD, egyetemicens, Infrastruktúra-fejlesztési és üzemeltetési tanszék, Ybl Miklós Építéstudományi Kar, Óbudai Egyetem

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

³ xeniaszeleccki@googlemail.com | ORCID:0009-0005-2177-3568 | EHS manager, ESAB-Mór Kft. | EHS vezető, ESAB-Mór Kft.

BEVEZETÉS

A fosszilis energiahordozók kimerülése, valamint a környezeti emissziók csökkentése miatt az elmúlt években erőteljes optimalizálási folyamat indult el a gépjárművek üzemanyag-hatékonysága terén. Ennek érdekében az autóiipari fejlesztések az ütközésbiztonság növelésével párhuzamosan a járművek tömegének csökkentését helyezték előtérbe. A tömegcsökkentés egyik módja könnyebb anyagok, mint például magnézium ötvözetek, alumíniumötvözetek, illetve korszerű nagy szilárdságú acélok (AHSS) alkalmazása a járművek karosszéria gyártásában. A melegalakítási eljárásokat speciális gyártási technológiaként fejlesztették ki a nagyszilárdságú acél alkatrészek előállítására, amely révén a hagyományos hidegalakítási technológiáknál tapasztalt hiányosságok kiküszöbölhetővé váltak. A technológia szerves részét képező présgép hidraulika olajának elfolyása gyakori jelenség, mely növelheti tűz kialakulásának valószínűségét adott üzemben. Tanulmányunkban vizsgáljuk, hogy milyen körülmények alakulhatnak a tűzvédelmi szempontból egy autóiipari gyártó üzemben a présgépből szivárgó hidraulikai olaj meggyulladására. Keresünk a választ arra, hogy a hidraulikai olaj minőségében bekövetkező változás gyakorol-e hatást a tűzkockázatra.

SZAKIRODALMI ÁTTEKINTÉS

Az autóiipari fejlesztések során kimagaslóan nagy szerepet tölt be a járművek tömegének csökkentése, mivel 10%-os tömegcsökkentés csaknem 2,5%-os üzemanyag fogyasztás csökkenéshez vezet [1]. A tömegcsökkentést teszi lehetővé korszerű nagyszilárdságú acélok alkalmazása az autóiiparban. Ennek egyik figyelemreméltó korai példája a 2014-es Volvo XC90, ahol a karosszéria körülbelül 38 %-a melegen préselt nagyszilárdságú acéllemezéből készült. Egy másik példa a 2014-es Honda MDX, amelyben szintén melegen préselt nagyszilárdágú acélt használtak az A és B oszlopok, továbbá a tető- és küszöberősítések gyártásánál [2].

Az autóiipari gyártói és üzemeltetői tapasztalatok alapján hidraulika olaj elfolyás mutatkozhat a hidraulikus présgépeknél a melegalakítás során. A szivárgó olaj gyújtóforrással (pl. közel 900 °C -os fémmel) érintkezve tüzet okozhat [3].

Az autóiiparban egy tüzeset igen komoly anyagi veszteséggel járhat. A berendezésekben, építményekben bekövetkezett károk, valamint magas helyreállítási költségek mellett a tűzkárok értékének sokszorosát kitevő termelés kieséssel is számolni kell.

A melegalakítási technológiát alkalmazó üzemeknél a tűz bekövetkezésének és szétterjedésének valószínűségét, valamint az esetlegesen bekövetkező tűz által okozott károk mértékét jelentősen mérsékelheti beépített tűzjelző- és oltóberendezés alkalmazása.

A tűz kifejlődésének korai szakaszában akkor lehet megbízható jelzést generálni, ha a tűzjelzők kiválasztásakor és elhelyezésekor a védett terület környezeti feltételeit (pl. rezgésterhelés, porszennyezés) és a technológiai sajátosságokat messzemenőig figyelembe veszik [4]. A technológiai sajátosságok tűzvédelmi szempontú mérlegelése tervezői kompetencia, amihez a technológia igen alapos ismerete is szükséges [5].

Fentiekén túl a tűz keletkezésének megelőzésében fontos szerepet tölthet be a normál, mérsékelt tűzveszélyes hidraulikai olajok helyett tűzálló (HF típusú) hidraulika olajok alkalmazása a présgépekben.

Mivel tűzvédelmi szempontból az autóiipari technológiák egyik kritikus pontja a szivárgó hidraulika olaj meggyulladása, így számos cég kezdett bele tűzálló hidraulika olaj kifejlesztésébe.

A Quaker Houghton amerikai cég kísérletet végzett 2019-ben különböző hidraulika olajok 900 °C-os fémmel való érintkezésekor létrejövő égési jelenségének feltárására. Mérsékeltén tűzveszélyes olajként HLP-46 típusú olajat, míg tűzálló olajként saját fejlesztésű HF típusú, QUINTOLUBRIC® 888-46 megnevezésű olajat alkalmaztak a kísérletek során [6]. A kísérleti eredményeket az alábbi 1. és 2. képek mutatják.

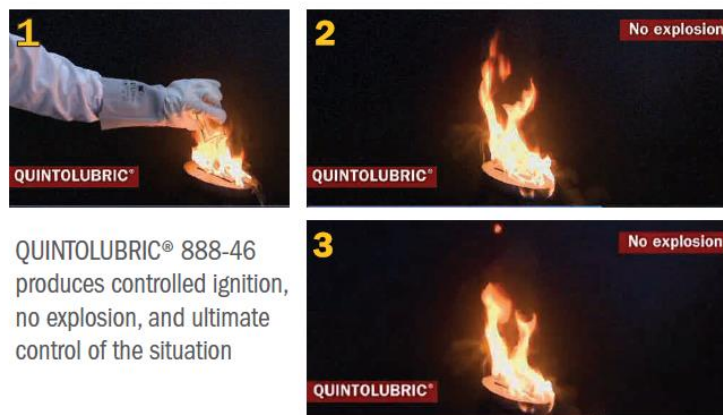
20 ML OF MINERAL OIL (HLP-46) POURED ON A 900°C PANEL



Mineral oil forms vapours which results in explosive ignition

1.kép: Mérsékeltén tűzveszélyes (HLP-46 típusú) hidraulika olaj égése [6]

20 ML OF QUINTOLUBRIC® 888-46 POURED ON A 900°C PANEL



QUINTOLUBRIC® 888-46 produces controlled ignition, no explosion, and ultimate control of the situation

2.kép: Tűzálló (QUINTOLUBRIC® 888-46 megnevezésű) hidraulika olaj égése [6]

Jól látható, hogy a tűzálló (HF típusú, QUINTOLUBRIC® 888-46 megnevezésű) hidraulika olaj esetében is bekövetkezett ugyan a lánggal égés, de a láng kisebb kiterjedésű és kontrolláltabb volt, mint a HLP-46 típusú olaj esetében. A kísérlet felhívta a figyelmet arra, hogy milyen jelentőséggel bírhat a szivárgó hidraulika olaj tűzállósága a tűzmegeelőzésben.

Még manapság is számos autóiipari üzemben mérsékeltén tűzveszélyes hidraulikai olajat alkalmaznak a présgépeknél. Vizsgáltuk, hogy az olaj éghetőségét befolyásolja-e az olaj minőségében esetlegesen bekövetkező változás. Ezt követően elemeztük beépített tűzjelző berendezéssel és hő-és üstelvezetéssel ellátott fiktív üzemben az olaj meggyulladásának következményeit, a tűz és füst szétterjedését adott tűzszakaszban. Ezt követően műszaki megoldási javaslatokat tettünk az üzemi tűzkockázat csökkentésére.

VIZSGÁLATI ANYAG ÉS MÓDSZERTAN

Hidraulika olajok vizsgálata

A hidraulikus présgépeknél alkalmazott mérsékeltén tűzveszélyes hidraulika olajok esetében arra kerestük a választ, hogy használatukkor mi az, ami növelheti a tűz létrejöttének valószínűségét. A vizsgálatainkhoz az alábbi 4 féle hidraulika olaj mintát készítettünk elő (3. kép):

- hidraulika olaj minta: MaxLube HLP-46 használt olaj (sötét színű),
- hidraulika olaj minta: MaxLube HLP-46 használt olaj (vizes, zavaros, tejkaramell színű),
- hidraulika olaj minta: Maxlube HLP-46 (tisztá, új),
- hidraulika olaj minta: Madit OH -HM-46 (tisztá, új).



3. kép: A vizsgálat során vizsgált 4 féle hidraulika olaj (balról jobbra: 1. minta, 2. minta, 3. minta, 4. minta)

A lobbanás- és gyulladáspont mérést három ismétlésben végeztük el mind a 4 féle hidraulika olaj minta esetében.

Hidraulika olajok lobbanáspontjának és gyulladáspontjának meghatározása

A vizsgált hidraulika olajok lobbanáspontjának meghatározását az MSZ EN ISO 2592:2002 szabvány [7] előírásai szerint Cleveland CLA 2 típusú automata nyílttéri lobbanáspont mérő készülékkel (4.kép) hajtottuk végre, mely hidraulika olajok esetében alkalmas gyulladáspont meghatározásra is.

A vizsgálat menete a következő volt:

A tiszta és száraz réz tégelybe a vizsgálati mintát óvatosan a jelölésig töltöttük. Ügyelve arra, hogy a minta ne fröccsenjen, ne legyen buborékos, a tégely fala a töltési szint fölött ne legyen nedves és a kondenzátor ne érjen a falhoz.

A megtöltött tégelyt óvatosan légfürdőbe helyeztük, ezt követően megkezdtük a tégely fűtését. Az elektromos fűtés szabályzó kapcsolóját úgy állítottuk be, hogy a fűtés se-

bessége 5-6 °C/perc legyen. A várható lobbanáspont alatt kb. 30-35 °C-kal a fűtés sebességét csökkentettük úgy, hogy a minta hőmérsékletének emelkedése 1-2 °C/perc legyen. Ekkor 1 °C-onként a gyújtólángot átvezettük a tégely fölött és megfigyeltük az olaj felszínén végbemenő jelenséget. Amikor az olaj teljes felszínére kiterjedő lobbanást észleltünk és az 5 másodpercen belül megszűnt, feljegyeztük a hőmérsékletet. Ezt követően a melegítést tovább folytattuk. A gyújtólángot minden 1 °C hőmérséklet emelkedésnél kb. 1 másodperc alatt átvezettük a minta fölött. Feljegyeztük azt a legalacsonyabb hőmérsékletet, amelyenél az olaj belobbanása után annak gőzei legalább 5 másodpercig folyamatosan égtek. Ez volt a minta gyulladási hőmérséklete, azaz gyulladáspontja.



4. kép: Lobbanáspont mérés CLA 2 típusú készülékkel (saját kép)

Tűzszimuláció

Tűzszimulációs vizsgálatot végeztünk annak érdekében, hogy a fiktív melegalakító technológiájú üzem esetén megállapíthassuk, hogy adottak-e a feltételek az üzem biztonságos kiürítéséhez, valamint a tűzoltói beavatkozáshoz.

A fiktív üzem jellemzése tűzvédelmi szempontból

A szimuláció tárgyát képező fiktív üzem csarnokszerkezetű, mely 500 MJ/m² tűzterhelés alatt méretezett védelem nélküli acélszerkezet, fémlemez vértetű szendvicspanel borítással. Az üzemben talajszint alatt létesült helység nincs. A tető magas hullámú trapézlemez. Fedésére ásványgyapot hőszigetelést és vízszigetelést építettek be. A csarnoktérben beton padozat található. A csarnok egy tűzszakaszt képez, melybe hő- és füstelvezető kupolák kerültek beépítésre. A létesítmény ipari rendeltetésű, ahol fém autóipari termékek gyártása és átmeneti tárolása történik. A csarnokban tűzjelző rendszer működik és kézi jelzésadó működteti a hő- és füstelvezető rendszert. A füstszakaszolásnál figyelembe vették az épület tartószerkezeti rendszerét. A légutánpótlást a megfelelő méretű, szabadba nyíló, tűzjelző által is vezérelt szekcionált kapuk biztosítják.

Modell adatok

A modell felépítéséhez a Pyrosim programot használtuk, mely az FDS (Fire Dynamics Simulator) grafikus tervezői felülete [8]. Az így elkészített modellt kiexportáltuk az FDS számára felhasználható formátumba, majd az FDS programmal lefuttattuk.

A Pyrosim programban 0,4 méteres cellaméret került betáplálásra az alábbi 1. és 2. táblázatban ismertetett mérethálóban. A méretezésnél a jobb modellezhetőség érdekében a teret két részre osztottuk.

min X [m]:	-2,0	min Y [m]:	-4,0	min Z [m]:	0,0
max X [m]:	48,0	max Y [m]:	56,0	max Z [m]:	14,4
cellák száma X:	125	cellák száma Y:	150	cellák száma Z:	36
cella méret X [m]:	1,0	cella méret Y [m]:	1,0	cella méret Z [m]:	1,0

1. táblázat: Üzemcsarnok egyik felének méretezése (saját szerkesztés)

min X [m]:	-248,0	min Y [m]:	-4,0	min Z [m]:	0,0
max X [m]:	98,0	max Y [m]:	56,0	max Z [m]:	14,4
cellák száma X:	125	cellák száma Y:	150	cellák száma Z:	36
cella méret X [m]:	1,0	cella méret Y [m]:	1,0	cella méret Z [m]:	1,0

2. táblázat: Üzemcsarnok másik felének méretezése (saját szerkesztés)

A szimuláció modellterét úgy határoztuk meg, hogy az a tűz- és füstterjedés szempontjából vizsgált teret és annak a környezetét is tartalmazza olyan módon, hogy a modellter határoló felületei a tűzfejlődést csak elhanyagolható mértékben befolyásolják.

A modellezés során a tűzhelyszín esetén két különböző (500 kW és 5 MW) tűz hőteljesítményt vettünk fel Y. J. Ko [9] és B. Truchot et al. [10] vizsgálati alapján, majd elvégeztük a szimulációt.

A tűzhelyszín esetében a tűz alapterületét 4 m x 2 m=8 m²-ben adtuk meg, mely a modellben (1. ábra) a pirossal jelölt terület.

A tűzhelyszín esetén 500 kW tűz hőteljesítményt feltételezve az alábbi jellemzőkkel végeztünk modellezést. A felhasznált reakcióegyenlet: heptán.

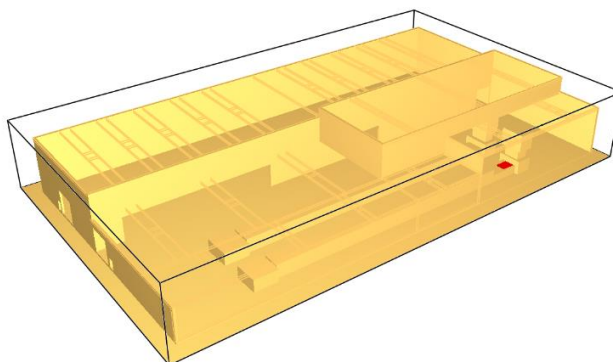
Modellezés során figyelembe vett adatok:

- Az épületben oltórendszer nem került kialakításra.
- Az épületben tűzjelző rendszer (pontoszerű füstérzékelőkkel) került kialakításra teljes lefedettséggel.
- A tűzjelző rendszer vezérli a légpótló, hő és füstelvezető rendszereket.

A tűzhelyszín esetén 5 MW tűz hőteljesítményt feltételezve az alábbi jellemzőkkel végeztünk modellezést. A felhasznált reakcióegyenlet: heptán.

Modellezés során figyelembe vett adatok:

- Az épületben oltórendszer nem került kialakításra.
- Az épületben tűzjelző rendszer (pontoszerű füstérzékelőkkel) került kialakításra teljes lefedettséggel.
- A tűzjelző rendszer vezérli a légpótló, hő és füstelvezető rendszereket.



1. ábra: Tűz feltételezett keletkezési helye (saját szerkesztés)

A szimulációban szereplő, feltételezett tűzhelyszínen fémek, nem éghető padozat, valamint nem jelentős mennyiségű kábelvezeték található. Emiatt a szimulációban a hidraulika olaj elfolyását és meggyulladását tócsatűzként értelmeztük. A szimulációba beillesztettük a lényegesebb méretű technológia eszközöket, illetve a hő és füstelvezető felületeket, melyek kézi jelzésadóra nyíltak.

A szimulációhoz kiválasztott folyadék anyagjellemzői

Az anyagtulajdonságok a lángterjedés modellezéséhez nélkülözhetetlenek. Ehhez meg kellett adni bemeneti adatként az anyagok gyulladási hőmérsékletét, hővezető képességét, fajhőjét, sűrűségét, a HRRPUA (heat release rate per unit) számértékét.

A tűzszimuláció során a Pyrosim adatbázisában fellelhető heptán tűzzel számoltunk, mivel az adott hidraulika olajok pontos összetétele, fizikai-kémiai jellemzői nem álltak rendelkezésünkre. Mivel a heptán égése kissé gyorsabb, mint a hidraulikai olajoké, így ez a biztonság javára történő eltérést jelentett a modellezésnél.

VIZSGÁLATI EREDMÉNYEK

Hidraulika olajminták lobbanás- és gyulladáspontja

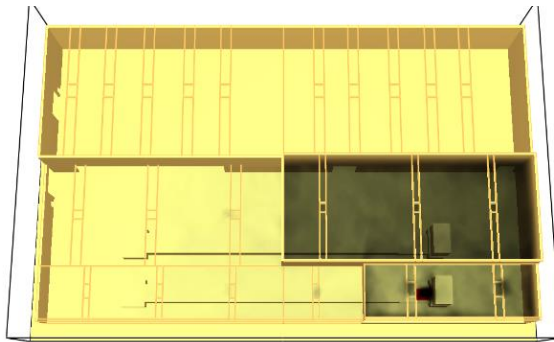
A 3. táblázatból kitűnik, hogy a 2. hidraulika olaj minta esetén meglepően alacsony lobbanás- és gyulladáspontot mértünk mindhárom mérés során. Ezt vélhetően az olaj egyéb anyaggal való szennyezettsége okozta, mely szabad szemmel is jól látható volt, mint ahogy azt a 3. képen láthatjuk. Ez mutatja azt, hogy a présgép üzemelése folyamán esetlegesen szennyeződő hidraulika olaj lobbanáspontja és gyulladáspontja csökkenthet idővel. Ez pedig kiváló oka lehet a tűz keletkezésének.

Hidraulika olajok	I. mérés		II. mérés		III. mérés	
	Lobbanáspont	Gyulladáspont	Lobbanáspont	Gyulladáspont	Lobbanáspont	Gyulladáspont
1. olaj	230 °C	256 °C	236 °C	258 °C	234 °C	256 °C
2. olaj	115 °C	124 °C	116 °C	124 °C	118 °C	126 °C
3. olaj	238 °C	268 °C	234 °C	260 °C	236 °C	262 °C
4. olaj	230 °C	256 °C	227 °C	245 °C	226 °C	248 °C

3. táblázat: különböző hidraulika olajok lobbanás- és gyulladáspontja (saját szerkesztés)

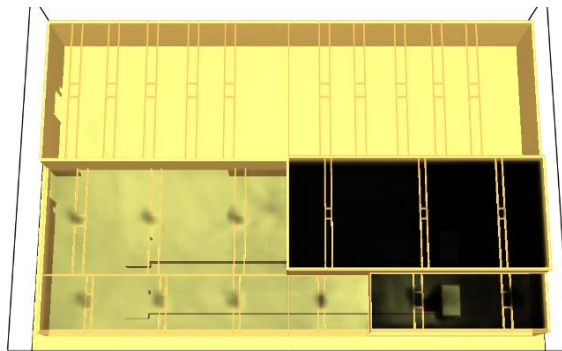
Tűszimulációs eredmények

A szimuláció alapján a füstterjedés a következőképpen alakult 5 MW-os tűz esetén 300 s és 600 s elteltével:



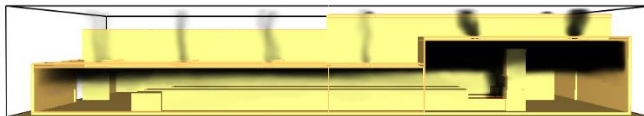
Time: 300.0

2. ábra: 5 MW-os tűz esetén füstterjedés 300s-nál felülnézetből (saját szerkesztés)



Time: 600.0

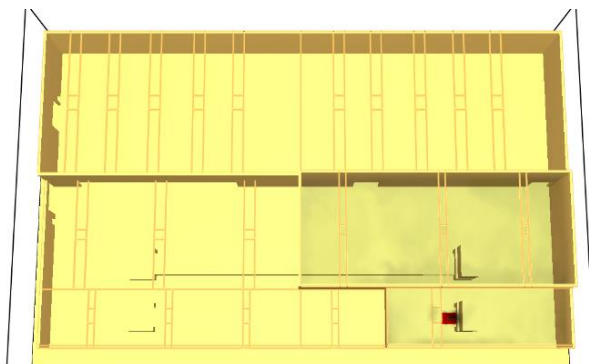
3. ábra: 5 MW-os tűz esetén füstterjedés 600s-nál felülnézetből (saját szerkesztés)



Time: 600.0

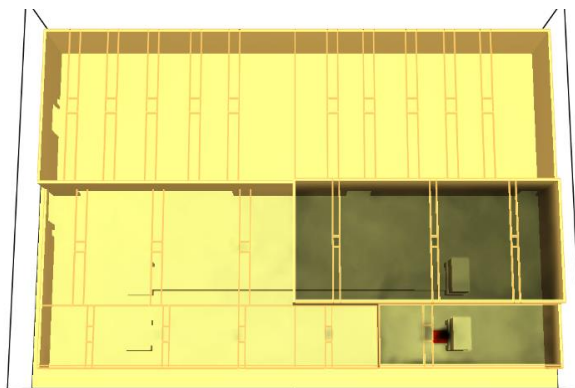
4. ábra: 5 MW-os tűz esetén füstterjedés 600s-nál oldalnézetből (saját szerkesztés)

A szimuláció alapján 500 kW-os tűz esetén a füstterjedés alakulását láthatjuk az alábbiakban 300 s és 600 s elteltével:



Time: 300.0

5. ábra: 500 kW-os tűz esetén füstterjedés 300s-nál felülnézetből (saját szerkesztés)



Time: 593.4

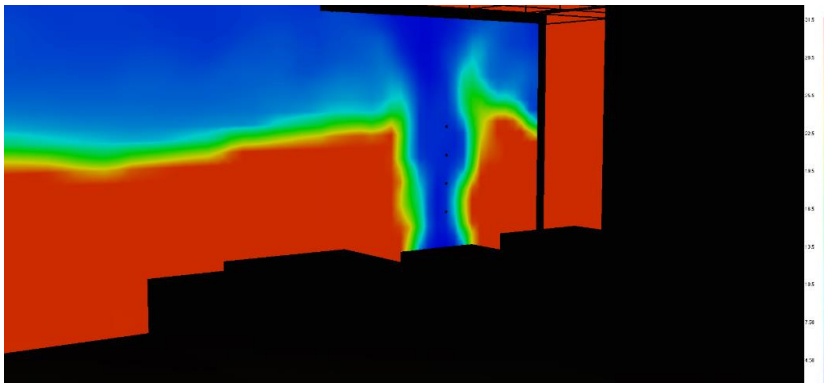
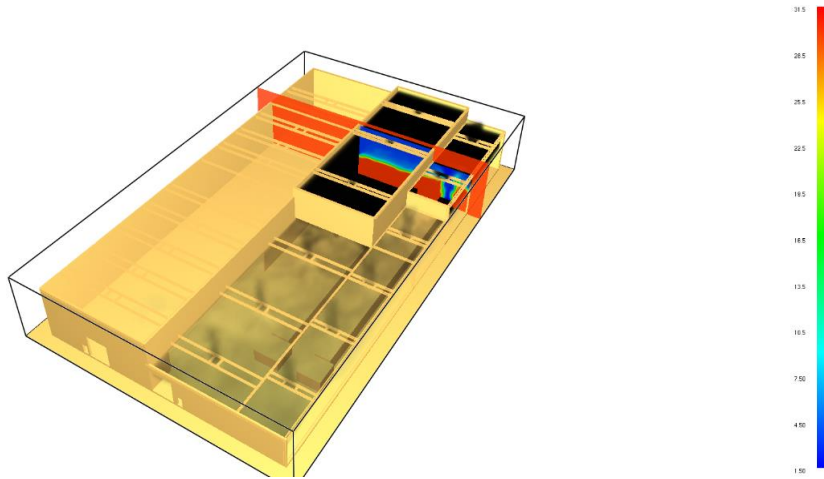
6. ábra: 500 kW-os tűz esetén füstterjedés 600s-nál felülnézetből (saját szerkesztés)



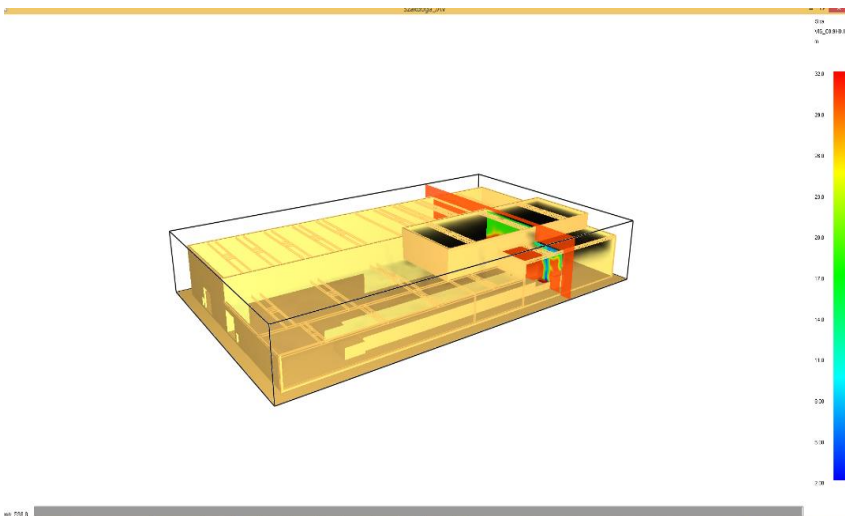
Time: 593.4

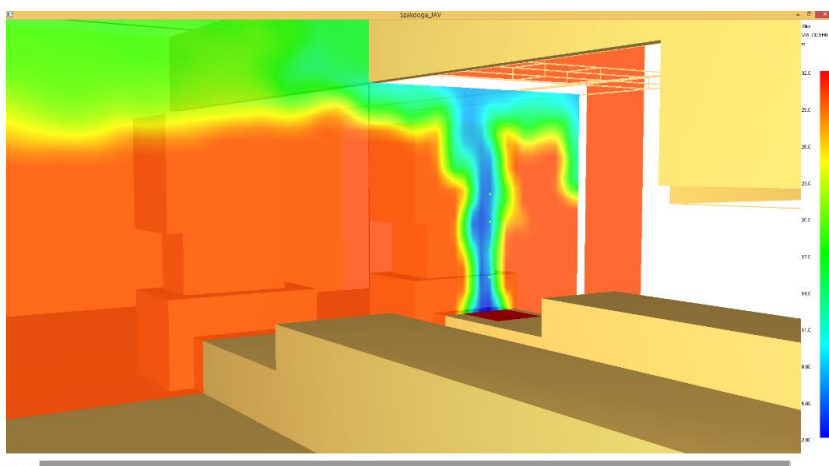
7. ábra: 500 kW-os tűz esetén füstterjedés 600s-nál oldalnézetből (saját szerkesztés)

A szimuláció alapján a láthatósági viszonyok a következőképpen alakultak az üzem területén a tűz keletkezését követő 600 s-nál.



8.ábra: Melegprés üzemből a láthatósági viszonyok alakulása 5 MW-os tűzterhelésnél 600 s-nál (saját szerkesztés)





9. ábra: Melegprés üzemben a láthatósági viszonyok alakulása 500 kW-os tűzterhelés esetén 600 s-nál (saját szerkesztés)

A modellezés eredményeképpen megállapítottuk, hogy az épületben a korábbiakban ismertetett feltételek teljesülése esetén – amely vonatkozik a tűz méretére, a kezdeti helyszínére, a hőfelszabadulás mértékére, a hőfelszabadulás lefolyására – milyen körülmények várhatók életvédelmi szempontból. A melegprés üzemben műszaki hibából eredő hidraulika olaj elfolyás során keletkező tűz esetén a látótávolság megfelelőnek adódott, a kiürítési útvonalon 25 m alatti látótávolság nem alakult ki. Megállapítottuk, hogy a tűzoltók kiérkezéskor (kb. 8 perc) meg tudják közelíteni a tűzfészket és nem kell 10 méternél kisebb látótávolságú területen áthaladniuk a beavatkozás során.

KÖVETKEZTETÉSEK, JAVASLATOK

A szimulációs vizsgálati eredmények alapján megállapítottuk, hogy tűz esetén a csarnokban a füstterjedés során kialakuló láthatósági viszonyok lehetővé teszik, hogy az ott tartózkodó kezelő személyzet (50 fő) a tűz jelzését követő 2 percnél belül elhagyja az épületet.

A lényegesen drágább tűzálló hidraulika olaj használata esetén a gyulladáspont emelkedése miatt a tűzkockázat ugyan csökken, de a 900 °C -os fém felülete mégis elég gyújtási energiát adhat ahhoz, hogy a tűzálló hidraulika olaj is meggyulladjon. Tehát a tűz keletkezés nem zárható ki teljes mértékben ebben az esetben sem. Számos üzemben még mérsékelt tűzveszélyes hidraulika olajat alkalmaznak, melynél a gyulladáspont alacsonyabb mint a tűzálló olajnál, valamint használat közben fennáll a kockázata az olaj szennyeződésének. Ez tovább növelheti a tűzkockázatot.

Emiatt a beépített tűzjelző rendszer mellett beépített oltórendszer kiépítését is javasoltuk az üzemben, mely ugyan drágább megoldás, de garantálja a tűzkár minimálisra csökkentését és az esetleges termelés kiesésből származó anyagi károkat is mérsékli.

Javasoltuk továbbá az épület statikai szakértővel történő felülvizsgálatát, mivel a teherhordó szerkezetek védelem nélküliek, ezért kérdéses a modellben szereplő tűzterhelés esetén a szerkezet állékonysága. Továbbá javasoltuk minél kevesebb éghető anyag csarnokban történő tárolását, illetve a hidraulika olaj minimum éves szintű labor vizsgálatát.

ÖSSZEFOGLALÁS

Tanulmányunkban laborvizsgálat során vizsgáltuk, hogy a présgép hidraulika olajának éghetőségét befolyásolják-e az olaj minőségében bekövetkező változások. Ezt követően szimuláltuk a tűzvédelmi berendezésekkel részben ellátott fiktív üzemben az olaj meggyulladásának következményeit, a tűz- és füstterjedést.

Elemzéseink által megállapítottuk, hogy a tűz keletkezés nem zárható ki teljes mértékben tűzálló hidraulika olaj alkalmazása révén sem. Ugyanakkor az égés lángja kisebb kiterjedésű, illetve kontrolláltabb, mely egy esetleges tűz térbeli szétterjedését lassíthatja. A mérsékelt tűzveszélyes olaj esetén a minőségében szennyezés miatt bekövetkezett változás valószínűleg hatást gyakorol annak tűzveszélyességi jellemzőire, csökkenti annak lobbanás- és gyulladáspontját.

A szimuláció rávilágított arra, hogy az üzemben a tűz- és füstterjedés során kialakuló láthatósági viszonyok lehetővé teszik ugyan, hogy az ott tartózkodó személyek a tűz jelzését követő 2 percen belül elhagyják az épületet, azonban az anyagi kár így is számottevő lehet. Ezért a beépített tűzjelző berendezés mellett beépített oltórendszer kiépítését is javasoltuk az üzemben, mely ugyan drágább megoldás, de garantálja a tűzkár minimálisra csökkentését és a termelés kiesésből származó anyagi károkat is jelentősen mérsékelheti.

Összességében megállapítható, hogy az autóiipari gyártásnál a présgép hidraulika olajának szivárgásából eredő tűzkockázat a tűzálló hidraulika olaj és a beépített tűzvédelmi jelző- és oltóberendezések együttes alkalmazása révén csökkenthető.

FELHASZNÁLT IRODALOM

- [1] M. I., Kiani, Gandikota, M., Rais-Rohani, K., Motoyama, „*Design of lightweight magnesium car body structure under crash and vibration constraints*” J. Magnes Alloys, 2 vol., pp. 99–108., 2014.
- [2] T., Chenpeng, Q., Rong, V. A., Yardley, X., Li, J., Luo 2, G., Zhu and Z., Shi, *New Developments and Future Trends in Low-Temperature Hot Stamping Technologies: A Review. Metals*, 10 (12), 1652. pp 1-27.,2020.
- [3] Quad Fluid Dynamics Inc., „*Common Hydraulic Press Problems, Causes and Prevention Options*”, 2021. Elérhető: <https://www.quadfluidynamics.com/3-common-hydraulic-press-problems-causes-and-prevention-options> (Letöltve: 2023. május 19.)
- [4] Á. Zs., Mohai, „*A tűzjelző berendezések riasztási hatékonysága*”, Műszaki Katonai Közlöny, XXVII. évfolyam, 3. szám, pp.20-37., 2017.
- [5] Á. Zs., Mohai, és L., Beda, „*Gondolatok a tűzjelző berendezések hatékonyságáról*”, Védelem Tudomány, I. évf. 4. szám, 2016.
- [6] Quaker Houghton, „*Fire Safety In Hot Forming Hydraulic Presses*”, 2019. Elérhető:https://fireresistantfluids.com/wp-content/uploads/ps_quintolubric_888_fire-safety-in-hot-forming-hydraulic-presses_EN_EU.pdf. (Letöltve: 2023. május 18.)
- [7] MSZ EN ISO 2592:2002, A lobbanás- és a gyulladáspont meghatározása. Cleveland szerinti nyitott tégelyes módszer. Kiadva: Budapest, Magyar Szabványügyi Testület, 2002.
- [8] L., Valasek, *The use of PyroSim graphical user interface for FDS simulation of a cinema fire*” International Journal of Mathematics and Computers in simulation, Issue 3, Volume 7, 2013.

- [9] Y. J., Ko, „*A Study of the Heat Release Rate of Tunnel Fires and the Interaction between Suppression and Longitudinal Air Flows in Tunnels*”, PhD thesis. Department of Civil and Environmental Engineering, Carleton University, 2011.
- [10] B., Truchot, T. Durussel, S., Duplatie, „*Combustion Rate of Medium Scale Pool Fire, an Unsteady Parameter*”, 2010. Elérhető: <https://hal-ineris.archives-ouvertes.fr/ineris-00973598/document>. (Letöltve: 2023. május 14.)

**THE ROLE OF OCCUPATIONAL SAFETY
AND HEALTH REPRESENTATIVES IN
PERFORMING OCCUPATIONAL SAFETY
AND HEALTH DUTIES****A MUNKAVÉDELMI KÉPVISELŐK
SZEREPE A MUNKAVÉDELMI
FELADATOK ELLÁTÁSÁBAN**LEISZTNER Péter¹**Abstract**

One of easily accessible forms of occupational safety and health advocacy is the occupational safety and health representative system. In addition to being dependent on the will of employers and employees, the conduct and success of the election also depends on the candidate's acceptance and ability. In order to effectively contribute to the representation of the rights and interests of employees, it is essential that they want to do something for them. During the research, we examined the acceptance of representatives, the company's role in occupational safety and health, their skills beyond the qualifications required to perform the task, and their professional knowledge of occupational safety and health from the perspective of professionals. The aim of the research is to examine the tasks of Hungarian occupational safety and health representatives, their location within the occupational safety and health organization, and their acceptance during qualitative research with the involvement of occupational health and safety specialists with the help of in-depth expert interviews, using the methodology of content analysis.

Keywords

occupational health and safety, occupational health and safety representative, efficiency, soft skill, consultation

Absztrakt

A munkavédelmi érdekképviselőt egyik legkézenfekvőbb, legkönnyebben elérhető formája a munkavédelmi képviselői rendszer. A munkavédelmi képviselő választás megtartása és eredményessége, azon felül, hogy a munkáltatók és a munkavállalók akaratán múlik, nagyban függ a jelölt elfogadottságától és rátermettségétől. Ahhoz, hogy hatékonyan tudjon közreműködni a munkavállalók jogainak és érdekeinek képviselésében, elengedhetetlen, hogy tenni akarjon értük. A kutatás során munkavédelmi szakemberek szemszögéből vizsgáltuk meg a munkavédelmi képviselők elfogadottságát, szerepüket a vállalkozás munkavédelmében, a feladat ellátásához szükséges szakmai képzettségen felüli készségeiket, és munkabiztonsági szakmai tudásukat. A kutatás célja a magyarországi munkavédelmi képviselők feladatainak, a munkavédelmi szervezeten belüli elhelyezkedésüknek, és elfogadottságuknak vizsgálata kvalitatív kutatás során, munkabiztonsági szakemberek bevonásával szakértői mélyinterjúk segítségével, tartalom elemzés módszertanával.

Kulcsszavak

munkavédelem, munkavédelmi képviselő, hatékonyság, soft skill, konzultáció

¹ leisztner.peter@uni-obuda.hu | 0000-0001-5302-5832 | PhD Student, Óbudai University Doctoral School for Safety and Security Sciences | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Tájékoztatás és konzultáció. Két szó, mégis mindennapjaink során számtalanszor találkozhatunk velük, alkalmazhatjuk ezeket. Mikor szakemberhez fordulunk egy-egy problémánkkal, máris konzultálunk, és amikor a kérdésünkre adott válasza ismeretanyagot, illetve adatot tartalmaz, akkor tájékoztat minket. Egyszerűnek tűnik, még akkor is, ha e két szó jelentését esetleg nem is ismerjük. De mi a helyzet, ha munkavédelmi környezetben helyezük el azokat? Munkabiztonsági szakemberként tanultuk, tudjuk, és adaptáljuk eme fogalmakat, tisztában vagyunk vele, hogy a munkavédelem szerves részét képezik. Már a Lisszaboni Szerződés, mely az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződést módosítása, a 153. cikkében foglalkozik munkavédelemmel, és ezen belül is a munkavállalók tájékoztatásával, és véleményük meghallgatásával[1]. A Tanács Irányelve (1989. június 12.) a munkavállalók munkahelyi biztonságának és egészségvédelmének javítását ösztönző intézkedések bevezetéséről (89/391/EGK) (HL L 183., 1989.6.29., 1. o.) (továbbiakban irányelv) 1. cikkének (2) pontja többek között általános elveket, továbbá általános iránymutatásokat tartalmaz a munkavállalók és képviselőik nemzeti jogszabályoknak, illetve gyakorlatnak megfelelő tájékoztatásáról, a velük folytatott konzultációról[2]. Az irányelv a további cikkek során részletesen kifejti az ezekkel kapcsolatos jogokat és kötelezettségeket, melyek a magyar szabályozásban az 1993. évi XCIII. törvény a Munkavédelemről című, és a 2012. évi I. törvény a Munka Törvénykönyvéről című törvényekben jelenik meg.

Azt láthatjuk, hogy jogok és kötelezettségek vannak a tájékoztatással, és konzultációval kapcsolatban, de a munkavállalók, képviselőik és a szakemberek élnek-e vele. A munkavédelmi képviselők munkavédelemben jártas személyeknek tekinthetőek-e, és megválasztásuk esetén (amennyiben igény merül fel a munkavállalók részéről részt venni a jelölési folyamatban, és a választáson) valóban részt tudnak-e venni ezekben az eljárásokban. Jelen tanulmány célja a tájékoztatás és konzultáció folyamatának megismerése volt a munkavállalók képviselőinek, azaz a munkavédelmi képviselőknek létjogosultságának, elfogadottságának és szerepének elemzésével, a munkabiztonsági szakemberek szemszögéből vizsgálva, különböző szektorokhoz tartozó magyarországi vállalkozások körében.

SZAKIRODALMI ÁTTEKINTÉS

„Minden munkavállalónak joga van az egészségét, biztonságát és méltóságát tiszteletben tartó munkafeltételekhez.” (Magyarország alaptörvénye XVII. cikk (3) pont)[3]. Azonban a tripartizmus elve szerint, ami az állam, a munkáltató és a munkavállalók jogain és kötelezettségein alapul[4], a munkavállalónak nem csak jogai, hanem feladatai is vannak, ezen munkafeltételek eléréséhez.

A munkavállalók a munkavédelmi tájékoztatáshoz, illetve konzultációhoz való jogukat érvényesíthetik saját maguk, vagy képviselőik által. A munkavédelmi törvény 70/A. § (1) pontja szerint jogosultak az érdekeik, és jogaik képviseletére maguk közül munkavédelmi képviselőt választani és a 70/A. § (1) a) pontja szerint választást kell tartani minden olyan munkáltatónál, ahol a munkavállalók létszáma legalább 20 fő[5]. Ez a törvény nem tesz különbséget a vállalkozási formában, pusztán a munkavállalók létszáma számít sarokpontnak. A KSH adatait a regisztrált vállalkozások száma létszám-kategória szerint megoszlásban az 1. táblázat tartalmazza.[6] Az adatok tanulsága szerint Magyarországon

~17 000 munkáltató kötelezett munkavédelmi képviselő választás megtartására. Ez nem azt jelenti, hogy a fennmaradó ~1,8 millió munkáltató esetén nem lehet munkavédelmi képviselőt választani, illetve azt sem, hogy megszűnik a munkáltató tájékoztatási és konzultációs kötelezettsége.

Létszám-kategóriák	2021
0 fős és ismeretlen létszámú	896 967
1–9 fő	921 155
10–19 fő	21 735
20–49 fő	11 077
50–249 fő	4 943
250 fő és több	982
Összesen	1 856 859

1. Táblázat: A regisztrált vállalkozások száma létszám-kategória szerint, saját szerkesztés, https://www.ksh.hu/stadat_files/gsz/hu/gsz0004.html (2022.10.21)

A törvény nem számszerűsíti a munkavédelmi képviselő választások számát sem a dolgozói létszám, sem a telephelyek függvényében, és arra már nem találunk adatot, valójában a vállalkozásoknál mennyi munkavédelmi képviselő került megválasztásra, hányan lettek oktattva és mennyien töltik ki a választási ciklusukat.

A magyarországi munkabalesetek számát és annak létszám szerint megoszlását az elmúlt négy és fél év vonatkozásában, illetve az ezekből halállal végződötteket a 2. táblázatban mutatjuk be[7]–[11].

Év	2018		2019		2020		2021		2022 első félév	
	Összes	Halálos	Összes	Halálos	Összes	Halálos	Összes	Halálos	Összes	Halálos
Létszám kategóriák										
1-9 fő munkavállaló	2 490	34	2 604	38	2 231	29	2 342	40	1 125	19
10-49 fő munkavállaló	6 555	28	6 829	30	5 985	20	6 330	22	2 898	13
50-249 fő munkavállaló	7 984	14	8 108	13	6 723	11	7 397	14	3 407	4
250-449 fő munkavállaló	2 549	1	2 426	1	2 048	1	2 094	4	959	1
500 fő, vagy több munkavállaló	4 093	2	3 992	1	3 338	3	3 355	4	1 372	0
A munkavállalók száma ismeretlen	67	0	96	0	41	0	73	0	15	1
Összesen	23 738	79	24 055	83	20 366	64	21 591	84	9 776	38

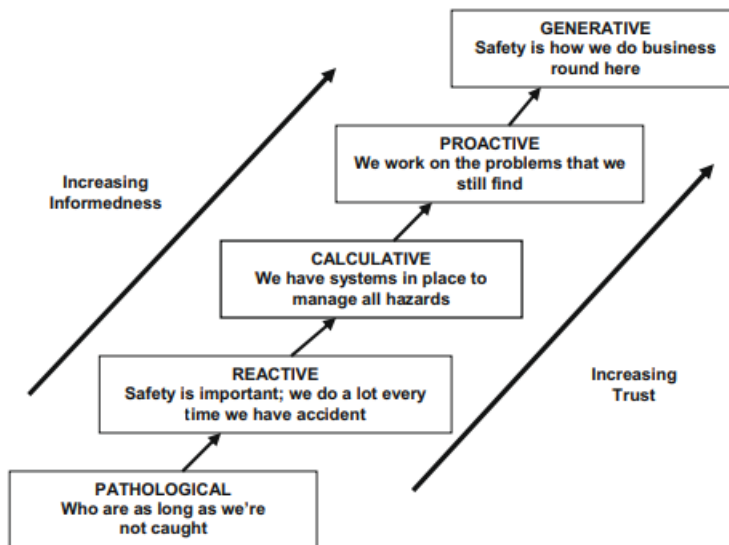
2. Táblázat: Balesetek és baleseti halálozások száma létszám-kategória szerint 2018-2022 első félév, saját szerkesztés, http://www.ommf.gov.hu/index.php?akt_menu=223 (2022.10.21)

A munkabaleseti statisztikák alapján nem lehet egyértelműen meghúzni a határt a munkavédelmi képviselő választás megszervezésére kötelezett, és nem kötelezett munkáltatók között. Ennek ellenére megállapíthatjuk, hogy 2018-2022 első féléve között, a munkabalesetek 10-12%-a az 1-9 főt foglalkoztató munkáltatóknál, 88-90%-a a 10 fő feletti munkavállalót foglalkoztatóknál következik be, míg a halálos balesetek közel fele-fele, 43-50% és 50-57% arányban oszlanak meg[7]–[11].

A balesetek számának folyamatos emelkedése miatt (a 2020-as visszaesésétől eltekintve), valamint a 2022 első félévében tapasztalt halálos munkabalesetek rendkívül magas

számát látva (2017 első féléve után a második legmagasabb szám 2017-2022 között vizsgálva), a munkabiztonsági szakemberekben felmerülhet a kérdés, mit tehetnek azért, hogy az általuk képviselt munkáltatónál milyen módon lehet a munkavállalókhoz közelebb hozni a munkabiztonságot. Ennek egyik módja, a munkavállalók által és közül választott munkavédelmi képviselő. Ezt támasztja alá az Országos Munkavédelmi Bizottság 2022.07.05-i „Tájékoztatása és Ajánlása”, mely a Munkavédelmi Törvény paragrafusai szerint tekinti át a munkavédelmi képviselő választástól, a bizottságaik megalakításán keresztül az oktatásukig való feladatokat[12]. Ilyen tananyagok és segédletek, szinte ágazatonként jelentek, jelennek meg, érhetőek el[13]–[16].

Az Európai Szakszervezeti Intézet 2006-ban indította az EPSARE (European Project on Safety Reps) programját, melyben elsődlegesen azt próbálták feltérképezni, hogy a munkahelyi egészségvédelem szempontjából mennyire hatékony a munkavédelmi képviselők által végzett tevékenység[17]. Ez leginkább a munkavédelmi teljesítmény mérése, valamint a szervezeti kultúra feltérképezése során mérhető[18], melynek szerves részét képezi a vállalkozás pozíciója a biztonsági kultúra modelljén[19], melyet az 1. ábra mutat be. Látható, hogy a biztonsági szint növekedésével együtt emelkedik a tájékozottság és a bizalom.



1. Ábra: A Hudson féle biztonság kultúra modell, Patrick Hudson, „Aviation safety culture,” in *Safeskie*, 2001, pp. 1–23.

Ez a modell az alábbi szintekből áll:

- „Patológiai” szint – amíg el nem kapnak minket szemlélettel
- „Reaktív” szint – már fontos a biztonság, és mindent megteszünk, mikor balesetet szenvedünk.
- „Kalkulatív” szint – már vannak rendszereink az összes veszély kezelésére
- „Proaktív” szint – dolgozunk a még mindig feltárt problémákon
- „Generatív” szint – a biztonság köré épül a vállalkozásunk

A munkavédelmi szakemberek célja természetesen a legfelső, a „Generatív” szint elérése kell, hogy legyen, melyben a kockázatkezelés, a kockázat értékelés és ezek kommunikációja a dolgozókkal vagy képviselőikkel folytatott konzultáció nyújt segítséget[20]. Ebben a folyamatban a munkavédelmi képviselőkre fontos feladat hárul, hiszen, ha „maradandó élményt” nyújtanak a munkavállalóknak, tehát emlékezetessé teszik a probléma megoldását, legyen az munkavédelmi, munkahelyi vagy magánéleti, akkor a választóik a tapasztalataik alapján szívesen fogják egymásnak ajánlani őket[21].

KUTATÁSMÓDSZERTAN

A kutatás célja feltárni a munkavédelmi képviselők elfogadottságát a munkabiztonsági szakemberek körében, megismerni véleményüket a munkavédelmi képviselők szervezeten belüli elhelyezkedéséről, a szervezet munkavédelmi teljesítményére gyakorolt hatásokról, és rávilágítani a munkavédelmi konzultációban és tájékoztatásban betöltött szerepükre. További célkitűzés megismerni a munkabiztonsági szakemberek véleményét a munkavédelmi képviselők képzésének, képzettségének a gyakorlatban történő hasznosíthatóságáról.

Kutatásunk során munkabiztonsági szakemberek körében az alábbi kutatási kérdésekre keressük a választ:

- Kutatási kérdés 1 – Milyen legyen a munkáltató munkavédelmi szervezetének felépítése?
- Kutatási kérdés 2 – Mi a munkavédelmi képviselők szerepe a vállalkozás munkavédelmi szervezetében?
- Kutatási kérdés 3 – Milyen hatása van a munkavédelmi képviselőnek a szervezet munkavédelmi teljesítményére, a szervezet biztonsági kultúrájára?
- Kutatási kérdés 4 – Milyen tevékenységet folytat a munkavédelmi képviselő a munkavédelmi tájékoztatásban és konzultációban?
- Kutatási kérdés 5 – Mennyire használható a gyakorlatban a munkavédelmi képviselők felkészültsége és képzettsége?

Szeretnénk a gondolataikat megismerni a munkavédelmi képviselők választásával, képzésével, szükségességével kapcsolatban. Célunk eléréséhez, a problémák, a folyamatok, és az emberi viselkedés mélyebb megértéséhez[22] kvalitatív technikát választottunk. Ez a kutatási módszer általában alkalmas mélyebb, árnyaltabb ismeretek megszerzésére, viszonylag kis elemszámú mintán történő adatfelvétel mellett[23], mely mintákban nem volt célunk a reprezentativitás.[22] Kutatásunkat kvalitatív kutatási módszer mentén végeztük, interjú és szövegelemzés által nyert kvalitatív adatokra alapoztuk[24]. Szakértői mélyinterjúk lefolytatása mellett döntöttünk, mivel interjú alanyaink személyes motivációira vagyunk kíváncsiak, és az interjúkat a munkabiztonsági terület szakértőivel végeztük.[23]. Módszertanát tekintve a kvalitatív kutatás tartalom elemzés módszerét választottuk, a szakértői mélyinterjúkat, mint közleményeket szisztematikusan objektív módszerrel vizsgáltuk[25]. A választásunkat támasztja alá, hogy az interjúk készítése során célunk az egyéni szempontok alapos megértése[26]. A kutatási kérdéseket figyelembe vettük az interjú vezérfonalának elkészítésekor, de a tartalomelemzés során az interjúk alapján készített átiratok szövegére fókuszáltunk[27].

Az interjúk készítéséhez a távolság és az interjú alanyok korlátozott elérhetősége miatt, az Óbudai Egyetem által biztosított BBB (BigBlueButton), illetve Microsoft TEAMS felületeken online egyénenkénti megkeresést választottuk, így egy-egy beszélgetésen, csak az interjúalany és az interjú készítője vett részt[26].

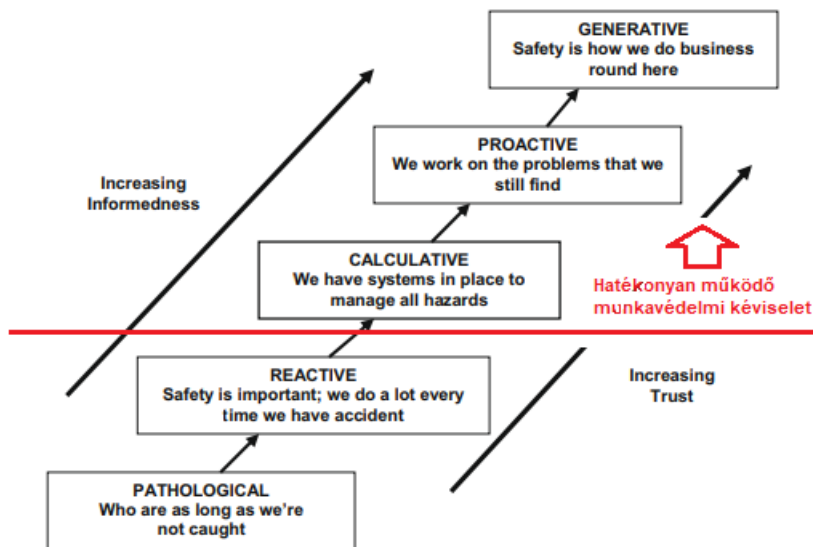
A mintavételezés során törekedtünk olyan szakértők megkeresésére, kiknek munkahelyén, illetve szolgáltatási területén, az általuk munkavédelmi képviselt szervezetek munkavédelmi képviselő választás megtartására kötelezettek, illetve munkájukkal összefüggésben jelentős ismeretekkel rendelkeznek a munkavédelmi képviselőkkel kapcsolatos jogszabályi háttérrel, és annak gyakorlati alkalmazásával. A mintavételezés úgynevezett kényelmes mintavételezés, hiszen a mintába olyan szakértőket választottunk, akiket a legkönnyebben elértünk[23]. Ezen szempontok alapján 8 fő tapasztalt munkabiztonsági szakembert (1 nőt és 7 férfit) választottunk ki multinacionális, nagyvállalati, KKV (Kis és közép vállalkozás) és állami környezetből.

KUTATÁSI EREDMÉNYEK

A szakértői mélyinterjúk elemzése során megállapítható, hogy a munkabiztonsági szakemberek számítanának rá, elvárják a munkavállalók és képviselőik részvételét a munkáltatók munkavédelmi szervezetében. Ezt a részvételt elsősorban a vállalkozás méretéhez kötik, és bár éles határ nem húzható, de „néhány fő” munkavállalóig III. veszélyességi osztályba sorolás esetén nem ragaszkodnak a munkavédelmi képviselőkhöz, viszont nagyobb méretű vállalkozások esetén, már előnyösnek látnák akár több (telephelyenként, és műszakonként) munkavédelmi képviselőt választani. Hangsúlyozottan megjelenik, hogy a vállalkozások elsősorban a jogszabályoknak kívánnak megfelelni, mind a munkavédelmi szakemberek (beleértve a munkabiztonságot és a foglalkozás egészségügyet is), mind a munkavédelmi képviselők esetén is, bár ennek többen látták pozitív irányú változását. A munkavédelmi szervezet, illetve a munkavédelem felépítése során fontosnak látják, hogy a szakemberek közvetlen a legfelső vezetéshez legyenek kapcsolva, és a hierarchikus szervezeti felépítéstől függetlenül, minden munkavállalónak részt kell, részt kellene vennie benne. „...ez szerintem egy kulcskérdés, hogy a legfelsőbb vezetők is legyenek a témában elhivatottak és közvetlen kapcsolatuk legyen a munkavédelmi szervezettel”

Az interjúalanyokat erősen megosztotta a munkavédelmi képviselők hatékony részvételének feltétele a munkáltató munkavédelmi szervezetében. Részben elmondható, hogy elsősorban az akarat a fontos, tehát, hogy részt akarjanak benne venni. Másrészt néhányan a hatékony részvételt a tudásukhoz kötötték. Ez a tudás nem feltétlenül munkavédelmi tudás, hanem elegendő lehet azzal tisztában lenniük, hogy kihez fordulhatnak az egyes problémáikkal, kérdéseikkel. Jól növeli a hatékonyságukat, ha nem a munkáltatóval, illetve a munkavédelmi szakemberekkel szemben próbálnak tevékenykedni, hanem velük párhuzamosan, munkájukat segítve tenni a munkahely egészségessé és biztonságossá tételéért. „...az ideális esetet kiegészítem azzal, hogy ebben az ideális világban a munkavállalók illetőleg a középvezetők tisztában vannak a munkavédelmi felelősségükkel és maguktól részt is vesznek a szervezet munkavédelmi kultúrájának a fenntartásában vagy építésében” Mindenképpen árnyékot vet a kutatási eredményeinkre, hogy többen véleménye szerint is bevált gyakorlat, a munkavédelmi képviselők, vezetők általi kijelölése és megválasztása. Szintén a hatékonyságot csökkenti a munkavállalók és képviselőik féltelme a közvetlen, illetve felső vezetőktől, és bár ez jellemzően nem hangzott el, de egyáltalán nem fordulhatna elő.

Abban egyetértenek az interjúalanyok, hogy az 1. Ábrán bemutatott Hudson féle biztonság kultúra modell minden szintjén működhet a munkavédelmi képviselő, de többségük véleménye szerint a hatékony megjelenését a Kalkulatív, illetve Proaktív szint körül lehet elképzelni, amit a 2. ábra szemléltet. Hatékonyságuk gyakorlatilag a munkáltató biztonság kultúrájával együtt fejlődik, azzal szorosan összefügg.



2. Ábra: A hatékonyan működő érdekképviselet a Hudson féle biztonság kultúra modellen, saját szerkesztés

A munkavédelmi teljesítmény méréséhez kapcsolódó kérdésünk során egyetlen esetben érkezett a munkavédelmi képviselők teljesítmény mérésével kapcsolatos, a konzultációk számát vizsgálható KPI (Key Performance Indicator – fő teljesítménymutató) meghatározása, de ez a szakértő elég jól ismeri a kutatási területünket, így ezt nem tekinthetjük eredménynek. Viszont megállapítható, hogy az interjúalanyok ismerik és alkalmazzák az úgynevezett „leading indikátorokat”, vagyis a jövőbe mutató teljesítménymutatókat, melyek közül több a munkavállalók és képviselők teljesítmény mérésére alkalmasat is felsoroltak. Ezek közé tartoznak az oktatások, az auditok, a hatósági ellenőrzések, de ide sorolhatjuk a dolgozók által elhárított rendellenességek számát, például egy mozgó kilincs csavarjának a meghúzását is.

A munkavédelmi képviselők feladatainak elemzése során az interjúkból levonható, hogy a megkeresett szakértők mindannyian jól ismerik a jogszabályi előírásokat, melyektől a későbbiek folyamán el tudtak vonatkoztatni, és a valós véleményüket, vágyaikat fogalmazták meg. A kötelező feladatokon felül kiemelték a kapcsolattartást, a kommunikációt, a megelőzést, a közvetítést. A felsorolt tevékenységeken túl egy esetben itt is megjelenik egy negatív felhang, miszerint egyes helyeken csak azért van munkavédelmi képviselő, hogy a munkáltató reprezentálni tudja a jogszabályi megfeleléseit. Egy másik interjú során, viszont rendkívül jól írja le az interjúalany a feladatot, miszerint a munkavédelmi képviselőnek egy úgynevezett „szeizmográfznak” kell lennie, és a vállalkozáson belüli legapróbb rezgést, származzon az a munkatársaktól, vezetőktől vagy beosztottaktól, észre kell, vagy észre

kellene vennie és annak esetleges a munkabiztonságra, illetve egészségvédelemre való negatív hatása előtt szükséges cselekednie, illetve beavatkoznia. A feladatok elemzése során kíváncsiak voltunk, vajon milyen soft skillekkel, azaz szakmai tudáson felüli képességekkel kell rendelkezzenek a munkavédelmi képviselők. Ennek eredményét a 3. táblázatban foglaljuk össze, mely alapján jól látható, hogy a szakértők a hangsúlyt a kommunikációra helyezték, de véleményük szerint nem elhanyagolható a közvetítő, kapcsolatteremtő, vagy empatikus készség, a nyitottság, illetve a műszaki érzék megléte sem.

Említett képesség	Említések száma
Legyen jó közvetítő	2
Legyen jó kapcsolatteremtő	2
Legyen nyitott	2
Legyen asszertív	3
Jól kommunikáljon	3
Legyen rugalmas	1
Legyen türelmes	1
Legyen önbecsülése	1
Legyen empatikus	2
Legyen műszaki érzéke	2
Legyen mosolygós	1
Legyen emocionális	1
Legyen nagyfokú diplomáciai érzéke	1
Legyen influenszer	1
Legyen kompromisszumkész	1
Legyen nyugodt	1

3. Táblázat: A munkavédelmi képviselők „soft skilljei”, saját szerkesztés

A munkavédelmi képviselők munkavédelmi tudását feltáró kérdések megosztják az interjúalanyokat. Többségük úgy gondolja, hogy az ilyen jellegű ismeretük semmire nem, vagy csak minimális feladatokra elegendő, de ennek ellenére hasznos segítői lehetnek a munkavédelmi szakembereknek, amennyiben a megszerzett tudást támogatólag és nem támadólag hasznosítják. „...egy tudás mindig arra elegendő, amire használom” Itt is fontosnak tartják, hogy a megválasztott munkavédelmi képviselők akarjanak tenni az egészséget nem veszélyeztető és biztonságos munkavégzésért, és érdeklődjenek, képezzék magukat, ha kell forduljanak szakemberhez vagy az adott terület szakértőjéhez. „... azt mondom, hogy a munkavédelmi képviselőknek egyébként joguk van munkavédelmi szakértőkhöz fordulni, tehát igazából a munkáltatónak ezt biztosítani kell a számukra”. Egy másik vélemény szerint, a több cikluson át tartó megbízatás során nagyon nagy szakmai fejlődés figyelhető meg, illetve a multinacionális vállalati környezetben a munkáltató által szervezett képzésekkel is jelentős fejlődés érhető el. „...ahogy elmondtam, hogy nekünk egy nagyon pozitív helyzetünk van, illetve nekem a munkahelyemen multinál, illetve én a gondozásomba is vettem ezt a témát, és képezzük a mi munkavédelmi képviselőinket” A közép vagy felsőfokú képzésüket nem gondolják megoldásnak, illetve úgy vélik, hogy akit mélyebben érdekel a munkabiztonság, az magától is elvégzi legalább a technikus vagy új nevén a munkavédelmi előadói tanfolyamot.

KÖVETKEZTETÉSEK

A vizsgálat rávilágított, hogy hatékonyan működő munkavállalói érdekképviseletet csak akkor lehet létrehozni, ha a tulajdonosokban, a vezetőkben és a munkavállalókban is megvan az egészséget nem veszélyeztető, biztonságos munkavégzés iránti vágy. Ennek felbresztése már gyermekkortól szükséges lehet, és ebben segíthet az úgynevezett biztonság-tudatos nevelés. Fontos feladatunk, hogy a munkakezdő fiatalok az első munkába lépéskor, már tisztában legyenek a munkavédelemmel kapcsolatos jogaikkal és kötelezettségeikkel, és az állásinterjúkon ne a fizetés és a juttatások legyenek az egyedüli szempontok, hanem jusson eszükbe az is, hogy majdan a nyugdíjas éveiket is szeretnék egészségileg magas minőségben megélni. Ebben a folyamatban a munkavédelmi szakemberekre nagy felelősség hárul, hiszen a munkahelyek biztonságkultúrájának fejlődése, valamint a munkavállalók munkavédelemmel kapcsolatos tudása és ismerete jelentős mértékben a munkájuk gyümölcse.

ÖSSZEFOGLALÁS

Jelen kutatás célja a Magyarországon megválasztott munkavédelmi képviselők szakemberek általi elfogadottságának felmérése, a munkabiztonsági tudásuk használhatóságának vizsgálata, valamint a feladat ellátásához szükséges szakmai tudáson felüli késések feltárása volt. A kvalitatív kutatás eredményei rámutattak, hogy a hatékonyan működő munkavédelmi képviselő mélyreható munkavédelmi ismeretek nélkül is fontos szerepet tölthet be egy vállalkozás munkavédelmében.

Az első kutatási kérdésben azt vizsgáltuk, hogy a munkavédelmi szakemberek véleménye szerint milyen a felépítése a hatékonyan működő munkavédelmi szervezetnek. Az interjúalanyok szerint legfontosabb, hogy legyen a munkavédelem irányába elkötelezett menedzment, ehhez közvetlenül kapcsolódó munkavédelmi szakemberek, és a saját biztonságuk érdekében tenni akaró munkavállalók. A munkavédelmi képviselők választását a munkavédelmi szervezetben a vállalkozás méretéhez kötötték.

A második kutatási kérdésben arra kerestük a választ, hogy milyen szerepe lehet a munkavédelmi képviselőknél a munkavédelmi szervezetben. A mintába bevont szakemberek gondolatai alapján, a megválasztott képviselők akkor tudnak hatékonyan részt venni ebben a szervezetben, ha rész akarnak venni, de ehhez a részvételhez nem magas szintű munkavédelmi tudással, hanem helyismerettel, és megfelelő érzékenységgel kell rendelkezzenek.

A harmadik kutatási kérdés a munkavédelmi képviselők a szervezet munkavédelmi teljesítményére, a szervezet biztonsági kultúrájára való hatását vizsgálta. Az interjúalanyok többségükben a Hudson féle biztonság kultúra modellen a kalkulatív illetve proaktív szinten tudták elképzelni a hatékony munkavédelmi képviseletet. A munkavédelmi képviselők teljesítmény mérését viszont nem tartották fő teljesítménymutatónak.

A negyedik kutatási kérdésben a munkavédelmi képviselő munkavédelmi tájékoztatásban és konzultációban betöltött szerepét tártuk fel. A szakemberek gondolatainak elemzése során megállapíthattuk, hogy a soft skilllek között hangsúlyosan jelenik meg a kommunikáció, így fontosnak tartják ezeket a feladatokat.

Az ötödik, egyben utolsó kutatási kérdésben a munkavédelmi képviselők szakmai tudásának gyakorlati alkalmazhatóságát vizsgáltuk. Az interjúk alapján ez a tudás szinte

sem mire nem elég, de a szakemberek szerint nem is munkabiztonsági szakemberekké, hanem egy hatékonyan működő kapoccsá kell váljanak, a munkáltatók és munkavállalók között.

A szakértői mélyinterjúk elemzése során megállapítható volt, hogy az interjúalanyok szívesen látnának hatékonyan működő munkavédelmi képviseleti rendszereket, melyek a munkájukat támogatják, és segítségével elkerülhetik az úgynevezett „szakmai vak-ság” következményeit.

A kutatás során az alábbi hipotézisek fogalmazódtak meg bennünk, melyeket további vizsgálatoknak kívánunk alávetni:

- Hipotézis 1 – A vállalkozások biztonsági kultúrájának növekedésével arányosan fog növekedni a munkavédelmi képviselők magasabb szintű képzésének az igénye
- Hipotézis 2 – A munkavédelmi képviselők nem a munkavédelmi szakmai tudásuk, hanem a szakmai tudáson felüli képességeik fejlesztésével válhatnak hatékonyá
- Hipotézis 3 – A munkavédelmi képviselők kiválasztása során segítséget nyújthat a jelöltek konfliktuskezelési stratégiájának vizsgálata
- Hipotézis 4 – A biztonságtudatos nevelést már a gyermekkorban el kell kezdeni, hogy munkába álláskor már igénye legyen a munkavállalónak az egészséget nem veszélyeztető és biztonságos munkavégzésre

FORRÁSOK

- [1] Az Európai Unió Hivatalos Lapja, “Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata,” *Az Európai Unió Hivatalos Lapja*, vol. 55, pp. 0001–0390, 2012, [Online]. Available: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A12012E%2FTXT>.
- [2] *A Tanács irányelve (1989. június 12.) a munkavállalók munkahelyi biztonságának és egészségvédelmének javítását ösztönző intézkedések bevezetéséről (89/391/EGK)*. 2010, pp. 1–89.
- [3] *Magyarország Alaptörvénye (2011. április 25.)*. 2011, pp. 1–49.
- [4] Dudás Katalin; Koch Mária; Spiegel István, *Munkavédelmi jog és eljárások*. Akadémiai Kiadó, 2018.
- [5] *1993. évi XCIII. törvény a munkavédelemről*, no. 10. 1993.
- [6] “Foglalkoztatottság.” <https://www.ksh.hu/docs/hun/xftp/gyor/fog/fog2103.html> (accessed Oct. 25, 2022).
- [7] “Tájékoztató a munkabalesetek alakulásáról a feldolgozott munkabaleseti jegyzőkönyvek alapján 2018. év,” 2018. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=223.
- [8] “Tájékoztató a munkabalesetek alakulásáról a feldolgozott munkabaleseti jegyzőkönyvek alapján 2019. év,” 2019. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=223.
- [9] “Tájékoztató a munkabalesetek alakulásáról a feldolgozott munkabaleseti jegyzőkönyvek alapján 2020. év,” 2020. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=223.
- [10] “Tájékoztató a munkabalesetek alakulásáról a feldolgozott munkabaleseti jegyzőkönyvek alapján 2021. év,” 2021. [Online]. Available:

- http://www.ommf.gov.hu/index.php?akt_menu=223.
- [11] “Tájékoztató a munkabalesetek alakulásáról a feldolgozott munkabaleseti jegyzőkönyvek alapján 2022. év I. félév,” 2022. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=223.
- [12] “Országos munkavédelmi bizottság tájékoztatása és ajánlása a munkavédelmi érdekképviselő, érdekegyeztetés egyes kérdéseiről,” 2022. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=172&hir_reszlet=857.
- [13] Kisgyörgy Sándor, *Munkavédelmi képviselői rendszer működése*. Budapest: Friedrich-Ebert-Stiftung Budapesti Irodája, 2021.
- [14] Bartos Szabolcs; Nagy József, *A munkavédelmi képviselők feladatainak összefoglalása*. Magyar Iparszövetség (OKISZ), 2018.
- [15] Benda Máté, *A munkavédelmi képviselők feladatainak összefoglalása 6. Független Szakszervezetek Demokratikus Ligája*, 2019.
- [16] Mandrik István; Lukács Péter, *Munkavédelmi képviselők tananyaga és segédlete szálláshely-szolgáltatás, vendéglátás ágazatban dolgozó munkavállalók részére*. X-TRA Média Kft., 2018.
- [17] M. Menéndez, J. Benach, and L. Vogel, “The impact of safety representatives on occupational health: A European perspective,” 2009. [Online]. Available: https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CEAQFjAC&url=http://www.etui.org/content/download/2248/24742/file/Report_107_EN.pdf&ei=Tji_UfWQCovVkwXyj4DoBg&usg=AFQjCNF0xkSRZ8zdN2l5qdXMhSeLiHYBeg&bvm=bv.47883778,d.dGI&cad=rjt.
- [18] Faragó Ferenc, “Munkavédelmi teljesítménymérés és szervezeti kultúra kvalitatív felmérése közép- és nagyvállalati környezetben,” *Biztonságtudományi Szle.*, vol. 4, no. 1, pp. 131–141, 2022.
- [19] Patrick Hudson, “Aviation safety culture,” in *Safeskie*, 2001, pp. 1–23.
- [20] Szabó Gyula, “A munkavédelmi kockázatkezelés sajátosságai,” *Bánki Közlemények*, vol. 3, no. 1, pp. 5–12, 2020.
- [21] Kelemen-Erdős Anikó; Mitev Ariel Zoltán, “Eszképizmustól az ajánlásig – Élmenyfokozatok és hatásai a romkocsmákban = From Escapism To Recommendation – Experience Stages and Their Impact on Guests in Ruinpubs,” *Tur. Bull.*, vol. 20, no. 2, pp. 14–21, 2020, doi: 10.14267/turbull.2020v20n2.2.
- [22] Boncz Imre, *Kutatásmódszertani alapismeretek*. 2015.
- [23] Hunkár Márta, *A kutatás módszertana*. Debrecen, 2013.
- [24] Hornyacsek Júlia, *A tudományos kutatás elmélete és módszertana*. 2014.
- [25] Antal László, *A tartalomelemzés alapjai*. Budapest: Magvető Kiadó, 1976.
- [26] Gyulavári Tamás at al., *A marketingkutatás alapjai*. Akadémiai Kiadó, 2017.
- [27] Kelemen-Erdős Anikó; Mitev Ariel, “Holisztikus szolgáltatásélmény - vendég-utazás és kölcsönös értékteremtés dimenziói az art- és romkocsmák példáján,” *Mark. Menedzsment*, vol. 50, no. 3–4, pp. 88–101, 2016.

**REVIEW ABOUT THE BOOK PETER
NORVIG AND STUART J. RUSSELL:
ARTIFICIAL INTELLIGENCE
A MODERN APPROACH****RECENZÍÓ PETER NORVIG ÉS
STUART J. RUSSELL MESTERSÉGES
INTELLIGENCIA MODERN
MEGKÖZELÍTÉSBEŒN CÍMŰ KÖNYVÉRŐL**KOLLÁR Csaba¹**BEVEZETÉS**

A Panem Kiadó weboldalán [1] a könyvet a következı gondolatokkal ajánlja: „Ez a könyv megkísérli a mesterséges intelligenciát teljes szélességében feltárni: átölelve a logikát, a valószínőségszámítást, a folytonos matematikát, az érzékelést, a következtetést, a tanulást, a cselekvést, a méltányosságot, valamint a bizalom, a társadalmi közjó és a biztonság kapcsolódó kérdéseit, továbbá a mikroelektronikától, a világűrt kutató robotokon keresztül a felhasználók milliárdjait kiszolgáló online szolgáltatásokig terjedı alkalmazásokat. A mára ismert dolgokat egy közös rendszerré szintetizálja, átdolgozva a korai eredményeket a ma elterjedt ötletek és terminológia felhasználásával. Elsődleges célja átadni azokat az ötleteket, amelyek az MI-kutatás elmúlt hetven éve és a kapcsolódó kutatások elmúlt két évezrede során merültek fel”.

A SZERZŐK RŐVID SZAKMAI ÉLETÚTJA

Peter Norvig 1956. december 14-én született amerikai matematikus a Stanford Institute for Human-Centered AI kiváló oktatósi munkatársa. Tanulmányait a Brown Egyetemen, illetve a Kaliforniai Egyetemen, Berkeleyben végezte, az elıbbinél alkalmazott matematikából szerzett fokozatot, az utóbbinál pedig számítástechnika szakon kapott PhD fokozatot. Szakmai életútjának fontosabb állomásai és munkakörei: Woods Hole Oceanographic Institute (nyári programozási gyakornok), Higher Order Software, Inc. (a mőszaki személyzet tagja), University of Southern California (adjunktus), University of California, Berkeley (kutató), Sun Microsystems Labs (vezetı kutató), Harlequin, Inc. (vezetı tervezı), Jungle Corp. (vezetı tudós), NASA Ames Research Center (a Számítástechnikai Tudományok részleg vezetıje), Stanford University (elıbb, mint oktató, majd a MediaX kiváló vendég tudósa). Jelenlegi egyetemi tudományos tevékenysége mellett a Google kutatójaként is dolgozik, illetve korábban a Google keresési algoritmusokkal foglalkozó csoportját és a Google kutatási csoportját vezette. [2]

Stuart J. Russell 1962-ben született Portsmouth-ban, Angliában, brit matematikus az UC Berkeley számítástechnika professzora. Tanulmányait az Oxfordi Egyetem Wadham College-ában, illetve a Stanford Egyetemen végezte, az elıbbinél fizikusi diplomát szerzett, az utóbbinál számítástechnika szakon kapott PhD fokozatot. Szakmai életútjának fontosabb állomásai és munkakörei: IBM Systems Engineering Centre (programozó), IBM Los An-

¹ 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 fı munkatárs és vezetı, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Mőhely

geles Scientific Center grafikai kutatási projekt (programozó), Stanford Egyetem (tanársegéd), Stanford Egyetem (a Számítástechnikai Részleg kutatási asszisztense), Kaliforniai Egyetem (adjunktus, docens, majd professzor), Berkeley Egyetem Számítástechnikai Részleg (vezető), Berkeley Egyetem Villamosmérnöki és Számítástudományi Tanszék (vezető), Kaliforniai Egyetem Neurológiai Sebészeti Osztály (adjunktus), Fondation de l'École Normale Supérieure (egyetemi tanár), Université Pierre et Marie Curie (meghívott professzor). [3]

A SZERZŐK PUBLIKÁCIÓS TEVÉKENYSÉGE

Peter Norvig eddig megjelent fontosabb könyvei a következők [2]:

- 2022: Data Science in Context (szerzőtársak: Alfred Spector, Jeannette Wing, Chris Wiggins) Cambridge University Press.
- 2020: Artificial Intelligence: A Modern Approach, 4th Edition. (szerzőtárs: Stuart Russell) Pearson.
- 2020: Instructor's Manual for Artificial Intelligence: A Modern Approach. (szerzőtárs: Stuart Russell) Prentice Hall.
- 2001: Intelligent Help Systems for UNIX (szerkesztőtársak: Stephen Hegner, Paul McKevitt, Robert Wilensky).
- 1995: Artificial Intelligence: A Modern Approach. (szerzőtárs: Stuart Russell) Prentice Hall.
- 1994: Verbmobil: A Translation System for Face-to-Face Dialog. (szerzőtársak: Martin Kay, Mark Gawron) CSLI Press.
- 1992: Paradigms of Artificial Intelligence Programming: A Common Lisp Approach. Morgan-Kaufmann.

Stuart J. Russell eddig megjelent fontosabb könyvei a következők [3]:

- 2020: Artificial Intelligence: A Modern Approach. (szerzőtárs: Peter Norvig) 4th Edition, Pearson.
- 2020: Instructor's Manual for Artificial Intelligence: A Modern Approach. (szerzőtárs: Peter Norvig) Prentice Hall.
- 1995: Artificial Intelligence: A Modern Approach. (szerzőtárs: Peter Norvig) Prentice Hall.
- 1991: Do the Right Thing: Studies in Limited Rationality. MIT Press.
- 1989: The Use of Knowledge in Analogy and Induction. Pitman.

A KÖTET(EK) BEMUTATÁSA

A Peter Norvig és Stuart J. Russell által írt *Mesterséges intelligencia modern megközelítésben* című könyv angol nyelvű (Artificial Intelligence: A Modern Approach) változatának első kiadása 1995-ben jelent meg, legutóbbi kiadása – melyből a magyar fordítás is készült – pedig 2020. április 28-án. Az angol nyelvű könyv sikerét jelzi, hogy a világ több mint 1400 egyetemén használják tankönyvként, több szakértő a világ legnépszerűbb mesterséges intelligenciával foglalkozó tankönyvének tartja. A könyv célcsoportjának elsősorban az egyetemi tanulmányokat folytató hallgatókat tekintik, de a posztgraduális képzésben

részt vevők is eredményesen használhatják, különösen akkor, ha a kiterjesztett bibliográfia alapján (szükség esetén) az egyes fejezeteknél a könyvben leírtakhoz képest mélyebb ismeretek elsajátítása a cél.

A könyv magyar kiadása a legújabb angol nyelvű kiadás alapján készült, s terjedelmi okok miatt két kötetben jelent meg, melyek ugyan külön-külön is megvásárolhatók, de alapvetően a két könyv együttesen nyújtja azt az ismeretanyagot, amelyik révén a téma iránt komoly szakmai-tudományos érdeklődést tanúsító hallgatóknak és szakembereknek érdemes elsajátítaniuk.

A kétkötetes kiadvány a matematikai és nyelvi-algoritmusi függeléken kívül huszonnyolc folyamatosan növekvő számú fejezetet tartalmaz, ami alapján akár kettő-négy féléves, egymásra épülő tantárgyak tematikája is kialakítható, s különösen az alapozó fejezetek vonatkozásában érdemes is az ott taglalt fejezetekkel megismerkednie az érdeklődőknek.

A könyv első része – mely a Mesterséges intelligencia címet viseli – két fejezetet tartalmaz: Bevezetés, illetve Intelligens ágensek.

Az első fejezet vezeti be az olvasót a mesterséges intelligenciába. Ebben a fejezetben kerül meghatározásra a mesterséges intelligencia fogalma, illetve itt lehet olvasni a mesterséges intelligencia alapjairól, történetéről, jelenlegi helyzetéről, illetve használatának előnyeiről és kockázatairól is.

A második fejezet az intelligens ágensekkel foglalkozik, s ennek részenként az ágensek és környezetük bemutatásával, a racionalitás koncepciójával, a környezetek természetével, illetve az intelligens ágensek felépítésével.

A könyv második részének a címe: Problémamegoldás, s a témát négy fejezetben tárgyalja.

A harmadik fejezet a kereséssel történő problémamegoldással foglalkozik. Ennek részeként szó esik többek között a problémamegoldó ágensekről, a példaproblémákról, a különböző keresési algoritmusokról, a neminformált, illetve informált (heurisztikus) keresési stratégiákról, valamint a heurisztikus függvényekről.

Keresés bonyolult környezetben – ez a negyedik fejezet címe. E fejezet kiemelt témái a következők: lokális keresés és optimalizációs problémák, lokális keresés folytonos terekben, keresés nemdeterminisztikus cselekvésekkel, keresés részlegesen megfigyelhető környezetben, online kereső ágensek és ismeretlen környezetek.

Az ötödik fejezet – Keresés ellenséges környezetben és kétszemélyes játékok – első része bevezet a játékelméletbe. Ezt követően a fejezet a kétszemélyes játékokban hozható optimális döntésekkel, a heurisztikus alfa-béta fa kereséssel, a Monte Carlo fa kereséssel, a sztochasztikus játékokkal, a részlegesen megfigyelhető játékokkal, s végül a játékok keresési algoritmusainak korlátaival foglalkozik.

A hatodik fejezet a kényszerkielégítési problémákra fókuszál. A téma definitív meghatározását követően szó esik többek között a kényszerek terjesztéséről a következtetés kényszerkielégítési problémákban, a visszalépéses keresés alkalmazásáról, a lokális keresés kényszerkielégítési problémáiról, illetve a problémák strukturájáról.

A harmadik rész a tudás, következtetés és tervezés témakörét öt fejezetben dolgozza fel.

Elsőként – a hetedik fejezetben – a logikai ágensekről olvashatunk. A logikai ágensekkel foglalkozó fejezet alfejezetei a következők: tudásalapú ágens, wumpus világ, logika,

az ítéletkalkulus, mint nagyon egyszerű logika, az ítéletkalkulusban alkalmazott tételbizonyítás, hatékony ítéletkalkulusbeli modellellenőrzés, valamint az ítéletlogikát alkalmazó ágensek.

Az elsőrendű logikáról a nyolcadik fejezet ír. Ebben a fejezetben még egyszer szó esik a reprezentációról, az elsőrendű logika szintaxisáról, szemantikájáról, illetve használatáról, valamint a tudásmérnökség lehetőségeiről az elsőrendű logikában.

Az elsőrendű logika következtetéseivel kapcsolatban a kilencedik fejezet ad értékes tudást az olvasó számára. A fejezet bemutatja az ítéletlogikai és elsőrendű logikai következtetés közötti különbségeket, az egyesítést és az elsőrendű logikai következtetést, az előrefelé, illetve a hátrafelé láncolást, s végül a rezolúciót.

Az ontológiaszervezéssel, a kategóriákkal és objektumokkal, az eseményekkel, a mentális logikával és a modális logikával, a következtető rendszerekkel, illetve az alapértelmezett információk alapján történő következtetéssel foglalkozik a tizedik fejezet.

A harmadik rész zárásaként, a tizenegyedik fejezetben a fókuszba az automatizált tervekészítés kerül. A fejezet három megközelítés – klasszikus, heurisztikus és hierarchikus – alapján foglalkozik a tervekészítéssel, illetve a klasszikus tervekészítés algoritmusával, a nemdeterminisztikus problémakörben történő tervekészítés és cselekvés kérdéseivel, az idővel, az ütemezéssel, az erőforrásokkal, valamint a tervekészítési megközelítések elemzésével.

Az első három rész, s az első tizenegy fejezet kapott helyet az első kötetben.

A második kötet negyedik része a bizonytalan tudással és a következtetésekkel foglalkozik, s a témát hét fejezetben taglalja.

Elsőként – a tizenkettedik fejezetben – a bizonytalanság számszerűsítési kérdései kerülnek a középpontba. Ennek részeként szó esik a bizonytalanság esetén történő cselekvésről, a valószínűségi jelölésekről, a teljes együttes eloszlásokon alapuló következtetésről, a függetlenségről, a „nagy klasszikusnak” számító Bayes-tételről és annak használatáról, a Naiv Bayes-modellekről, s végül a wumpus világ újragondolásáról.

A tizenharmadik fejezet a valószínűségi következtetésekkel foglalkozik. A fejezet alfejezetei a bizonytalanság esetén történő tudás reprezentálásával, a Bayes-hálók szemantikájával, a Bayes-hálókkal kapcsolatos egzakt, illetve közelítő következtetéssel, valamint az oksági hálókkal foglalkoznak.

Az időbeli valószínűségi következtetés a témája a tizennegyedik fejezetnek, melyben a fontosabb gondolatok az idő és a bizonytalanság, az időbeli modellek, a rejtett Markov-modellek, a Kalman-szűrők, a dinamikus Bayes-hálók fogalmi köré rendeződnek.

A valószínűségi programozás fókusza a tizenötödik fejezetben jelenik meg. A négy alfejezetet tartalmazó fejezet a relációs, illetve a nyílt világ valószínűségi modelljeivel, az összetett világ követésével, s végül a programokkal, mint valószínűségi modellekkel foglalkozik.

A döntéshozatal a témája három fejezetnek, s elsőként az egyszerű döntések meghozataláról olvashatunk a tizenhatodik fejezetben. Az egyszerű döntések meghozatalánál bizonytalanság esetén összekapcsolhatjuk a meggyőződések és kívánságokat, foglalkozhatunk a hasznosságok elméletével, illetve a hasznosságfüggvényekkel, a különböző döntési hálókkal, az információ értékével, illetve az ismeretlen preferenciákkal.

A komplex döntésekről szóló tizenhetedik fejezet öt alfejezetben tárgyalja a témát, s kitér a szekvenciális döntési problémákra, az MDF-ekhez kapcsolódó algoritmusokra, a

rablós problémákra, a részlegesen megfigyelhető Markov döntési folyamatokra, az algoritmusok RMMDF-ek megoldására.

A negyedik részt a többágenses döntéshozattal foglalkozó tizenharmadik fejezet zárja. A fejezet bemutatja a többágenses környezetek tulajdonságait, a kooperatív, illetve nem-kooperatív játékelméletet, valamint a közös döntéshozattal.

A gépi tanulással négy fejezet foglalkozik a második kötet ötödik részében.

A megfigyelések alapján történő tanulásról a tizenkilencedik fejezetben olvashatunk. Ez a fejezet kilenc alfejezetben taglalja a témát, úgymint: a tanulás formái, felügyelt tanulás, döntési fák tanulása, modellszelekció és optimalizálás, a tanulás elmélete, lineáris regresszió és osztályozás, nemparametrikus modellek, együttes tanulás, gépi tanuláson alapuló rendszerek fejlesztése.

Viszonylag rövidebb terjedelemben ismerhetjük meg valószínűségi modellek tanulását a huszadik fejezetben. A fejezet gondolatai a statisztikai tanulás, a teljes adatokkal történő tanulás és a rejtett változókkal történő tanulás köré szerveződnek.

A huszonegyedik fejezet a mélytanulással foglalkozik. A fejezet részletesen ír az egyszerű előrecsatolt hálózatokról, a mélytanulásban alkalmazott számítási gráfokról, a konvolúciós hálózatokról, a tanulóalgoritmusokról, az általánosítóképességről, a visszacsatolt neurális hálózatokról, a nemellenőrzött, illetve transzfertanulásról, valamint a különböző alkalmazásokról.

A gépi tanulási formák közül utolsóként a megerősítéses tanulással ismerkedhetünk meg a huszonegyedik fejezetben. Itt szó esik többek között a jutalmak alapján történő tanulásról, az aktív-, illetve a passzív megerősítéses tanulásról, a megerősítéses tanulás általánosító képességéről, az eljárásmod-keresésről, a gyakornoki tanulásról, az inverz megerősítéses tanulásról, valamint a megerősítéses tanulás alkalmazásáról.

Bár az előző fejezetekben is számos példával, gyakorlati alkalmazással lehetett találkozni, véleményem szerint a kommunikációval, érzékeléssel és cselekvéssel foglalkozó hatodik rész az, amelyik zömében gyakorlati fókuszú, s áttekinti a mesterséges intelligencia fontosabb összefoglaló felhasználási területeit, mint a nyelvfeldolgozás, a látás, illetve a robotika.

A természetesnyelv-feldolgozással két fejezet foglalkozik, az első (huszonharmadik fejezet) a téma részletes alapjait ismerteti, míg a második (huszonegyedik fejezet) a mélytanulásra fókuszál.

A huszonharmadik fejezet kitér a különböző nyelvi modellekre, a nyelvtanra, a szintaktikai elemzésre, a kiterjesztett nyelvtanokra, a valódi természetes nyelvek komplikációira, valamint a természetes nyelvi feladatokra.

Tartalmában e fejezet folytatása a huszonegyedik fejezet, amelyik szóbeágyazásokra, a rekurrens neurális hálókra, a szekvenciális modellekre, a transzformer architektúrára, az előtanításra és transzfertanulásra, illetve a legkorszerűbb módszerek bemutatására fókuszál.

A huszonötödik fejezet a számítógépes látással foglalkozik. A bevezetés után a képalkotással, az egyszerű képjellemzőkkel, a képek osztályozásával, az objektumdetekcióval, a háromdimenziós világgal, valamint a számítógépes látás alkalmazásával ismerkedhetnek meg az érdeklődő olvasók.

A robotikával foglalkozó huszonhatodik fejezet kiter többek között a robotok hardver-fókuszú megközelítésére, az érzékelésre, a bizonytalan mozgások tervezésére, a robotikában alkalmazott megerősítéses tanulásra, az emberek és robotok kapcsolatára, az alternatív robotikai keretrendszerre, s végül az alkalmazási területekre.

Egy mesterséges intelligenciával foglalkozó átfogó mű, mint amilyen Peter Norvig és Stuart J. Russell szerzőpáros *Mesterséges intelligencia modern megközelítésben* című könyve nem lenne teljes, ha a téma klasszikus műszaki-informatikai fejezetei mellett nem jelenének meg a mesterséges intelligencia etikai, filozófiai, alkalmazásának biztonsági kérdéseivel, valamint jövőjével foglalkozó gondolatok. A kétkötetes mű hetedik részében, a *Következtetésekben* ezekről lehet részletesebben olvasni.

A huszonhetedik fejezet a mesterséges intelligencia filozófiai, etikai és biztonsági keretét vázolja fel, bemutatva a mesterséges intelligencia korlátait, etikáját, valamint választ keres arra a kérdésre, hogy a gépek tényleg tudnak-e gondolkodni.

A huszonnyolcadik fejezet a mesterséges intelligencia szerzők által elképzelt jövőjéről szól, s a mesterséges intelligencia komponenseivel, illetve a mesterséges intelligencia architektúrákkal foglalkozik.

Az 1187. oldaltól kezdődően – a Függelékekben – a szerzők alapvető ismereteket adnak a mesterséges intelligenciához kapcsolódó matematikai módszerekről, illetve a nyelvekről és algoritmusokról.

A könyvet egy több mint hatvan oldalas irodalomjegyzék, s végül a tárgymutató zárja.

A KÖTET(EK) KÖNYVÉSZETI ADATAI

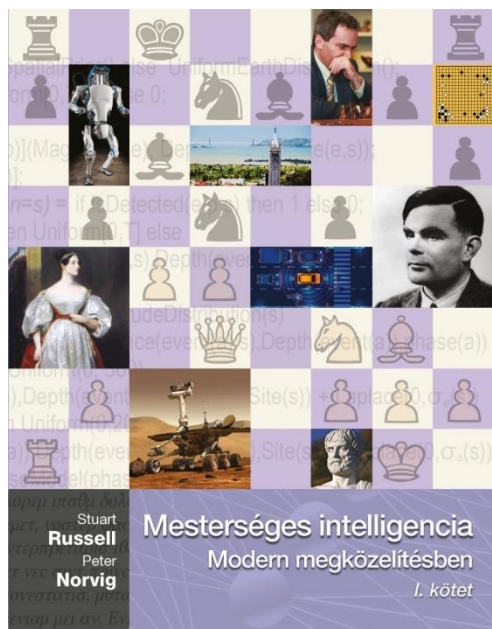
Peter Norvig (1956-) és Stuart J. Russell (1962-) *Mesterséges intelligencia modern megközelítésben*. – Budapest: Panem Kiadó, 2023. 584 p. (első kötet), 864 p. (második kötet) : ill. Bibliogr.: p. 1199-1260. ISBN 978-615-5186-76-9 (első kötet), ISBN 978-615-5186-94-3 (második kötet) (nyomtatott).

Peter Norvig és Stuart J. Russell *Mesterséges intelligencia modern megközelítésben* című kétkötetes könyve a www.panem.hu oldalon keresztül rendelhető meg.

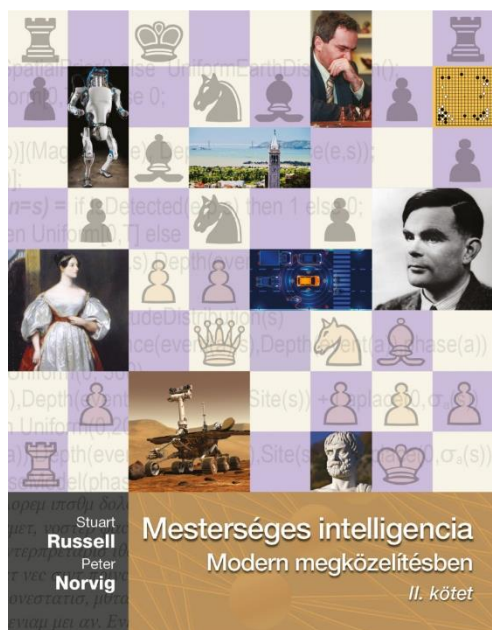
FELHASZNÁLT IRODALOM

- [1] <https://panem.hu/kezdolap/1533-mesterseges-intelligencia-modern-megkoezelitesben-i-koetet.html>
- [2] <http://www.norvig.com>
- [3] <https://people.eecs.berkeley.edu/~russell>

A KÖTET(EK) BORÍTÓJA



1. ábra: Peter Norvig és Stuart J. Russell „Mesterséges intelligencia modern megközelítésben” című könyvének borítója (első kötet)



2. ábra: Peter Norvig és Stuart J. Russell „Mesterséges intelligencia modern megközelítésben” című könyvének borítója (második kötet)

**REVIEW ABOUT THE BOOK
CONFLICT AND PEACE IN
WESTERN SAHARA
BY JÁNOS BESENYŐ**

**RECENZÍÓ BESENYŐ JÁNOS:
KONFLIKTUS ÉS BÉKE A
NYUGAT-SZAHARÁBAN
CÍMŰ KÖNYVÉRŐL**

KUN Tamás¹

INTRODUCTION

The MINURSO is a UN Peacekeeping mission, which dates back to 24 April 1991, the abbreviation comes from the Spanish “*Misión de las Naciones Unidas para la Organización de un Referéndum en el Sáhara Occidental*”. The more than three decades old mission was originally planned for to verify the reduction of Moroccan troops in the Western Sahara.

THE EDITORS BRIEF CAREER PATH

János Besenyő is professor at the Doctoral School on Safety and Security Sciences and Director of the Africa Research Institute at Óbuda University, Hungary. Between 1987 and 2018, he served as a professional soldier and served in several peace operations in Africa and Afghanistan. He received a PhD in military science from Zrínyi Miklós National Defense University (Hungary) and a Habilitation doctorate at Eötvös Loránd University (Hungary). In 2014, he established the Scientific Research Centre of the Hungarian Defence Forces General Staff, and he was its first leader from 2014 to 2018. His most recent publication is Darfur Peacekeepers: The African Union Peacekeeping Mission in Darfur (AMIS) from the Perspective of a Hungarian Military Advisor.

R. Joseph Huddleston is an assistant professor in the School of Diplomacy and International Relations at Seton Hall University. He studies diplomacy by self-determination and secessionist groups, international responses to intrastate conflict, and war economies in protracted social conflicts.

Yahia H. Zoubir is a professor of International Studies and Director of Research in Geopolitics at KEDGE Business School, France. He has published works on the Western Sahara conflict for nearly 35 years, including articles in the Middle East Journal, Middle East Policy, Journal of Modern African Studies, California Western International Law Journal, and others.

THE MAIN EDITOR'S RECENT PUBLICATION ACTIVITY

- Besenyő János: Darfur Peacekeepers - The African Union peacekeeping mission in darfur (AMIS) from the perspective of a Hungarian military advisor, L'Harmattan (Paris)
- Besenyő János: Another Showdown in Western Sahara?, *TERRORISM AND POLITICAL VIOLENCE* 33: (3) pp. 649-656.

¹ kun.tamas@uni-obuda.hu | ORCID: 0000-0002-6620-7157 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz Óbudai Egyetem Biztonságtudományi Doktori Iskola

- Besenyő János: A visegrádi országok Afrika-politikája és részvételük az afrikai békefenntartó műveletekben, KÜLÜGYI SZEMLE 2020/1: pp. 51-79.
- Besenyő János: Magyarország és a nyugat-szaharai válság, Óbudai Egyetem, Biztonságtudományi Doktori iskola; Monarchia Kiadó
- Besenyő János: The Africa Policy of Russia, TERRORISM AND POLITICAL VIOLENCE 31: (1) pp. 132-153.

ABOUT THE CONTENT

Marco Balboni, professor of European Union (EU) and International Law at the University of Bologna, where he is also Coordinator of the Degree in International Relations and Diplomatic Affairs addresses the intro section: *“Introduction: Peacekeeping Operations in Situations of Conflict: The Case of MINURSO”* where he describes the basis of the mission. The main reason for the conflict in the region was the status of the POLISARIO, what Morocco refused to acknowledge.

In the first chapter – *“An Overview of MINURSO: Legal History, Framework, Missions, Structure: A Balance”* – Carlos Ruiz Miguel, professor of Constitutional Law at the University of Santiago de Compostela, starts with a historical background, where the author highlights a few key events which eventually led to the MINURSO. In the following, there is a brief showcase of the legal framework, after that there is a section about the missions (such as the case of the Referendum and the Case-fire between the two belligerent parties, etc.) and the MINURSO structure.

In the second chapter – *“Relevant Events in the MINURSO History”* – Yolanda Blanco Souto, PhD student at the University of Santiago de Compostela, writes about the Mission’s history, where starting from the “Obstructionism” goes through “The Aborted Human Rights Component” section, where in last the author describes how human rights have been systematically abused since the first moment of the occupation until nowadays.

In the third chapter – *“The End of the Western Sahara Peace Process and the Collapse of the UN Ceasefire”* – Jacob Mundy, associate professor of Peace and Conflict Studies and Middle Eastern and Islamic Studies at Colgate University, writes about the road that led to the end of the approximately three decades UN ceasefire between Morocco and the Sahrawi nationalist movement.

In the fourth chapter – *“The Legal Aspects of the Functioning of the UN Mission for the Referendum in Western Sahara”* – Meriem Naïli, PhD candidate in Security, Conflict and Human Rights at the University of Exeter, writes about the political and legal obstacles that affected the mission and about the loopholes in the international human rights law, that has been abused throughout the recent decades.

In the fifth chapter *“Human Rights: MINURSO between a Rock and a Hard Place”* – Toby Shelley, journalist, and author of several books, including *Endgame in the Western Sahara*, writes about how the Sahrawi people lived under Moroccan control and how the MINURSO should have had a role in mediation between the Polisario and the Rabat.

In the sixth chapter – *Participation of Women in the MINURSO: Scope, Evolution, and Factors for the Contribution to the Mission* – María López Belloso, postdoctoral researcher at the University of Deusto, writes a detailed analysis about the role of women in peacekeeping operations, making oppositions with other missions.

In the seventh chapter – “*MINURSO and the Saharawi Archaeological Heritage*” – Elia Quesada, specialist in prehistoric rock paintings, based at the University of Córdoba. and Nick Brooks, co- director of the Western Sahara Archeological Project and visiting research fellow at the School of Environmental Sciences, University of East Anglia, Norwich, are writing about how the 40 years of conflict in the Western Sahara threatens the archeological heritage in the region. These are important in the understanding of past human migration and climate change causes in the Sahara.

In the eighth chapter – “*Building Sandcastles in the Desert? MINURSO Military-Component: Tasks, Duties, and Their Fulfillment*” – Cyprian Aleksander Kozera, expert at the Interdisciplinary Research Centre of the University of Warsaw and Błażej Popławski, researcher at the Polish Africanist Society, have made qualitative research about the military component, a survey done in the Autumn of 2020.

In the ninth chapter – “*The MINURSO Police Contingent*” – János Besenyő, mentioned in editors brief and Marcell György Pintér, researcher at the African Research Institute of the Doctoral School for Safety and Security Sciences of the University of Óbuda, are writing about the police contingent’s role, duties, and challenges through the Mission, as a middle ground between military forces and civilians.

In the tenth chapter – “*Integrated Logistics Support and Financial Issues of the United Nations Mission for the Referendum in Western Sahara (MINURSO)*” – Mirela Atanasiu, senior researcher at the Center for Defense and Security Studies at Carol I National Defence University, writes about the financial and logistical background of the Mission. To provide successful support for the operations, these supply chains must be secure and mobile in order to enhance durability and self-reliance in solving tasks.

In the eleventh chapter – “*Military and Police Experiences from Western Sahara: The Case of Hungary*” – János Besenyő, mentioned in editor’s brief, writes about military and police experiences based on both international and national experiences towards peace-keeping missions supplemented with a comparative analysis conducted by the author.

In the twelfth chapter – “*The United States and MINURSO: 31 Years*” – R. Joseph Huddleston mentioned in editors brief and Edder A. Zarate holds an MA at the School of Diplomacy and International Relations, Seton Hall University, are writing about the historical ties of the US within the region and its role that led to the ceasefire in 1991, furthermore, the relationship of US administrations with Mission throughout its history.

In the thirteenth chapter – “*China and the MINURSO: Eyes on Peak Phosphorus?*” – Csaba Barnabás Horváth, writes about China’s interest in the Mission, its foreign policy focused on the exploit of business opportunities and gaining political influence in the region, mostly over Morocco due to the rock phosphate reserves, which could play a key role in food production in the future.

In the fourteenth chapter – “*Russia and MINURSO: This Is Not Our Conflict*” – Sergey Nikonov, professor and research fellow at St. Petersburg State University and a member of the International Political Research Association (IPSA), writes about Russia’s perspective as an observer, who recognizes the Saharan Arab Democratic Republic based on Algeria’s official recognition. On the other hand, the author describes the “Language Barriers” throughout the Mission.

In the fifteenth chapter – “*France and MINURSO*” – Éva Fábrián, an independent researcher focusing on the security and defense policy of France, especially in the European

and African regions, writes about France's role in the Mission also its ties with the Maghreb states and human right issues regarding to the conflict.

In the sixteenth chapter – “*The Approach of the African States towards MINURSO*” – Dávid Vogel, senior researcher of Doctoral School for Safety and Security Sciences at Óbuda University, Africa Research Institute, , writes about how UN peacekeeping operations are affecting Africa as a whole, moreover the continent's support towards peacekeeping, what describes through the example of the MINURSO.

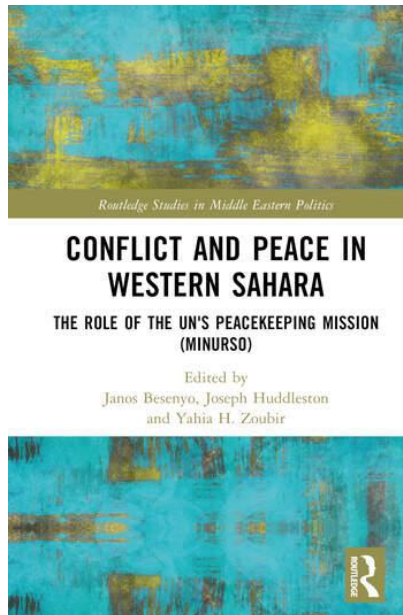
In the seventeenth chapter – “*MINURSO: A Mission for Maintaining the Status Quo?*” – Souadou Lagdaf, associate professor of the History of Islamic countries at the University of Catania and Yahia H. Zoubir, mentioned in editor's brief, are writing about how the MINURSO was a testing ground for UN resolutions, furthermore the conflict between Morocco and the Saharawi people, who seek independence opposing a former colonial power.

In summary, I recommend this book to anyone, who interested in the Western Sahara, African studies, and geopolitics. It is a gap filling volume on its respected field, it discusses nowadays and the defining processes for the future.

THE BOOK'S BIBLIOGRAPHY

János Besenyő (Eds.), R. Joseph Huddleston and Yahia H. Zoubir: *Conflict and Peace in Western Sahara - The Role of the UN's Peacekeeping Mission (MINURSO)* – USA, New York: Routledge, Taylor and Francis Publishing, 2023. - 333 p. ISBN: 978-1-032-25762-4 (hardcover);

THE VOLUME'S COVER



1. ábra: „*Conflict and Peace in Western Sahara*”
 Edited By János Besenyő, R. Joseph Huddleston, Yahia H. Zoubir című könyv borítója.

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>