ISSN 2676-9042

Vol 7, No 1, 2025.

2025, VII. évf. 1. szám

Safety and Security Sciences Review

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

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

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

On the cover can be seen | A borítón
BORS Györgyi
painter/festőművész
In a black box painting | **Fekete dobozban** című festménye látható

The Military Science Committee of the 9th Department of Economics and Law of the Hungarian Academy of Sciences classified our journal as a "C" category.

Folyóiratunkat a Magyar Tudományos Akadémia IX. Gazdaság- és Jogtudományok Osztályának Hadtudományi Bizottsága „C" kategóriás folyóiratnak minősítette.

The Safety and Security Sciences Review is a classified journal by Hungarian Science Bibliography.

A Biztonságtudományi Szemle a Magyar Tudományos Művek Tára (MTMT) által minősített folyóirat.

Our journal is indexed by the following databases

Folyóiratunkat a következő adatbázisok indexelik

EBSCO

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

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

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

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

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

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

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

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

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

The studies of the staff and students of Óbuda University, published in the Journal, are recorded by the staff of the University Library at the Hungarian Scientific Works Library (MTMT).

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

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

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

Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).

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

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

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

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

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

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

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

Vol 7, No 1, 2025. | **2025. VII. évf. 1. szám**

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

AICHAOUI, Nada El Yasmine

nada.aichaoui@phd.uni-obuda.hu

Nada El Yasmine AICHAOUI is a Ph.D. candidate at the Doctoral School on Safety and Security Sciences, Óbuda University. Her research focuses on the development of a control system for safe, collaborative human-robot work in welding applications. She has experience working in robotics labs and has strong expertise in automation engineering, 3D vision optical systems, and control systems. In addition, she is actively engaged in academic research and international collaborations, contributing to advancements in robot safety and industrial automation.

AICHAOUI, Nada El Yasmine az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorjelöltje. Kutatásának középpontjában a hegesztési alkalmazásokban a biztonságos, ember-robot együttműködésre képes vezérlőrendszer fejlesztése áll. Tapasztalatot szerzett robotikai laboratóriumokban, és komoly szaktudással rendelkezik az automatizálási tervezés, a 3D vizuális optikai rendszerek és az irányítási rendszerek területén. Emellett aktívan részt vesz a tudományos kutatásban és nemzetközi együttműködésekben, hozzájárulva a robotbiztonság és az ipari automatizálás terén elért eredményekhez.

BEREK Lajos

berek.lajos@bgk.uni-obuda.hu

Prof. Dr. Lajos BEREK until 2019, he was a professor at Obuda University and the Zrínyi Miklós National Defense University, and since 2019, he has been a professor emeritus at Obuda University. He served as a colonel in the Hungarian Defense Forces between 1972 and 2006. He has been a university lecturer since 1981. He was the dean of the János Bolyai Faculty of Military Engineering at the National Defense University from 2000 to 2007. He was involved in the founding of three doctoral schools. As a university professor, his main areas of expertise are combat and operations of land forces, personal and property security and safety, and troop leadership.

Prof. Dr. BEREK Lajos 2019-ig az Óbudai Egyetem és a Zrínyi Miklós Nemzetvédelmi Egyetem professzora, 2019-től az Óbudai Egyetem pofessor emeritusa. 1972-2006 között a Magyar Honvédségben szolgált ezredesként. 1981-től egyetemi oktató. 2000-2007 a Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar dékánja. Három doktori iskola alapításában közreműködött. Egyetemi tanárként a fő szakterülete a szárazföldi csapatok harca és hadművelete, a személy- és vagyonbiztonság, a csapatok vezetése.

ČOVIĆ, Emili

28224008@vts.su.ac.rs

Emili ČOVIĆ is a Master's student in Information Technology at Subotica Tech – College of Applied Sciences. She earned her BSc degree in Informatics in 2024 from the same institution, obtaining the title of Bachelor of Information Technologies and Systems Engineering - BSc Applied. She was recognized as the Student of the Generation for the 2023/2024 academic year in the Informatics program. Her areas of interest include web programming, computer networks, IoT systems, cybersecurity, animation, and web game development. She has participated in several competitions and European Researchers' Night projects, gaining additional practical experience through several months of internship programs in local IT companies.

ČOVIĆ, Emili a Szabadkai Műszaki Szakfőiskola hallgatója, ahol Információs technológiák mesterképzésen tanul. 2024-ben ugyanitt szerezte meg BSc diplomáját informatikából, és ezzel elnyerte az Információs technológiák és rendszerek mérnöke címet. A 2023/2024-es tanévben az Informatika szakon a generáció hallgatójának választották. Érdeklődési területei közé tartozik a webprogramozás, a számítógépes hálózatok, az IoT rendszerek, a kiberbiztonság, az animáció és a webes játékfejlesztés. Részt vett számos versenyen, valamint az Európai Kutatók Éjszakája projektjeiben is. Helyi IT vállalatoknál végzett több hónapos szakmai gyakorlatok során további értékes gyakorlati tapasztalatot szerzett.

ČOVIĆ, Zlatko

zlatko.covic@uni-obuda.hu

Zlatko ČOVIĆ is a university professor and researcher at the Doctoral School of Safety and Security Sciences at Óbuda University. Additionally, he is a professor and Assistant Director for Public Relations and Student Affairs at Subotica Tech – College of Applied Sciences. He earned his Ph.D. in Information Science and Technology. His primary areas of expertise include web programming, mobile application development, integrated web systems, cybersecurity, and the use of hackathons in engineering education. He successfully collaborates with companies specializing in web programming and the development of integrated web systems. Throughout his career, he has worked on more than 30 web-based projects as both a web programmer and project manager. From 2023, he is an external member of the Hungarian Academy of Sciences.

ČOVIĆ, Zlatko az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának egyetemi oktatója és kutatója. Emellett oktató és a Közkapcsolatokért és Hallgatói Ügyekért Felelős Igazgatóhelyettes a Szabadkai Műszaki Szakfőiskolán. Doktori fokozatát informatika területén szerezte meg. Fő szakterületei közé tartozik a webprogramozás, a mobilalkalmazás-fejlesztés, az integrált webrendszerek, a kiberbiztonság és a hackathonok alkalmazása a mérnöki oktatásban. Sikeresen együttműködik olyan vállalatokkal, amelyek webprogramozással és integrált webrendszerek fejlesztésével foglalkoznak. Pályafutása során több mint 30 webes projektben vett részt webprogramozóként, valamint projektmenedzserként. Számos mobilitási programban vett részt, amelyek során előadásokat tartott. Több tudományos cikk szerzője és társszerzője, amelyeket folyóiratokban publikált és konferenciákon mutatott be. 2023-tól az MTA köztestületének külső tagja.

CZERNY József

czerny@mti.bme.hu

József CZERNY is a chartered civil engineer, corrosion engineer, and facility manager. He founded the first Hungarian facility management training course at the BME Institute of Continuing Engineering Education in 2000, which has been running continuously since then. Since 2004, he has been a member of the Austrian Standards Committee ON 240 Immobilien- und Facility Management. In the mid-2000s, he founded the Hungarian MSZT MB 267 Facility Management Standardization Committee and its predecessor, of which he was also the chairman for a significant period. He is the founding chairman of the Hungarian Facility Management Society established in 2005 and is a member of the Board of Directors at GlobalFM (www.globalfm.org). He has been involved in and led the development of several facilities management curricula, works as a facilities management consultant, and is an international speaker, chairman and organizer of national facilities management conferences.

CZERNY József, okleveles építőmérnök, korróziós szakmérnök, létesítménygazda. A BME Mérnöktovábbképző Intézetben 2000-ben alapította meg az első magyarországi létesítménygazdálkodási képzést, amely azóta is folyamatos. 2004 óta tagja az osztrák Komitee 240 Immobilien- und Facility Management szabványbizottságnak. A 2000-es évek közepén alapította meg a magyar MSZT MB 267 Létesítmény- és vagyongazdálkodás szabványosító bizottságot, ill. annak elődjét, amelynek hosszú ideig elnöke is volt. A 2005-ben megalakult Magyar Létesítménygazdálkodási Szövetség alapító elnöke. A GlobalFM (www.globalfm.org) világszervezet igazgatótanácsának tagja. Számos létesítménygazdálkodási tananyag fejlesztésében vett részt ill. irányította a tananyagok fejlesztését. Létesítménygazdálkodási tanácsadó, nemzetközi előadó, hazai létesítménygazdálkodási konferenciák elnöke, szervezője.

HUSZÁK Csenge

huszak.csenge@bgk.uni-obuda.hu

Csenge HUSZÁK is a departmental engineer at the Department of Materials Technology at the Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering. She obtained her bachelor's degree in mechanical engineering at Óbuda University and continued her studies at the Budapest University

HUSZÁK Csenge az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Karának, Anyagtechnológiai Intézeti Tanszékének egyetemi gyakornoka. Gépészmérnöki alapdiplomáját az Óbudai Egyetemen szerezte, tanulmányait a Budapesti Műszaki és Gazdaságtudományi Egyetemen folytatta. Jelenleg

of Technology and Economics. Currently, she is a student at the Doctoral School of Safety and Security Sciences at Óbuda University. Her research area is metallography and welded structures. During her doctoral research, she is working on developing the requirement system for safety-critical components.

az Óbudai Egyetem Biztonságtudományi Doktori iskolájának hallgatója. Kutatási területe a metallográfia, a hegesztett anyagok és szerkezetek. Doktori kutatása során a biztonságkritikus komponensek követelményrendszerének kidolgozásával foglalkozik.

ILLÉS Mihály

illes.mihaly@bgk.uni-obuda.hu

Mihály ILLÉS is a lecturer at the Donát Bánki Faculty of Mechanical and Safety Engineering of Óbuda University, working as an assistant lecturer. He also holds a degree in safety engineering and electrical engineering. His areas of education: safety technology, information security. In addition to his teaching activities, he is a student at the Doctoral School of Security Sciences of Óbuda University. His research area is the examination of the application of body cameras in railway passenger transport. He has been working in security technology for more than two decades, during which time he has taken an active role in numerous large-scale projects on both the contractor and client side.

ILLÉS Mihály az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar oktatója, egyetemi tanársegéd beosztásban. Okleveles biztonságtechnikai mérnöki és villamosmérnöki diplomával is rendelkezik. Oktatási területei: biztonságtechnika, információbiztonság. Oktatási tevékenysége mellett az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának hallgatója. Kutatási területe a testkamerák vasúti személyszállításban történő alkalmazásának vizsgálata. Biztonságtechnikával több, mint két évtizede foglalkozik, ez idő alatt mind a kivitelezői és megrendelői oldalon számos nagy volumenű projektben vállalt aktív szerepet.

KÁRÁSZ Balázs

karaszb@gmail.com

KÁRÁSZ Balázs (1992) economist in leadership and management, risk management expert. Research topic: role of human factors in the complex approach of information security, especially the development of information security awareness. Former PhD Student of the National University of Public Service, Doctoral School of Military Engineering, currently credit manager at Oberbank AG Hungarian Branch Office.

KÁRÁSZ Balázs (1992) okleveles közgazdász, kockázatkezelési szakértő. Kutatási területe a humán tényezők szerepe az információbiztonság komplex értelmezésében, kiemelten az információbiztonság-tudatosság fejlesztése. A Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola hallgatója volt, jelenleg az Oberbank AG Magyarországi Fióktelep kockázatkezelési hitelmenedzsere.

KISS Csaba

kiss.csaba@uni-nke.hu

Csaba KISS is a doctoral student at the Doctoral School of Military Engineering of the National Public Service University. He completed his studies in the Soviet Union at the Ulyanovsk Military Journalism University, where he graduated in 1986. In the last year of university, he graduated as a Russian military interpreter. During his years of service in the Hungarian Army from 1986 to 1996, he completed a Civil Service Officer course and obtained the "C" type intermediate level language exam with the addition of the military vocational test in German. From 1996, he worked at the Education Directorate of the Hungarian Telecommunications Company (MATÁV) in the Transmission

KISS Csaba a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola doktorandusza. Tanulmányait a Szovjetunióban végezte az Uljanovszki Katonai Híradó Egyetemen, ahol 1986-ban diplomázott. Az egyetem utolsó évében orosz katonai tolmács diplomát szerzett. 1986-tól 1996-ig a Magyar Hadseregben eltöltött szolgálati évek alatt Törzstiszti tanfolyamot végzett és német nyelvből megszerezte a katonai szakmaival bővített “C” típusú középfokú nyelvvizsgát. 1996-tól dolgozott a Magyar Távközlési Vállalat (MATÁV) Oktatási Igazgatóságán a Műszaki Osztály Átviteltechnikai részlegén. A tanári szakképesítés megszerzése után műszaki tárgyakat

Technology Department of the Technical Department. After obtaining his teacher's qualification, he taught technical subjects. In addition to the technical courses, he also obtained a trainer's qualification, so he held various skill-building and team-building trainings. During the trainings, he used his self-developed skills development program for the computer (Octopus-32). In 2010, he won 2nd place with his skills development software in the "smart software" competition at the European level announced by the LUDUS project.

tanított. A műszaki oktatások mellett tréneri képesítést is szerzett így különböző készségfejlesztő, csapatépítő tréningeket tartott. A tréningek során használta a saját fejlesztésű számítógépre írt készségfejlesztő programját (Octopus-32). 2010-ben a LUDUS project által meghirdetett „okos szoftver" európai szintű pályázaton a 2. helyezést érte el a készségfejlesztő szoftverével.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

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

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

KOVÁCS Tünde Anna

kovacs.tunde@bgk.uni-obuda.hu

Prof. Dr Tünde Anna KOVÁCS is a full professor in the Department of Materials Technology at the Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Hungary. Member of the editorial board of the Acta Materialia Transylvania, Safety and Security Sciences Review and Security Engineering of Anthropogenic Objects. Her research interests are in materials science and technologies, as well as unique welding processes (ultrasonic and explosive welding). She is an International Welder Engineer (IWE),

Prof. Dr. KOVÁCS Tünde Anna az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Karának, Anyagtechnológiai Intézeti Tanszékének egyetemi tanára. Tagja az Acta Materialia Transylvania, a Biztonságtudományi Szemle, az Antropogén Objektumok Mérnöki Biztonsága folyóiratok szerkesztő bizottságának. Kutatási területe az anyagtudomány és technológia területén a különleges hegesztési eljárások (ultrahangos és robbantásos hegesztés), nemzetközi hegesztőmérnökként (IWE), hegesztő robotok

welder robots and collaborative welding robotics. She is a supervisor in the Doctoral School on Materials and Technologies of the Óbuda University and the Doctoral School on Safety and Security Sciences, Hungary. Author and co-author of numerous scientific publications. Member in several research projects and supervisor of doctoral students.

és collaborative robothegesztés. Témavezetőként dolgozik az Anyagtudományok és Technológiák, valamint a Biztonságtudományi Doktori iskoláknál. Számos tudományos publikáció szerzője és társszerzője. Tagja kutatási projekteknek és doktori témák témavezetője.

KURMAY Sándor

kurmay.sandor@uni-obuda.hu

Sándor KURMAY, physicist and physics teacher, graduated from the nuclear physics department of Uzhgorod State University. He wrote his thesis on the study of electron-positron pairings. After graduating from university, he taught physics at Bethlen Gábor Hungarian High School in Beregszász, and then worked as the head of a foundation. In 2023, he was admitted to Doctoral School of Security Sciences of Óbuda University. The title of his research topic: "Improving the operational safety of nuclear energy facilities, considering the presence of external threats".

KURMAY Sándor fizikus, fizikatanár szakpáron végzett az Ungvári Állami Egyetem magfizikai tanszékén. Diplomamunkáját az elektron-pozitron párkeltések tanulmányozásából írta. Az egyetem elvégzése után fizikát tanított a Beregszászi Bethlen Gábor Magyar Gimnázium, majd egy alapítvány vezetőjeként tevékenykedett. 2023-ban nyert felvételt az Óbudai Egyetem Biztonságtudományi Doktori Iskolájába. Kutatási témájának címe: „Nukleáris energetikai létesítmények üzembiztonságának fejlesztése, a külső fenyegetettség tükrében".

MÁRTON Zoltán

marton.zoltan@uni-obuda.hu

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

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

MICHELBERGER Pál

michelberger.pal@bgk.uni-obuda.hu

Pál MICHELBERGER has been full professor at the Institute of Safety Science and Cybersecurity, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, Hungary. He has received his M.Sc. degree in Mechanical and Industrial Engineering from the Technical University of Budapest (1988 & 1997) and

Dr. MICHELBERGER Pál, egyetemi tanár az Óbudai Egyetem, Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Karán, a Biztonságtudományi és Kibervédelmi Intézetében. 1988-ban gépészmérnöki, 1997-ben pedig integrált menedzser-gazdasági mérnöki oklevelet szerzett a Budapesti Műszaki Egye-

Ph.D. degree from the Ph.D. Institute of Military Technology of Miklós Zrínyi National Defence University, Hungary (2005). His Ph.D. thesis deals with the selection and implementation of information system elements for purposes of national defence. He has more than ten years practice at different Hungarian industrial companies in area of IT and production management. He has been teaching at various Hungarian higher education institutions since 1997. Currently, he participates in the work of the Óbuda University Doctoral School on Safety and Security Sciences as a core member, supervisor and lecturer. His research interests are project management at implementation of business IT solutions and development of ISO management systems.

tem Gépészmérnöki Karán. Doktori (PhD) fokozatát a Zrínyi Miklós Nemzetvédelmi Egyetemen kapta katonai műszaki tudományokból 2005-ben. 2015-ben az Óbudai Egyetemen habilitált. Több mint 10 év iparvállalati gyakorlat után 2001-ben kezdett el a felsőoktatásban dolgozni. Volt a Gábor Dénes Főiskola, a Pannon Egyetem és Budapesti Műszaki Főiskola oktatója is. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola munkájában is közreműködik törzstagként, témavezetőként és tantárgyfelelős oktatóként. Szakmai érdeklődése és kutatásai a projektmenedzsmenthez, valamint a szabványos irányítási (minőség-, környezet-, információbiztonsági-) rendszerek kialakításához köthető.

NAGY Rudolf

nagy.rudolf@uni-obuda.hu

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

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

PAPP Zoltán

zoltan.papp@magister.uns.ac.rs

Zoltán PAPP is an associate professor at the Hungarian Language Teacher Training Faculty of the University of Novi Sad. Additionally, he is a lecturer at the Subotica Tech - College of Applied Sciences and an associate professor at the Institute of Informatics at the University of Dunaújváros, Department of Mathematics and Computer Science. He obtained his Ph.D. in mathematics in 2019. His main research areas include numerical optimization, numerical solutions of nonlinear systems of equations, solving nonlinear complementarity problems, and statistics. He has participated in several mobility programs during which he has given lectures. He is the author and co-author of numerous scientific articles published in journals and presented at conferences. He is also an external member of the public body of the Hungarian Academy of Sciences.

PAPP Zoltán az Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Karának docense, emellett a Szabadkai Műszaki Szakfőiskola oktatója és a Dunaújvárosi Egyetem Informatikai Intézetének Matematika és Számítástudományi Tanszékének egyetemi docense. Doktori fokozatát matematika területen szerezte 2019-ben. Kutatási területei közé tartozik a numerikus optimalizáció, a nemlineáris egyenletrendszerek numerikus megoldása, a nemlineáris komplementaritási problémák megoldása és a statisztika. Több mobilitási programban vett részt, amely során előadásokat tartott. Számos tudományos cikk szerzője és társszerzője, amelyeket folyóiratokban publikált és konferenciákon mutatott be. A Magyar Tudományos Akadémia köztestületének külső tagja.

PINKE Péter

pinke.peter@bgk.uni-obuda.hu

Dr. Péter PINKE is an associate professor in the Department of Materials Technology at the Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Hungary. Member of the editorial board of the Acta Materialia Transylvanica. His scientific activities focus on materials science, physical metallurgy and the investigation of the limit states of materials. He has participated in several scientific research projects aimed at the investigation of the properties of steels and non-ferrous alloys. His areas of expertise include heat treatment, mechanical material testing, and the investigation of the microstructure of metals and alloys. He is a supervisor in the Doctoral School on Materials and Technologies of the Óbuda University and the Doctoral School on Safety and Security Sciences, Hungary.

Dr. PINKE Péter az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Karának, Anyagtechnológiai Intézeti Tanszékének egyetemi docense. Tagja az Acta Materialia Transylvanica folyóirat szerkesztő bizottságának. Tudományos tevékenysége az anyagtudományra, a fizikai metallurgiára és az anyagok határállapotainak vizsgálatára fókuszál. Több tudományos kutatásban is részt vett, amelyek acélok és nemvasfém ötvözetek tulajdonságvizsgálatára irányultak. Szakterülete a hőkezelés, a mechanikai anyagvizsgálatok, valamint fémek és ötvözetek mikroszerkezetének vizsgálata. Témavezetőként dolgozik az Anyagtudományok és Technológiák, valamint a Biztonságtudományi Doktori iskoláknál.

RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

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

Prof. Dr. RAJNAI Zoltán Magyarország nemzeti kiberkoordinátora, az Óbudai Egyetem professzora, 2015-tól az Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karának dékánja. A Biztonságtudományi Doktori Iskola alapítója, vezetője, kutatási területe a kiberbiztonság, az információbiztonság, az infokommunikáció és a távközlési rendszerek fejlesztése. Korábban (1981–2013) ezredesként szolgált a Magyar Honvédségben, 1993–2013 között a Zrínyi Miklós Nemzetvédelmi Egyetem tanáraként fő szakterülete az információs, kommunikációs és távközlési rendszerek szervezése és azok biztonsága volt. Rajnai professzor a katonai főiskolai és egyetemi tanulmányait követően a Hadtudományi Doktori Iskolában (1997–2000) és a párizsi Összhaderőnemi Védelmi Kollégiumban (CollègeInterarmées de Défense – CID) tanult.

SOMOGYI Tamás

somogyi.tamas@phd.uni-obuda.hu

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

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

SZŰCS Endre

szucs.endre@bgk.uni-obuda.hu

Dr. Endre SZŰCS is a supervisor at the Doctoral School of Security Sciences at Óbuda University. He earned his PhD in Military Sciences from Zrínyi Miklós National Defence University in 2006. His research discipline is military engineering, with a focus on the possibilities of applying renewable energy sources in safety technology, as well as the history of safety technology. Several of his doctoral students have already obtained their degrees, some are actively participating in ongoing doctoral research, and others are in the process of completing their absolutory degree.

Dr. SZŰCS Endre az Óbudai Egyetem Biztonságtudományi Doktori Iskola témavezetője. Tudományos, PhD fokozatát a Zrínyi Miklós Nemzetvédelmi Egyetemen, hadtudományok tudományágon szerezte 2006-ban. Kutatásainak tudományága a katonai műszaki tudomány. Kutatási területe: a megújuló energiaforrások alkalmazásának lehetőségei a biztonságtechnikában és a biztonságtechnika története. Témavezetettjei közül többen már fokozatot szereztek, a jelenlegiek közül egy részük folyamatban lévő doktori cselekményekben vesz részt, mások az abszolutórium megszerzése előtt járnak.

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 szóljanak valamiről, egy érzésről, egy gondolatról, egy benyomásról, vagy akár egy emberi tulajdonságról. Az absztrakt festészet eszközeit felhasználva alkot. Innovatív stílusával olyan tapasztalatokat, érzéseket és gondolatokat emel a festészet eszközeivel egyetemes szintre, melyeket mindnyájan ismerünk vagy megéltünk már valamilyen formában. Munkái sikeresen szerepeltek különféle hazai és nemzetközi versenyeken és kiállításokon. (Budapest, London, New Jersey, Hong Kong) Több kortárs művészeti albumban, art magazinban jelentek meg munkái. Egyik alkotása a Magyar Cirkuszművészeti Múzeum közgyűjteményében is megtalálható. Kifejezésmódja a geometriai- és lírai absztrakt, melyek egymás mellett, de mégis szervesen összefonódva erősítik művészetét.

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

Vol 7, No 1, 2025. | 2025. VII. évf. 1. szám

CONTENT | TARTALOM

DOI: https://doi.org/10.12700/btsz.2025.7.1.1

AI-Driven Control System for Safe and Adaptive Human-Robot Collaboration in Welding Applications

AI-támogatott vezérlőrendszer a biztonságos és adaptív ember--robot együttműködéshez hegesztési alkalmazásokban

AICHAOUI Nada El Yasmine[1] – KOVÁCS Tünde Anna[2]

Abstract

The study presents a system to support safe collaboration in a human-robot welding environment. The welding parameters change dynamically according to the evaluation of real-time sensed environmental data by an artificial intelligence algorithm. The system follows the movement of the human working in a collaborative environment, takes into account the UV danger zone and integrates the welding robot's operation. Simulations show that the system effectively minimises risks without compromising weld quality. The algorithm developed aims to reduce the risk of human-robot collaboration in the field of occupational health and safety by evaluating real-time environmental data with AI support, while meeting the quality requirements of welding. Currently, it can't find a similar innovation with the presented AI-supported system in the welding industry.

Keywords

Welding Robotics, Collaborative Environment, Real-time Sensor, Artificial Intelligence (AI), Risk Assessment, UV Zone

Absztrakt

Az ember-robot hegesztési környezetben történő biztonságos együttműködést támogató rendszert mutat be a tanulmány. A hegesztési paraméterek dinamikusan változnak a valós időben érzékelt környezeti adatok mesterséges intelligencia algoritmus értékelése és szerint. A rendszer követi a kollaboratív környezetben dolgozó ember mozgását figyelembe veszi az UV veszélyzónát és ehhez integrálja a hegesztő robot működését. Szimulációk igazolják, hogy a rendszer hatékonyan minimalizálja a kockázatokat a hegesztés minőség romlása nélkül. A kifejlesztett algoritmus a human-robot együttműködés munkavédelmi kockázatát kívánja csökkenteni a valós idejű környezeti adatok AI támogatással történő értékelése alapján a hegesztés minőségi követelményeinek kielégítése mellett. Jelenleg a hegesztési ipari gyakorlatban még nem található a bemutatott fejlesztéshez hasonló AI támogatott rendszer.

Kulcsszavak

Robotos hegesztés, kollaboratív környezet, valós idejű érzékelő, mesterséges intelligencia (AI), kockázatértékelés, UV zóna

[1] nada.aichaoui@phd.uni-obuda.hu | ORCID: 0009-0008-4361-675X | PhD candidate, Doctoral School on Safety and Security Sciences, Óbuda University | PhD hallgató, Biztonságtudományi Doktori Iskola, Óbudai Egyetem

[2] kovacs.tunde@bgk.uni-obuda.hul | ORCID: 0000-0002-5867-5882 | professor, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University | egyetemi tanár, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem

INTRODUCTION

The welding robot has control systems that reflect a significant evolution toward advanced automation and precision [1]. Traditional control systems relied heavily on predefined trajectories and fixed parameters, limiting their adaptability to variations in welding conditions and workpiece geometries [2], [3]. This approach, while functional in controlled environments, often fell short when faced with unpredictable factors or complex shapes, highlighting the limitations in addressing diverse industrial needs [3], [4]. Consequently, the current state of welding technology lacks extensive integration of advanced algorithms for optimizing parameters and identifying defects, which is evident from limited accessible information and practical implementation gaps [5], [6].

However, recent advancements have revolutionized this landscape [7]. Modern welding robot control systems incorporate sophisticated sensor technologies such as vision systems, laser scanners, and force/torque sensors, enabling real-time feedback and adaptive control [8], [9], [10]. These systems leverage advanced algorithms, including machine learning and artificial intelligence [11], [12], to optimize welding parameters and trajectories dynamically. Such adaptability ensures that welding processes are not only precise but also resilient to variations in environmental and operational conditions [13], [14]. Furthermore, cobots with advanced safety features have emerged as a prominent trend, allowing for human-robot collaboration in welding tasks [15], [16], [17]. These cobots are equipped with sensors and safety protocols that minimize risks and enhance productivity, making them increasingly viable for tasks requiring human oversight or intervention [12].

Overall, the current state-of-the-art of welding robot control systems emphasizes flexibility, efficiency, and quality, paving the way for increased productivity and competitiveness in industries reliant on welding technology [18]. The integration of adaptive algorithms, real-time feedback, and collaborative capabilities ensures that welding processes are not only efficient but also safe and reliable, setting a new standard for automation in this domain [19], [20].

This paper will outline the simulation environment used, describe the modeling of the welding process, and provide an analysis of safety testing. The results from the simulations serve as an initial validation of the control system's performance, offering insights into its real-world applicability and identifying areas for further optimization. By providing a foundation for testing safety and collaborative workflows, simulation ensures the robustness and reliability of the control system before it is introduced into industrial welding applications.

Integrative Control with Operator Interaction and Safety

The current state of welding technology still lacks significant incorporation of advanced algorithms for optimizing parameters and detecting defects, as evidenced by the limited amount of readily available information [21], [22]. However, recent advancements have shown promising progress in harnessing neural networks to automate these processes, even though such developments are still in the early stages [23], [24], [25]. These advancements aim to improve the precision and efficiency of welding operations while reducing human intervention and error [26].

One of the primary goals in this field is to gain a deeper understanding on how welding robots operate, especially in scenarios where an object, often a person, accidentally

enters the robot's hazardous zone during its work as shown in Figure 1. This understanding is essential to ensure both safety and productivity in industrial settings. In typical situations, the main risks emerge when humans approach the robot's danger zones while it is actively functioning. This underscores the need for a thorough comprehension of the robot's response mechanisms and the application of effective safety protocols to avoid accidents and injuries.

In industrial welding environments, the danger zone is often defined by the spread of ultraviolet (UV) radiation emitted during the welding process [27]. This radiation poses serious health risks to humans, particularly with prolonged exposure, and can lead to severe harm if safety measures are not properly enforced [28], [29]. A critical challenge occurs when a person inadvertently enters the robot's hazardous UV zone during operation. While stopping the robot immediately can prevent harm, it may also interrupt vital welding tasks, causing production delays or material waste.

To address this issue, the following study proposes the development of an intelligent control system designed to prioritize human safety while enabling adaptive decision-making. This system will assess risks in real-time and make decisions that balance the need for safety with the demands of the welding process. By integrating advanced technologies and algorithms, the solution aims to create safer, more efficient industrial environments that can respond dynamically to potential hazards without compromising productivity.

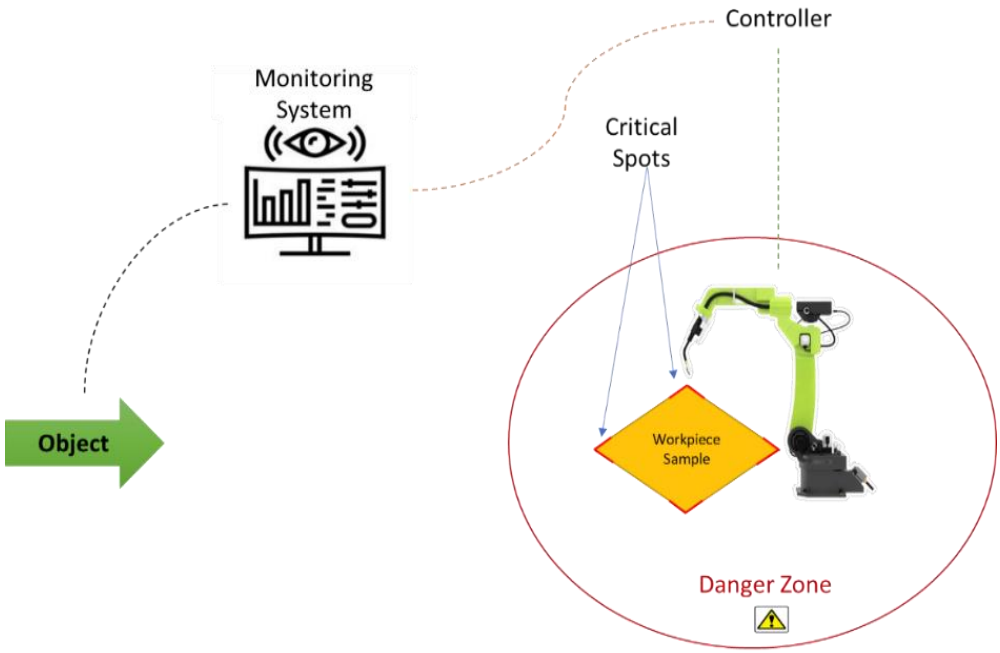


Figure 1. The general implementation of an object approaching to welding robot danger zone.

The implementation of the safety and quality requirement should pass as the flowchart in Figure 2 , where this system starts when a human comes closer to the danger zone, the monitoring system shall detect this action and provide an immediate response relative to the welding robot control system

The proposed system detects human presence in the UV zone of the welding robot, assesses the risk associated with the presence, and makes an intelligent decision based on the risk level and the stage of the welding process. The general scenario follows these steps:

- **Human Detection:** The system detects when a human accidentally enters the dangerous UV zone.
- **Risk Assessment:** The AI system evaluates the risk to human health:
  - If the risk level is unacceptable, the welding robot is immediately stopped, and the human is instructed to exit the zone, and for the next step and because the welding status in this case is unknown, it is necessary to relaunch or resume the process manually by human-operator who cooperate to evaluate the operated sample.
  - If the risk level is acceptable, the system further evaluates the welding process.
- **Welding Process Evaluation:**
  - If the robot is working at a normal point in the welding process (where stopping the process does not affect the quality), the robot is stopped, and the human is instructed to exit, in this case, since the workpiece is in known status, the next step, the robot will relaunch or resume the process automatically.
  - If the robot is working at a critical point (where stopping the process could damage the sample), the robot continues welding. Simultaneously, warnings are issued to the human.
- **Timeout Mechanism:**

If the human exits the UV zone before a preset timeout, the welding continues, and the robot moves to the next operation after finishing the current one.

If the human remains in the zone beyond the timeout, the AI reassesses the risk level. If the risk level becomes unacceptable, the robot is stopped. If it remains acceptable, the robot continues the welding process.

The following presented workflow in 2. Figure ensures that safety protocols are followed while minimizing downtime or wastage during critical welding operations. The behavior of this workflow was modeled using Python. The scenarios outlined in the research were implemented as follows:

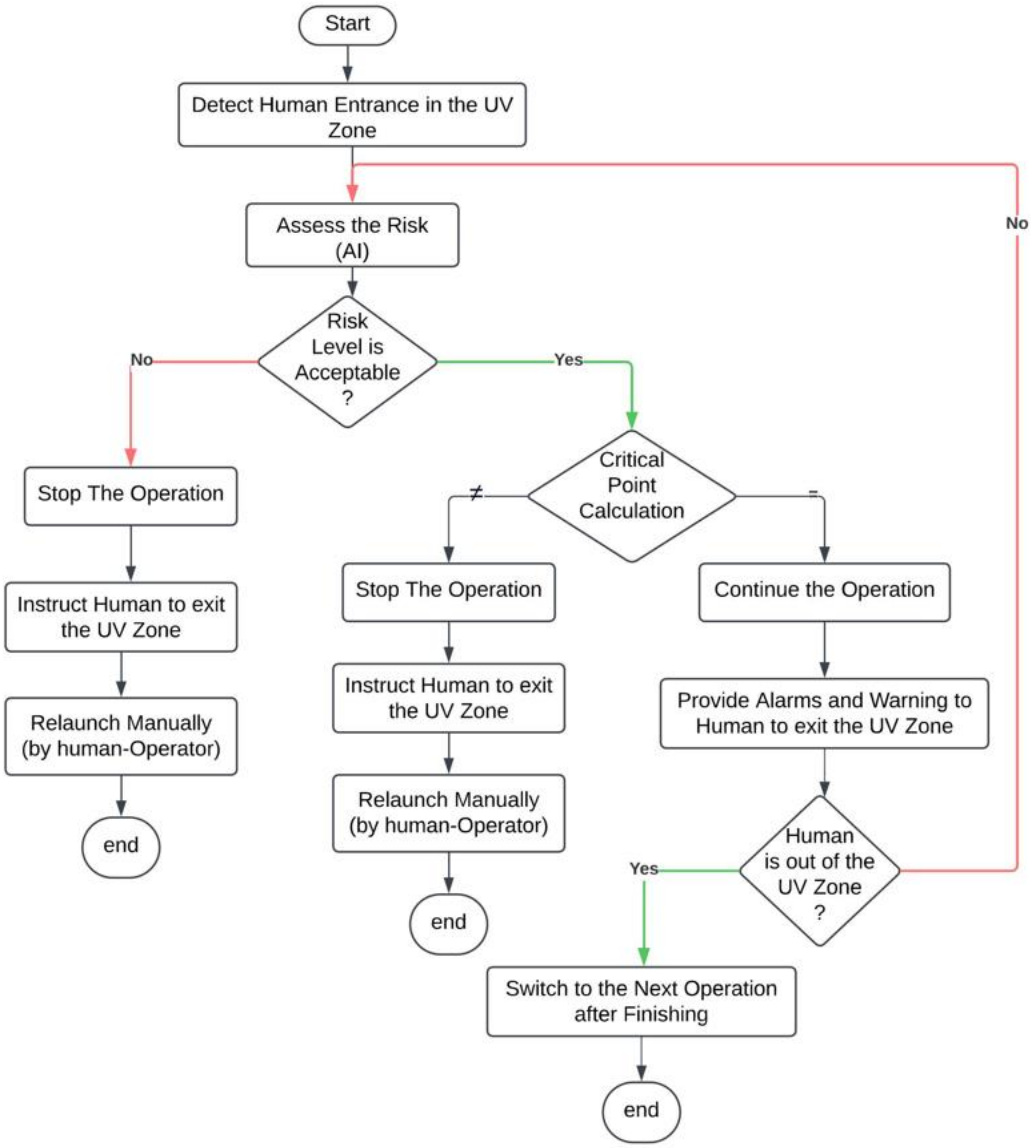


Figure 2. Workflow for Safety Control in Human-Robot Collaborative Welding Environments

The behavior of this workflow was modeled using Python. The four scenarios outlined in the research were implemented as follows:

1. **Scenario 1:** The system detects a human, assesses an unacceptable risk level, and immediately stops the welding robot. The human is instructed to exit the UV zone, and the system waits for manual relaunch. The script is as follows in Figure 3 and the result of the simulation appears in Figure 4:

```python
#Python Code Scenaio 1:
def detect_human_entry():
    # Simulate detection of human entry in the UV zone : Return True if human is detected, False otherwise.
    return True  # Human is detected
def assess_risk():
    # Simulate AI assessing the risk level : Return True if risk level is acceptable, False otherwise.
    return False  # Risk level is not acceptable
def determine_welding_point():
    # Simulate determining if the welding point is normal or critical : Return True if welding at a normal point, False if at a critical point.
    return True  # This function will not be called in this scenario
def does_human_exit_before_timeout():
    # Simulate checking if the human exits the UV zone before timeout : Return True if human exits before timeout, False otherwise.
    return True  # This function will not be called in this scenario
def continue_welding():
    # Simulate continuing the welding operation.
    print("Welding continues.")  # This function will not be called in this scenario
def send_stop_signal():
    # Simulate sending a stop signal to the robot.
    print("Stop signal sent to the robot.")
def instruct_human_to_exit():
    # Simulate instructing the human to exit the UV zone.
    print("Human instructed to exit UV zone.")
def wait_for_manual_relaunch():
    # Simulate waiting for manual relaunch of the robot.
    print("Waiting for manual relaunch.")
def wait_for_automatic_relaunch():
    # Simulate waiting for automatic relaunch of the robot.
    print("Waiting for automatic relaunch.")
def switch_to_next_operation():
    # Simulate switching to the next operation after finishing.
    print("switching to the next opperation after finishing")
def reassess_risk():
    # Simulate AI reassessing the risk level.
    print("Reassess the risk.")
def main():
    # Start of the workflow
    print("Workflow started.")
    if detect_human_entry():
        if not assess_risk():  # Risk level is not acceptable
            send_stop_signal()
            instruct_human_to_exit()
            wait_for_manual_relaunch()
        else:  # Risk level is acceptable
            if determine_welding_point():  # Welding at a normal point
                send_stop_signal()
                instruct_human_to_exit()
                wait_for_manual_relaunch()
            else:  # Welding at a critical point
                continue_welding()
                if does_human_exit_before_timeout():  # Human exited before timeout
                    continue_welding()
                else:  # Human did not exit before timeout, reassess risk level
                    if not assess_risk():  # Risk level is not acceptable after reassessment
                        send_stop_signal()
                        instruct_human_to_exit()
                        wait_for_manual_relaunch()
                    else:  # Risk level is acceptable after reassessment
                        continue_welding()
if __name__ == "__main__":
    main()
```

Figure 3. Python Script of Scenario 1

```
Workflow started.
Stop signal sent to the robot.
Human instructed to exit UV zone.
Waiting for manual relaunch.
```

Figure 4. Scenario 1 Response Result

2. **Scenario 2:** The system detects a human, assesses an acceptable risk level, and detects that the robot is working at a normal point (Figure 5). The robot is stopped, and the human is instructed to exit. The system then waits for automatic relaunch (Figure 6).

```python
#Python Code Scenaio 2:
def detect_human_entry():
    # Simulate detection of human entry in the UV zone: Return True if human is detected, False otherwise.
    return True  # Human is detected
def assess_risk():
    # Simulate AI assessing the risk level : Return True if risk level is acceptable, False otherwise.
    return True  # Risk level is acceptable
def determine_welding_point():
    # Simulate determining if the welding point is normal or critical : Return True if welding at a normal point, False if at a critical point.
    return True  # Welding at a normal point
def does_human_exit_before_timeout():
    # Simulate checking if the human exits the UV zone before timeout : Return True if human exits before timeout, False otherwise.
    return True  # This function will not be called in this scenario
def continue_welding():
    # Simulate continuing the welding operation.
    print("Welding continues.")  # This function will not be called in this scenario
def send_stop_signal():
    # Simulate sending a stop signal to the robot.
    print("Stop signal sent to the robot.")
def instruct_human_to_exit():
    # Simulate instructing the human to exit the UV zone.
    print("Human instructed to exit UV zone.")
def wait_for_manual_relaunch():
    # Simulate waiting for manual relaunch of the robot.
    print("Waiting for manual relaunch.")
def wait_for_automatic_relaunch():
    # Simulate waiting for automatic relaunch of the robot.
    print("Waiting for automatic relaunch.")
def switch_to_next_operation():
    # Simulate switching to the next operation after finishing.
    print("switching to the next opperation after finishing")
def reassess_risk():
    # Simulate AI reassessing the risk level.
    print("Reassess the risk.")
def main():
    # Start of the workflow
    print("Workflow started.")
        if detect_human_entry():
        if not assess_risk(): # Risk level is not acceptable
            send_stop_signal()
            instruct_human_to_exit()
            wait_for_manual_relaunch()
        else # Risk level is acceptable
            if determine_welding_point(): # Welding at a normal point
                send_stop_signal()
                instruct_human_to_exit()
                wait_for_automatic_relaunch()
            else: # Welding at a critical point
                continue_welding()
                if does_human_exit_before_timeout(): # Human exited before timeout
                    continue_welding()
                else: # Human did not exit before timeout, reassess risk level
                    if not assess_risk(): # Risk level is not acceptable after reassessment
                        send_stop_signal()
                        instruct_human_to_exit()
                        wait_for_manual_relaunch()
                    else: # Risk level is acceptable after reassessment
                        continue_welding()
if __name__ == "__main__":
    main()
```

Figure 5. Python Script of Scenario 2

```
Workflow started.
Stop signal sent to the robot.
Human instructed to exit UV zone.
Waiting for automatic relaunch.
```

Figure 6. Scenario 2 Response Result

3. **Scenario 3**: The system detects a human, assesses an acceptable risk level, and detects that the robot is working at a critical point (Figure 7). The robot continues working while warning the human. If the human exits the zone before the timeout, the robot continues welding (Figure 8).

```python
#Python Code Scenaio 3:
def detect_human_entry():
    # Simulate detection of human entry in the UV zone : Return True if human is detected, False otherwise.
    return True  # Human is detected
def assess_risk():
    # Simulate AI assessing the risk level : Return True if risk level is acceptable, False otherwise.
    return True  # Risk level is acceptable
def determine_welding_point():
    # Simulate determining if the welding point is normal or critical : # Return True if welding at a normal point, False if at a critical point.
    return False  # Welding at a critical point
def does_human_exit_before_timeout():
    # Simulate checking if the human exits the UV zone before timeout : Return True if human exits before timeout, False otherwise.
    return True  # Human exits before timeout
def continue_welding():
    # Simulate continuing the welding operation.
    print("Welding continues.")
def send_stop_signal():
    # Simulate sending a stop signal to the robot.
    print("Stop signal sent to the robot.")
def instruct_human_to_exit():
    # Simulate instructing the human to exit the UV zone.
    print("Human instructed to exit UV zone.")
def wait_for_manual_relaunch():
    # Simulate waiting for manual relaunch of the robot.
    print("Waiting for manual relaunch.")
def wait_for_automatic_relaunch():
    # Simulate waiting for automatic relaunch of the robot.
    print("Waiting for automatic relaunch.")
def switch_to_next_operation():
    # Simulate switching to the next operation after finishing.
    print("switching to the next opperation after finishing")
def reassess_risk():
    # Simulate AI reassessing the risk level.
    print("Reassess the risk.")
def main():
    # Start of the workflow
    print("Workflow started.")
    if detect_human_entry():
        if not assess_risk(): # Risk level is not acceptable
            send_stop_signal()
            instruct_human_to_exit()
            wait_for_manual_relaunch()
        else: # Risk level is acceptable
            if determine_welding_point(): # Welding at a normal point
                send_stop_signal()
                instruct_human_to_exit()
                wait_for_manual_relaunch()
            else: # Welding at a critical point
                continue_welding()
                if does_human_exit_before_timeout(): # Human exited before timeout
                    instruct_human_to_exit()
                    switch_to_next_operation()
                else: # Human did not exit before timeout, reassess risk level
                    if not assess_risk(): # Risk level is not acceptable after reassessment
                        send_stop_signal()
                        instruct_human_to_exit()
                        wait_for_manual_relaunch()
                    else: # Risk level is acceptable after reassessment
                        continue_welding()
if __name__ == "__main__":
    main()
```

Figure 7. Python Script of Scenario 3

```
Workflow started.
Welding continues.
Human instructed to exit UV zone.
switching to the next operation after finishing
```

Figure 8. Scenario 3 Response Result

4. **Scenario 4**: The system detects a human, assesses an acceptable risk level, and detects that the robot is working at a critical point. Human do not exist before the timeout (Figure 9), triggering a reassessment of the risk. If the risk becomes unacceptable, the robot is stopped; otherwise, it continues welding (Figure 10).

```python
#Python Code Scenaio 4:
def detect_human_entry():
    # Simulate detection of human entry in the UV zone : Return True if human is detected, False otherwise.
    return True  # Human is detected
def assess_risk():
    # Simulate AI assessing the risk level : Return True if risk level is acceptable, False otherwise.
    return True  # Initial risk level is acceptable
def determine_welding_point():
    # Simulate determining if the welding point is normal or critical : Return True if welding at a normal point, False if at a critical point.
    return False  # Welding at a critical point
def does_human_exit_before_timeout():
    # Simulate checking if the human exits the UV zone before timeout : Return True if human exits before timeout, False otherwise.
    return False  # Human does not exit before timeout
def continue_welding():
    # Simulate continuing the welding operation.
    print("Welding continues.")
def send_stop_signal():
    # Simulate sending a stop signal to the robot.
    print("Stop signal sent to the robot.")
def instruct_human_to_exit():
    # Simulate instructing the human to exit the UV zone.
    print("Human instructed to exit UV zone.")
def wait_for_manual_relaunch():
    # Simulate waiting for manual relaunch of the robot.
    print("Waiting for manual relaunch.")
def wait_for_automatic_relaunch():
    # Simulate waiting for automatic relaunch of the robot.
    print("Waiting for automatic relaunch.")
def switch_to_next_operation():
    # Simulate switching to the next operation after finishing.
    print("switching to the next opperation after finishing")
def reassess_risk():
    # Simulate AI reassessing the risk level.
    print("Reassess the risk.")
def main():
    # Start of the workflow
    print("Workflow started.")
    if detect_human_entry():
        if not assess_risk(): # Initial risk level is not acceptable
            send_stop_signal()
            instruct_human_to_exit()
            wait_for_manual_relaunch()
        else: # Initial risk level is acceptable
            if determine_welding_point(): # Welding at a normal point
                send_stop_signal()
                instruct_human_to_exit()
                wait_for_manual_relaunch()
            else: # Welding at a critical point
                continue_welding()
                if does_human_exit_before_timeout(): # Human exited before timeout
                    continue_welding()
                else: # Human did not exit before timeout, reassess risk level
                    if not reassess_risk(): # Risk level is not acceptable after reassessment
                        send_stop_signal()
                        instruct_human_to_exit()
                        wait_for_manual_relaunch()
                    else: # Risk level is acceptable after reassessment
                        continue_welding()
if __name__ == "__main__":
    main()
```

Figure 9. Python Script of Scenario 4

```
Workflow started.
Welding continues.
Reassess the risk.
Stop signal sent to the robot.
Human instructed to exit UV zone.
Waiting for manual relaunch.
```

Figure 10. Scenario 4 Response Result

The Python code for each scenario handles the decision-making logic using conditional checks, simulating the workflow discussed above. The system's operations depend on the real-time input from sensors (simulated in code) and the intelligent assessment by the AI module. Below is a brief explanation of the key components:

- **detect_human_entry():** Simulates the sensor detecting a human entering the UV zone.
- **assess_risk() / reassess_risk():** Simulates the AI evaluating the risk level based on various factors such as distance and exposure.
- determine_welding_point(): Identifies if the welding operation is at a critical or normal stage.
- **does_human_exit_before_timeout():** Simulates the system waiting for the human to exit the dangerous zone.
- **continue_welding() / send_stop_signal() / instruct_human_to_exit():** Functions that simulate the actual responses of the system based on the situation.

This simulation code ensures that all the potential scenarios are covered, where either the system stops the robot for safety reasons or continues the welding process when it is safe to do so.

Results

The safety control system successfully demonstrates a flexible and robust decision-making process that guarantees human safety without significantly hindering the welding process. The integration of AI-based risk assessment with real-time monitoring provides an efficient solution to collaborative human-robot environments in welding applications.

Key Outcomes

- **Safety First:** The system prioritizes human safety in all scenarios, whether the risk is initially acceptable or not. The system ensures that if the risk level is unacceptable, the robot is immediately stopped.
- **Efficiency in Critical Processes:** For critical welding points where stopping would result in damage or waste, the system intelligently allows the robot to continue working while issuing warnings to humans.
- **Adaptive Response:** The system adapts based on real-time inputs and reassessments. If a human stays in the hazardous zone too long, the system re-evaluates the risk dynamically, ensuring continuous safety monitoring.
- **Manual Control:** After a safety stop, the robot can only be relaunched manually because the human operator decides whether the workpiece can be resumed or if it is already wasted where they need to launch another new operation.
- **Automatic Control:** After an efficiency stop, the current welding sample is at a normal stage, where there is no need for human interaction to make the decision, instead the robot relaunches the process by itself.

CONCLUSION

In this research, we developed a safety-first control system for collaborative human-robot work environments in welding applications, integrating Artificial Intelligence (AI)

with real-time monitoring and decision-making processes. The system prioritizes human safety while maintaining operational efficiency, particularly in scenarios involving unexpected human intrusions into hazardous zones like the UV area generated by a welding robot. The aim was to strike a balance between safety, quality, and production rate without compromising the welding process. The control system design incorporates AI-driven decision-making, real-time monitoring, and robust safety protocols, with a Python implementation successfully simulating various workflow scenarios and demonstrating the system's adaptability to different risk situations. Future advancements could involve integrating more advanced sensor technologies and AI models to further enhance risk prediction accuracy and overall system reliability.

REFERENCES

[1] J. T. Kahnamouei and M. Moallem, Advancements in control systems and integration of artificial intelligence in welding robots: A review, Ocean Engineering, 2024, vol. 312, pp. 119294.

[2] B. Wang, S. J. Hu, L. Sun and T. Freiheit, Intelligent welding system technologies: State-of-the-art review and perspectives, Journal of Manufacturing Systems, 2020, vol. 56, pp. 373-391.

[3] Q. Guo, Z. Yang, J. Xu, Y. Jiang, W. Wang, Z. Liu, ... and Y. Sun, Progress, challenges and trends on vision sensing technologies in automatic/intelligent robotic welding: State-of-the-art review, Robotics and Computer-Integrated Manufacturing, 2024, vol. 89, pp. 102767.

[4] M. Marecek-Kolibisky, S. Janik, M. Mikva, P. Szabo, and G. Czifra, Human-Machine Co-Working for Socially Sustainable Manufacturing in Industry 4.0, Acta Polytechnica Hungarica, 2024, vol. 21, no. 2.

[5] Y. Cao, Q. Zhou, W. Yuan, Q. Ye, D. Popa and Y. Zhang, Human-robot collaborative assembly and welding: A review and analysis of the state of the art, Journal of Manufacturing Processes, 2024, vol. 131, pp. 1388-1403.

[6] S. I. Wahidi, S. Oterkus and E. Oterkus, Robotic welding techniques in marine structures and production processes: A systematic literature review, Marine Structures, 2024, vol. 95, pp. 103608.

[7] Z. Wang, The active visual sensing methods for robotic welding: review, tutorial and prospect, 2024, arXiv preprint arXiv:2405.00685.

[8] A. Mehta and H. Vasudev, Advances in welding sensing information processing and modelling technology: an overview, Journal of Adhesion Science and Technology, 2024, pp. 1-45.

[9] J. T. Kahnamouei and M. Moallem, Advancements in control systems and integration of artificial intelligence in welding robots: A review, Ocean Engineering, 2024, vol. 312, pp. 119294.

[10] G. D. Putnik, P. B. Petrovic and V. Shah, Spatial Visual Feedback for Robotic Arc-Welding Enforced by Inductive Machine Learning, Journal of Manufacturing Science and Engineering, 2024, vol. 146, no. 4.

[11] A. Hyllbrant C. Janpechpanao, Exploring Machine Learning Approaches for Predicting Stops in Welding Robot Operarions, 2024.

[12] D. A. Suciu, E. H. Dulf, and L. Kovacs, Low-Cost Autonomous Trains and Safety Systems Implementation, using Computer Vision, Acta Polytechnica Hungarica, 2024, vol. 21, no. 9.

[13] Y. Chu, K. Ma, L. Zhao, J. Xu, W. Zhou, X. Wang, ... and Y. Zhang, Structural design and adaptive tracking control of automatic welding robot for liquefied natural gas containment system, Discover Applied Sciences, 2024, vol. 6, no. 3, pp. 118.

[14] M. A. Nasser and M. M. Asy, Virtual numerical control: an approach towards autonomous manufacturing with a case study in welding, The International Journal of Advanced Manufacturing Technology, 2024, pp. 1-19.

[15] S. Kumar, Introductory Chapter: Welding in the Era of Industry 5.0, In Welding-Materials, Fabrication Processes, and Industry 5.0. IntechOpen, 2024.

[16] Kollár, Csaba ; Ványa, László: Szerethetők-e a robotok?: Az ember-robot interakció humán oldalának empirikus aspektusa. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 27 : 1-2 pp. 163-177. , 15 p. (2017)

[17] Kollár, Csaba: Szerethetők-e a robotok: Az ember-robot interakció humán oldalának teoretikus aspektusa. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 26 : különszám pp. 142-154. , 13 p. (2016)

[18] Zhang, H, Optimization and Efficiency Improvement of Robot-based Industrial Production Process, International Journal of New Developments in Engineering and Society, 2024, vol. 8, no. 2.

[19] D. K. Naik, V. P. Sharma and R. Dinesh Kumar, Automation in Welding Industries, Automation in Welding Industry: Incorporating Artificial Intelligence, Machine Learning and Other Technologies, 2024, pp. 37-48.

[20] I. M. Sarivan, O. Madsen and B. V. Wæhrens, Automatic welding-robot programming based on product-process-resource models, The International Journal of Advanced Manufacturing Technology, 2024, vol. 132, no. 3, pp. 1931-1950.

[21] A. Biber, R. Sharma, U. Reisgen, Robotic welding system for adaptive process control in gas metal arc welding, Welding in the World, 2024, pp. 1-10.

[22] D. Curiel, F. Veiga, A. Suarez and P. Villanueva, Advances in robotic welding for metallic materials: Application of inspection, modeling, monitoring and automation techniques, Metals, 2023, vol. 13, no. 4, pp. 711.

[23] M. Amarnath, N. Sudharshan and P. Srinivas, Automatic detection of defects in welding using deep learning-a systematic review, Materials Today: Proceedings, 2023.

[24] D. Say, S. Zidi, S. M. Qaisar and M. Krichen, Automated categorization of multiclass welding defects using the x-ray image augmentation and convolutional neural network, Sensors, 2023, vol. 23, no. 14, pp. 6422.

[25] S. Perri, F. Spagnolo, F. Frustaci and P. Corsonello, Welding defects classification through a Convolutional Neural Network, Manufacturing Letters, 2023, vol. 35, pp. 29-32.

[26] S. Ma, Z. Chen, D. Zhang, Y. Du, X. Zhang and Q. Liu, Interpretable Multi-task Neural Network Modeling and Particle Swarm Optimization of Process Parameters in Laser Welding, Knowledge-Based Systems, 2024, pp. 112116.

[27] G. A. Gourzoulidis, C. A. Bouroussis, A. Achtipis, M. Kazasidis, D. Pantelis, A. Markoulis, ... and F. V. Topalis, Photobiological hazards in shielded metal arc welding, Physica Medica, 2023, vol. 106, pp. 102520.

[28] S. S. Murugan and P. Sathiya, Analysis of welding hazards from an occupational safety perspective, Vietnam Journal of Science, Technology and Engineering, vol. 66, no. 3, 2024, pp. 63-74.

[29] A. S. Shote, S. A. Aasa and H. O. Adeyemi, Environmental Trends Due to Arc Welding Activities: Sensitivity of some Typical Workplaces, Arid Zone Journal of Engineering, Technology and Environment, 2024, vol. 20, no. 3, pp. 619-624.

DOI: https://doi.org/10.12700/btsz.2025.7.1.15

KEY CONCEPTS OF SAFETY AND SECURITY

A BIZTONSÁG FONTOSABB FOGALMAI

KOLLÁR Csaba[1]

Abstract

The concept of security is complex and multidimensional, having undergone significant evolution over time. This study reviews various interpretations of security, ranging from early lexicon definitions to modern security science approaches. It examines both static and dynamic aspects of security, as well as its objective and subjective nature. The author analyzes the concepts of protection, guarding, and risk, and their relationship to security. Special attention is given to defining public security and private security, as well as the role of the private security sector in society. The study also addresses the importance of security awareness, which is a key element in addressing modern security challenges. The review highlights that the concept of security is continuously evolving, and its interpretation depends on social, technological, and economic changes.

Keywords

safety and ecurity sciences, public security, private security, protection, security awareness

Absztrakt

A biztonság fogalma komplex és multidimenzionális, amely az idők során jelentős fejlődésen ment keresztül. A tanulmány áttekinti a biztonság különböző értelmezéseit, kezdve a korai lexikonok definícióitól a modern biztonságtudományi megközelítésekig. A biztonság statikus és dinamikus aspektusait, valamint objektív és szubjektív természetét egyaránt vizsgálja. A szerző elemzi a védelem, őrzés és kockázat fogalmait, illetve ezek kapcsolatát a biztonsággal. Külön figyelmet szentel a közbiztonság és magánbiztonság meghatározásának, valamint a magánbiztonsági szektor szerepének a társadalomban. A tanulmány kitér a biztonságtudatosság jelentőségére is, amely kulcsfontosságú elem a modern biztonsági kihívások kezelésében. Az áttekintés rávilágít arra, hogy a biztonság fogalma folyamatosan alakul, és annak értelmezése függ a társadalmi, technológiai és gazdasági változásoktól.

Kulcsszavak

biztonságtudomány, közbiztonság, magánbiztonság, védelem, biztonságtudatosság

[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 főmunkatárs és vezető, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely

BEVEZETÉS

Tanulmányomban több helyen fogok utalni a különböző tudományterületeken megalkotott, teoretikus és empirikus tartalommal gazdagított biztonság fogalmára. A fogalom multidimenzionalitása, inter-, transz-, illetve multidiszciplinaritása adja a nehézséget, mivel az egyes tudományterületek által megalkotott biztonságfogalmak és -tartalmak gyakran alapjaiban másfajta fókuszba helyezik a biztonságot, s ebben a kaotikus fogalomalkotásban a különböző tudományterületek kapcsolódási pontjainál sem mindig találkozhatunk szinergiával, illetve konszenzussal.

FOGALMAK

A ***biztonságtudomány*** a biztonsággal foglalkozó tudomány, mely diszciplináris besorolását tekintve a katonai műszaki tudományokhoz tartozik annak ellenére, hogy e tudományterületen arányait tekintve sokkal több rendészet-, illetve jogtudományi megközelítés található. A biztonságtudomány célja [1 pp. 39-40] „az emberi élet védelme melyre kockázatot jelent a természet, az épített környezet, a műszaki rendszerek és a társadalom, azaz a társadalmi, politikai viszonyok". Definíciójukat egy tetraéderben ábrázolják, ahol az alakzaton belül az emberi élet, az egyes csúcsokon pedig a természet, a társadalom, a műszaki rendszerek és a környezet helyezkedik el. Ez az elképzelés hasonlít a Magyar Biztonságtudományi Társaság elnöke [2] által felvázolt biztonságtudomány triád-rendszeréhez, ahol a háromszög csúcsaiban a természet, a technológia és a társadalom helyezkedik el. Akár a tetraéder, akár a triád interpretációt vesszük alapul, megállapítható, a nevezett területek között szoros, egymásra ható kapcsolat van.

Gazdag és Remek [3 p. 17] a ***biztonság*** fogalmának etimológiai elemzése során a szó latin alakját veszi alapul: „A szótő a cura, -ae (f) szóalakra vezethető vissza, amelynek jelentése: aggodalom, félelem. A se- a sine+abl. fosztóképző módosult alakja, amelynek jelentése: nélkül. Tehát, ha párosítjuk a fogalmi elemeket, megállapíthatjuk, hogy a latin kifejezés egy félelem vagy aggodalom nélküli állapot kifejezésére szolgál".

Az általam feldolgozott szakirodalmak közül a fogalom legkorábbi magyarázatával az Athenaeum kézi lexikonában találkoztam [4 III.kötet, p. 247]: „Biztonság v. közbiztonság az állampolgárok azon állapota, mely szerint személyüket és vagyonukat érhető veszélyt, támadást vagy kárt az államhatalom közhatóságai, a biztonsági közegek útján távoltart". A közbiztonság „a jogállamban a rendőri igazgatás által a polgároknak biztosított vagyon- és életbiztonság minden jogtalan támadással szemben". [4 VIII. kötet, p. 954] Két évtizeddel később a Révai nagy lexikona [5 III. kötet, p. 374] így fogalmaz a biztonsággal kapcsolatban: „az egyeseknek, társadalomnak s államhatalomnak az az érzése, melyet a jog uralma teremt meg. A jog uralmát végső esetben ugyan a bíróság működése tartja fenn, de annak és tehát a jognak s bírói működésnek előfeltételeit a rendőrség teremti meg, melynek ezt az ágazatát biztonsági rendőrségnek nevezzük. A biztonsági rendőrség a bírói működéstől abban különbözik, hogy a jognak nemcsak eszményi uralmát biztosítja, mint a bíróság, mely a jogellenes tényt megtorolja, hanem a jogvédte állapotokat tényleg külső hatalommal is fenntarthatja, azok jogellenes megzavarását folytonos éber őrködéssel megakadályozva, a büntetendő cselekmény elkészületeit s a kísérletet csirájában nyomja el." A definíciók alapján megállapítható, hogy adva van az államhatalom, amelyik törvényeket alkot, s ennek

alapján jár el a biztonság fenntartása érdekében a rendőrség. Ezt a képet árnyalják majd a modern definíciók, ahogy azokat az alábbiakban bemutatom.

Jávor [6 p. 62] szerint a biztonság „egy olyan sokoldalú, sokdimenziós fogalom, hogy definíciója rendkívül nehéz, vitatott és vitatható. Ezért kiinduló pontja lehet az a szükséglet, ami indokolja, magyarázza létrejöttét. Ez pedig nem más, mint általában az élet, különös formájában az emberi élet ösztönös, kibővített formájában pedig a társadalom működőképessége védelmének szükséglete".

A Rendészettudományi szaklexikon [7 pp. 66-67] 2019-es kiadása a biztonságot többtényezős, komplex fogalomként definiálja, amely „az állam és társadalom érdekeinek, értékeinek, az ország területének és lakosságának külső és belső veszélyektől, fenyegetéstől mentes állapotát fejezi ki", majd hozzáteszi, hogy a biztonság a „létezés és a működés káros befolyásoló hatásaitól és a veszélytényezőktől kellően mentesített, védett állapot". Ez a meghatározásbeli eltérés véleményem szerint az elmélet (mentes) és a gyakorlat (kellően mentesített, védett) közti különbséget hivatott érzékeltetni, vagyis azt, hogy a gyakorlatban nem valósítható meg a teljesen biztonságos állapot, de olyan intézkedéseket kell megtennünk, ami ez irányba konvergál.

A Hadtudományi lexikon 1995-ös kiadása [8] a biztonsággal kapcsolatban úgy fogalmaz, hogy az „az egyének, csoportoknak, országoknak, régiónak (szövetségi rendszereknek) a maguk reális képességein és más hatalmak nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete (és annak tudati tükröződése), amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkezhető veszély, illetve adottak az ellene való eredményes védekezés feltételei." A 2019-es kiadású Hadtudományi lexikon [9 pp. 100-102] szócikke szerint a biztonság „a fenyegetettség hiányát vagy kivédésének képességét jelenti". A szócikk szerzője szerint a biztonságnak kettős természete van, ami lehet objektív és szubjektív. „Objektív értelemben a megszerzett értékek elleni fenyegetést méri, szubjektív értelemben a félelem hiányát, hogy ezek az értékek nem lesznek megtámadva". Ez a felfogás „nagy mozgásteret ad az államoknak az objektív és szubjektív felfogás befolyásolására, amit sokszor biztonságosítás útján érnek el".

Az online formában elérhető Közszolgálati lexikon [10] biztonság definíciója Finszter [11] és Balla [12] alapján a biztonságot statikus és dinamikus állapotként értelmezi. A statikus aspektus a Rendészettudományi szaklexikon [7] elméleti megközelítéséhez hasonlatos. A dinamikus értelmezés szerint a biztonság „olyan egyensúlyi állapot, kedvező élethelyzet, melyben valamely tevékenység azért képes zavartalanul megvalósulni, mert a tevékenységet támogató és az azt fenyegető hatások egyensúlyban vannak". Nevezett lexikon [10] a biztonság statikus és dinamikus értelmezése mellett azt nem anyagi természetű infrastruktúraként, együttműködésen alapuló termékként, illetve szolgáltatásként is definiálja. A szolgáltatási aspektus szerint „ha ezt a szolgáltatást a közigazgatás adja, akkor közbiztonságról, ha a privát szféra (biztonsági vállalkozás) adja, akkor magánbiztonságról lehet beszélni".

A biztonság fogalma a veszély és az ellenintézkedés fogalmi keretébe is elhelyezhető, ahogy ezt Szövényi [13 p. 16] is teszi: „a biztonság a veszélyek és az ellenintézkedések hatásai között kialakított egyensúlyi állapot", s később hozzáteszi: „a biztonság megfelelő szintje csak szakadatlan figyelemmel és a veszélyek módosulásához igazodó állandó reagálással érhető el".

Hazánkban a biztonságtudomány területén a Berek és szerzőtársai által megalkotott definíció az elfogadott a biztonság fogalmára: „személyek és szervezetek azon állapota, melyet, a létüket, illetve rendeltetésszerű működésüket veszélyeztető szándékos jogellenes magatartások és az azokkal szemben alkalmazott védelmi erőforrások együtthatása határoz meg". [14 p. 6]

A Magyar értelmező kéziszótár [15] a ***védelem*** fogalmát egyfelől cselekvésként definiálja: valakit, vagy valamit megvédenek, oltalmaznak, vigyáznak rá. Másfelől valakinek, vagy valaminek „az érdekeit védő jogi, erkölcsi hatalom". Ahogy majd a fogalom további értelmezéseinél látni fogjuk a biztonságtudományok területén inkább az előbbi értelmezés az elterjedt. A hétköznapi életben a biztonság és a védelem fogalma gyakran keveredik egymással. Gazdag és Remek [3 p. 18] szerint míg a biztonság fogalmát tágan értelmezve egyaránt vonatkozhat egyénekre, közösségekre, államokra, nemzetközi szervezetekre, s „konkrét értelmezését mindig valamely érték, illetve annak veszélyeztetése határozza meg", addig a védelem „olyan tevékenységek sorozata, amelyek éppen a biztonságosnak tekintett állapot fenntartására, megteremtésére, fejlesztésére irányulnak". Jávor [6 p. 72] is úgy véli, hogy a védelem, pontosabban a védelmi intézkedések révén áll elő a biztonság állapota, s ezek az intézkedések biztosítják „az ellenséges tevékenység, vagy befolyás elleni sérthetetlenséget". Berek és szerzőtársai [14 p. 15] a védelemmel kapcsolatban úgy fogalmaznak, hogy „egy bekövetkező, vagy folyamatban lévő szándékos jogellenes magatartással szembeni ellentevékenység", illetve, azt írják, hogy a védelem az őrzést követő tevékenység, ahol a körülmények (időpont, helyszín, szándék, elkövető, stb.) ismertek, az ellentevékenység során arányos védelmi erőforrást lehet szembe állítania támadással, illetve, hogy miután a jogellenes magatartást elhárították, visszaáll az őrzés.

Az ***őrzés*** [7 p. 435] feladata kettős egyfelől személyek, objektumok, meghatározott területek, valamint értékek ellenőrzése annak érdekében, hogy megakadályozzák annak sértését, bántását, eltulajdonítását, illetve a behatolást, vagy kijutást, másfelől pedig a „védelem feltételeinek megteremtésére irányuló tevékenység". Berek és szerzőtársai [14 p. 14] szerint a „nagy valószínűséggel bekövetkezhető számunkra nem kedvező, illetve szükséges tevékenység megelőzését, megakadályozását célzó ellentevékenység"-et nevezzük őrzésnek. Ez a gyakorlatban azt jelenti, hogy megpróbálunk felkészülni az esetleges jogellenes magatartásokra azáltal, hogy különféle erőforrásokat (pl.: élőerős őrzés), vagy technikákat (pl.: riasztó-, illetve kamerarendszer) alkalmazunk. Az egyének biztosításával, a fogvatartottak, illetve az objektumok és értéktárgyak őrzésével megbízott személy szakmai és gazdasági megfontolások alapján mérlegeli az őrzéssel (és védelemmel) kapcsolatos lehetőségeket, a lehetséges veszélyeket, vagyis megbecsüli a kockázatot.

A ***kockázat*** [15] valamely „cselekvéssel járó veszély, veszteség lehetősége". Vagy más megfogalmazásban [7 p. 325] „kárt, veszteséget, hátrányt, nemkívánatos állapotot okozó, véletlen, egyedileg nem látható és nem kívánt jövőbeni esemény lehetősége", „bizonytalan bekövetkezésű negatívan értékelt következmény", a „veszély realizálódásának valószínűsége". A kockázat úgy is értelmezhető, hogy a környezet- illetve egészségkárosító hatások valószínűsége adott térben és/vagy meghatározott időtartamon belül. Egy adott állapot, vagy helyzet megváltoztatása – az őrzés-védelem fogalmi keretében – kockázattal jár az őrző-védők és a bűnelkövetési szándékú támadók számára is. Az előbbiek azonban ezáltal megbizonyosodhatnak arról, hogy a védelmi rendszereik megfelelően működnek, az élőerős védelem felkészülten és a megtanult és begyakorlott protokoll szerint jár-e el. Ha az

állapot, vagy helyzet megváltoztatása sikertelen volt, vagy csekély mértékű volt, vagy a védelem a támadás észlelése után intézkedett, s így visszaállította a támadás előtti állapotot, akkor azt lehet mondani, hogy a kockázat becslése sikeres volt. Az utóbbiak, vagyis a támadók számára a kockázat abból adódik, hogy ha a támadást a védők meghiúsítják, vagy elhárítják, akkor (1) a támadásba fektetett erőforrásaik odavésznek, (2) feltartóztatják őket, (3) a róluk készül felvétel alapján rövid időn belül a nyomukra akadnak, (4) a védők sokkal nagyobb ellencsapást mérnek a támadókra, mint azt ők előzetesen megbecsülték. Természetesen a biztonságtudomány területén nem csak az őrzés-védés, hanem számos más területen is értelmezhető a kockázat, mint az információbiztonság, a munkabiztonság, a gazdasági biztonság, az iparbiztonság, stb. de ezek közül bővebben csak az információbiztonsággal, s azon belül is a humán információbiztonsággal foglalkozom. A kockázat fogalmának létezik egy olyan interpretációja is, amikor az információk hiánya, vagy az információk nem megfelelő minősége rejt magában kockázatot, mivel így nem, vagy nem megalapozott, vagy hibás döntéseket lehet csak hozni.

Ahogy arról fentebb írtam, a Közszolgálati lexikon [10] meghatározása alapján a biztonság közbiztonságra és magánbiztonságra osztható. A ***közbiztonság*** „alapvetően olyan közállapot, amelyben az egyes személyek és közösségek élete, működése és javai a jogellenes támadásoktól nincsenek veszélyeztetve". [7 pp. 342-343] A definíció további értelmezései alapján a társadalmi békés együttélés biztosítása, az állampolgárok élet- és vagyonbiztonságának jogi szabályozása, s ennek állami általi garantálása a feladata. Látható, hogy a [7] és [9] alapján az akkor megalkotott definíciók inkább a közbiztonság meghatározására vonatkoztak. A Nemzeti Bűnmegelőzési Stratégiáról szóló kormányhatározat megfogalmazásában a közbiztonság „a társadalom életminőségének a része, olyan kollektív, értékkel bíró termék, amelynek kialakítása és megőrzése közös ügy". A 'közös ügy' azt jelenti, hogy a büntető igazságszolgáltatás mellett szükség van prevencióra, biztonságtudatossági nevelésre/fejlesztésre, az állampolgárok biztonságtudatosabb viselkedésére és rendőrséggel történő együttműködésükre, valamint a téma kutatására, s a kutatási eredmények alapján a közbiztonság és a hozzá kapcsolódó területek fejlesztésére. Christián [16 p. 17] Finszter [17] alapján azt állítja, hogy a közbiztonság államcél, „melyért a végrehajtó hatalom felelős", ugyanakkor „a jog által is elismert társadalmi érték", s ennek megóvása érdekében akár az emberi jogok korlátozása is szükséges lehet. A közbiztonság jogi értelemben törvényekben és rendeletekben szabályozott, így az azt megsértőket számon lehet kérni, felelősségre lehet vonni. Ugyan a közbiztonság és a közrend nem befolyásolja a személy- és vagyonbiztonságot közvetlenül, Berek és szerzőtársai [14 p. 9] rámutatnak arra, hogy a közbiztonság és a magánbiztonság között kapcsolat van, mivel „ahol magasabb szintű a közbiztonság ott sokkal kevesebb a személyek és a tulajdon kárára elkövetett szándékos jogellenes cselekmények száma".

A ***magánbiztonság*** fogalmának nemzetközi értelmezésében elsőként Green [18] alapján ismertetem. Szerinte a magánbiztonság az állami bűnüldöző szervektől eltérő személyek, szervezetek és szolgáltatások, amelyek elsősorban a bűncselekmények, az egyes személyek, szervezetek, vagy létesítmények veszteségének, vagy kárának megelőzésében vesznek részt. Egy másik [19] meghatározás szerint a magánbiztonság az emberek, a tulajdon és az információk védelmének, a vizsgálat lefolytatásának és a szervezet vagyona védelmének nem kormányzati gyakorlatára vonatkozik. Az amerikai Biztonsági Vállalatok

Országos Szövetsége (NASCO) magánbiztonságot úgy határozza meg [20], hogy az a személyek, ingatlan- és ingó vagyontárgyak és egyéb érdekek védelmére vonatkozik, az államtól vagy annak szerveitől eltérő egyének és szervezetek által a bűnözés, a veszteségek és károk megelőzése és csökkentése céljából. Egy másik, amerikai központú szervezet, a biztonság fejlesztésével foglalkozó ASIS [21] álláspontja szerint a magánbiztonság a védelmi, nyomozati és kapcsolódó szolgáltatások széles körét foglalja magában, amelyeket magánszemélyek, vállalatok vagy szervezetek, nem kormányzati szervek nyújtanak. Az Európai Biztonsági Szolgálatok Konföderációja (CoESS) [27] a magánbiztonságról úgy vélekedik, hogy az minden olyan tevékenységre vonatkozik, amely a magáncégek vagy egyéni vállalkozók által végzett vagyonvédelmi szolgáltatásokkal és biztonsági berendezésekkel személy-, vagyon- és egyéb vagyonvédelemmel kapcsolatos. Az amerikai-európai definícióhoz hasonló az indiai NCERT [22] meghatározása, mely különválasztja a magánbiztonságot és a közbiztonságot, kiemelve, hogy a magánbiztonsági tevékenységet a közalkalmazottaktól eltérő személy végzi az emberek, vagyontárgyak vagy mindkettő védelme, vagy őrzése céljából, ideértve a páncélozott autók szolgáltatását is. A magánbiztonságot magánügynökségek biztosítják az ügyfeleknek térítés ellenében. A Nemzetközi Vöröskereszt által kiadott Montreaux-i Document [23], mely a katonai és biztonsági magáncégek fegyveres konfliktusok során végzett műveleteivel kapcsolatos nemzetközi jogi kötelezettségekről ír, azt állítja, hogy nincs egységes definíciója annak, hogy mi a 'katonai' és mi a 'biztonsági' vállalat. A hétköznapi szóhasználatban bizonyos tevékenységeket (például a harcban való részvételt) hagyományosan katonai jellegűnek, míg más tevékenységeket (például a lakóhelyek őrzését) a biztonsággal kapcsolatosnak tekintenek. A valóságban sok vállalat a szolgáltatások széles skáláját nyújtja, amelyek a tipikusan katonai szolgáltatásoktól a tipikusan biztonsági szolgáltatásokig terjedhetnek. Ezért nem könnyű őket kategorizálni. Sőt, humanitárius szempontból nem az a lényeges kérdés, hogy egy céget hogyan címkéznek, hanem az, hogy az adott esetben milyen konkrét szolgáltatásokat nyújt. Emiatt a Montreux-i dokumentum elkerüli a katonai és magán biztonsági magáncégek szigorú elhatárolását, és a „katonai és biztonsági magánvállalatok" (PMSC) kifejezést használja, amely magában foglalja mindazon vállalatokat, amelyek katonai vagy biztonsági szolgáltatásokat vagy mindkettőt nyújtanak.

A ***magánbiztonság*** fogalmának komplex megközelítése olvasható a Közszolgálati Online Lexikon [10], Finszter [11 pp. 96-97], Mészáros [27 pp. 380-381], Christián [16 pp. 15-30] írásaira, illetve a személy és vagyonvédelemről szóló törvényre hivatkozó szócikke, melyben a magánjog védelmének széles lehetőségei, a fizikai erőszak alkalmazásának korlátja, a személy- és vagyonvédelmi, illetve magánnyomozói szolgáltatás közrend és közbiztonság javításához való hozzájárulása, kerülnek kiemelésre. A szócikk azzal a megállapítással zárul, hogy „az egyének magánbiztonsága együttesen eredményezheti a közbiztonságot. Ez úgy is értelmezhető, hogy a magánbiztonság a közbiztonság részének tekinthető." A magyarországi terminológiában a magánbiztonság kifejezést Christián [25 p. 81] alapján úgy lehet meghatározni, hogy az „egy olyan, ellenszolgáltatás keretében, piaci alapon működő, engedéllyel bíró vállalkozás – vagy természetes személy – által nyújtott szolgáltatás, amely a megbízó személyes biztonságát, tulajdonát védelmezi, elősegíti a jogainak teljesebb körű gyakorlását." A magán- és a közbiztonság vonatkozásában Lippai és Christián [26 p. 73] friss kutatásában megállapítja, hogy „az állami rendészet monopóliuma megtörésével a

magánbiztonsági szektor szereplői egyre növekvő szerepet vállalnak a biztonság, mint termék megteremtésében. Tevékenységük az állami rendészeti szervek tehermentesítését, annak költséghatékonyabb működését eredményezi, amelynek kapcsán további tevékenységek racionalizálására, megfelelő állami garanciális szabályok és kontrollmechanizmusok megalkotásával egyes tevékenységek fokozatos átcsoportosítására kerülhet sor". Vagyis a szakértők körében is végzett felmérésük alapján a jövőben elképzelhető, hogy a magánbiztonsági szektor vállalatai többlettevékenységeket végezhetnek olyan területeken, jelenleg még csak az állami szereplők által végzett tevékenységekkel találkozhatunk.

A ***biztonságtudatosság*** definíció szerint „azon tanult képesség, amely a biztonsági kockázatok feltárt eredményei ismeretében azok előkészületi, kezdeti fázisában megfigyelhető jellemzők tudatos felismerésére és megelőzésére teszi képessé az egyént". [7 p. 73] Egy másik megfogalmazás szerint „Biztonsági tudatosság alatt a tágabb értelemben vett rendvédelmi és magánbiztonsági szervek komplex, plakátok, emléktárgyak előállításában és átadásában; előadások, filmvetítések, e-learning-anyagok létrehozatalában és megtartásában megnyilvánuló oktatási képzési tevékenységet értjük. Eredményeképpen létrejön a biztonsági kihívásokat jól ismerő, a megelőzéshez és elhárításhoz szükséges magatartási formákat szintén ismerő és a gyakorlatban azokat alkalmazó, implementáló attitűd, viszonyulás, eljárásrend, amely kiterjed a biztonság sérülése esetén a rendvédelmi szervek megkeresésére, tájékoztatására is". [28 p. 5] Dallos és Molnár [29] a biztonságtudatosságot a vagyon- és személybiztonság, a közbiztonság és a(z általános) biztonság együtteseként képzeli el. Értelmezésükben a biztonságtudatosság mindenkitől (egyének, társadalmi közösségek, vállalkozások, önkormányzatok, állam és állami intézmények) elvárható, hiszen csak biztonságtudatos tevékenységük révén tudnak figyelemmel lenni a saját és embertársaik életére, épségére, az ingó- és ingatlanvagyon megvédésére és védelmére.

ÖSSZEFOGLALÁS

A biztonság fogalma összetett és multidimenzionális, amely folyamatos fejlődésen megy keresztül. A tanulmány bemutatta a biztonság különböző értelmezéseit a történeti lexikális meghatározásoktól a modern biztonságtudományi megközelítésekig. Elemezte a biztonság statikus és dinamikus aspektusait, valamint annak objektív és szubjektív természetét. Az írásmű részletesen tárgyalta a védelem, az őrzés és a kockázat fogalmait, és azok kapcsolatát a biztonsággal. Kiemelt figyelmet kapott a közbiztonság és a magánbiztonság fogalmának meghatározása, valamint a magánbiztonsági szektor társadalmi szerepe. A biztonságtudatosság, mint a modern biztonsági kihívások kezelésének kulcseleme, szintén hangsúlyos volt a tanulmányban. Rámutattam arra, hogy a biztonság fogalma folyamatosan alakul, és annak értelmezése nagyban függ a társadalmi, technológiai és gazdasági változásoktól.

FELHASZNÁLT IRODALOM

[1] ROHÁCS J. – HORVÁTH Zs. Cs.: A repülésbiztonság problémája és fejlesztési tervei. Repüléstudomány közlemények, XXV. évf. 3. szám, 2013.
[2] NAGY T.: Biztonság és biztonságtudomány. Budapest: Magyar Biztonságtudományi Társaság, 2001.

[3] GAZDAG F. – REMEK É.: A biztonsági tanulmányok alapjai. Budapest: Dialog Campus, 2018.
[4] ACSÁDY I. (szerk): Az Athenaeum kézi lexikona: A tudományok enciklopédiája, különös tekintettel Magyarországra. Budapest: Athenaeum, 1891-1893
[5] MÓR J. (főszerk): Révai nagy lexikona: Az ismeretek enciklopédiája. Budapest: Révai, 1911-1935.
[6] JÁVOR E.: Fésületlen gondolatok a biztonságról. Nemzetbiztonsági szemle, MMXIV/III, 2014.
[7] BODA J. (főszerk.): Rendészettudományi szaklexikon. Budapest: Dialog Campus, 2019.
[8] SZABÓ J. (szerk.): Hadtudományi Lexikon. Magyar Hadtudományi Társaság, 1995.
[9] KRAJNC Z. (főszerk.): Hadtudományi lexikon. Budapest: Dialóg Campus, 2019.
[10] Közszolgálati Online Lexikon. https://lexikon.uni-nke.hu (megtekintés: 2023.02.10.)
[11] FINSZTER G.: A rendészet elmélete és a rendészeti eszközrendszer. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó, 2013. pp. 37-39.
[12] BALLA Z.: Monográfia a rendészetről. Budapest: Rejtjel Kiadó, 2016.
[13] SZÖVÉNYI Gy.: Biztonságszervezői menedzsment. Budapest: ProSec, 2003.
[14] BEREK L. – BEREK T. – BEREK L.: Személy- és vagyonbiztonság. Budapest: Óbudai Egyetem, 2016.
[15] Magyar értelmező kéziszótár online változata. https://www.szotar.net/szocikk/lerte022003-69228-vea (megtekintés: 2023.02.13.)
[16] CHRISTIÁN L. (szerk.): A magánbiztonság elméleti alapjai. Budapest: NKE Rendészettudományi Kar, 2014.
[17] FINSZTER G.: A rendészeti szervek működésének jogi alapjai. Budapest: RTF Alkotmányjogi és Közigazgatási Jogi Tanszék, 2008.
[18] GREEN, G.: Introduction to security. Boston: Butterworth. 1981.
[19] SHAPIRO, L. R. – MARAS, M-H. (szerk.): Encyclopedia of Security and Emergency Management. Springer Cham, 2021.
[20] National Association of Security Companies (NASCO) https://www.nasco.org megtekintés: 2022.12.20.
[21] Advancing Security Worldwide (ASIS) https://www.asisonline.org megtekintés: 2022.12.20.
[22] NCERT Introduction to Security Services (oktatási anyag). https://ncert.nic.in/vocational/pdf/iesg101.pdf megtekintés: 2022.12.20.
[23] International Committee of the Red Cross THE MONTREUX DOCUMENT. Genf: ICRC, 2009.
[24] MÉSZÁROS B.: A magánbiztonság és a rendészettudomány kapcsolódási pontjai. In: BODA J. – FELKAI L. – PATYI A. (szerk.): Ünnepi kötet a 70 éves Janza Frigyes tiszteletére. Budapest, Dialóg Campus Kiadó, 2017. pp. 380-381.
[25] CHRISTIÁN L.: A magánbiztonság és önkormányzati rendészet egyetemi szintű képzése. Belügyi Szemle, 66(11), 2018. pp. 85–86.
[26] LIPPAI Zs. – CHRISTÁN L.: Újragondolt biztonság, kutatási jelentés. Belügyi Szemle, 71(1), 2023. pp. 53–76.
[27] Confederation of European Security Services (CoESS) https://www.coess.org megtekintés: 2022.12.20.

[28] JASENSZKY N. – REGÉNYI K. M. – LIPPAI Zs.: A biztonságtudatosság fogalma, fejlődése nemzetbiztonsági, terrorelhárítási és magánbiztonsági szempontból. NEMZETBIZTONSÁGI SZEMLE 9. évfolyam 4. szám, 2021. pp. 3–17.
[29] DALLOS E. – MOLNÁR I. J.: BIZTONSÁG ÉS ÉLHETŐSÉG A XXI. SZÁZADBAN. Budapest: A Biztonságos és Élhető Városokért Egyesület (BEVE), 2020.

DOI: https://doi.org/10.12700/btsz.2025.7.1.25

INTEGRATED ENTERPRISE RISK MANAGEMENT - OPPORTUNITIES AND THREATS IN THE LIGHT OF STANDARDS AND RECOMMENDATIONS

INTEGRÁLT VÁLLALATI KOCKÁZATMENEDZSMENT - LEHETŐSÉGEK ÉS VESZÉLYEK A SZABVÁNYOK ÉS AJÁNLÁSOK TÜKRÉBEN

MICHELBERGER Pál[1]

Abstract

What are the problems of an integrated corporate risk management system? The study draws attention to some of the pitfalls of the integrated corporate risk management system affecting the implementation and effectiveness of business- and technological processes, and to the possibilities of its design and operation. The methodological separation of the specific risk management of functional enterprise sub-areas due to tradition could be a serious threats. Corporate management cannot afford to deal with the effects of the resulting risk events only in detail. Risk management based on an unified basis must now be present in all areas of the operation of companies. One of the aims of the study was to review some of the major Hungarian publications related to integrated risk management in the past two decades. The bibliographical data of more than a dozen easily accessible, relevant journal articles from Hungarian authors can be found in the bibliography.

Keywords

risk level, process risk, FMEA, ISO 31000, ISO/IEC 27005

Absztrakt

Milyen problémák lehetnek egy integrált vállalati kockázatmenedzsment rendszerrel kapcsolatban? A tanulmány felhívja a figyelmet az üzleti- és technológiai folyamatok végrehajtását és eredményességét befolyásoló teljeskörű és integrált vállalati kockázatmenedzsment rendszer néhány buktatójára és kialakításának és működtetésének lehetőségeire. Komoly veszély a funkcionális vállalati részterületek sajátos kockázatértékelésének és -kezelésének hagyományok miatti módszertani elkülönülése. A vállalati vezetés nem engedheti meg magának, hogy a bekövetkező kockázati események hatásai csak részleteiben legyenek kezelve. Az egységes alapokon nyugvó kockázatmenedzsmentnek ma már a cégek működésének minden területén meg kell(ene) jelennie. A tanulmány egyik célja volt az elmúlt két évtized néhány jelentős, integrált kockázatmenedzsmenthez köthető, magyarnyelvű publikációjának áttekintése is. Az irodalomjegyzékben több mint egy tucat, könnyen elérhető, releváns, magyar szerzőktől származó folyóiratcikk bibliográfiai adatai találhatók meg.

Kulcsszavak

kockázati szint, folyamatkockázat, FMEA, ISO 31000, ISO/IEC 27005

[1] michelberger.pal@bgk.uni-obuda.hu | ORCID: 0000-0001-5752-0224 | professor, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

ELŐZMÉNYEK

Frank H. Knight az Egyesült Államokban 1921-ben már elkülönítette a „kockázat" és a „bizonytalanság" fogalmát és talán elsőként foglalkozott művében az üzleti kockázatok jelentőségével [12] [21]. Martin Kenneth Starr 1972-ben írt átfogó termelésmenedzsment témájú könyvében még külön-külön foglalkozik a minőség-ellenőrzés és a beruházások (pénzügyi) kockázataival [19]. A kockázatelemzés tudományos megalapozása az 1980-as években volt megfigyelhető [18] [3]. Ennek folytatása volt a kockázatmenedzsment követelményeket leíró szabványok és ajánlások, illetve a kockázatelemzés, -értékelés és -kezelés gyakorlatát, módszertani hátterét bemutató szakmai dokumentumok megjelenése [41], amelyek napjainkban is folyamatosan fejlődnek, bővülnek. A később említett kockázatmenedzsment szabványok közül a COSO ERM ajánlás [36] [38] már 2004-ben is megvolt. Az ISO/IEC 31000-es szabvány korábbi változata már 2009-ben megjelent. Jelenlegi formájában 2018-ban adta ki a nemzetközi szabványügyi testület és az iso.org tanúsága szerint már fejlesztik az ISO/WD 31000-es új változatot is.

A holisztikus megközelítést, az egész vállalatra vonatkozó integrált kockázatmenedzsmentet a vezetők és az üzleti partnerek egyre jobban igénylik. A vállalatok sokszor ezért látszatintézkedéseket tesznek. A kockázatelemzéssel és -értékeléssel megbízott szakmai kör kialakít egy formális, általában írott szabályrendszert a tulajdonosi vagy üzleti partneri elvárások alapján. A kockázatkezelési szabályzat elkészül, de az láthatóan nem kényszeríti a szervezetet működése megváltoztatására, javítására. Általában kevesen és elszigetelten használják. Nincs meg a folyamatos felülvizsgálat [6]. A kockázatmenedzsment módszerek pedig nem illeszkednek a vállalati stratégiákhoz [11]. A kockázatok számbavétele, elemzése és értékelése nem folyamatos, hanem kampányszerű vagy periodikus, esetleg egy-egy nagyobb kockázati esemény bekövetkezése utáni pótcselekvés.

Vannak olyan gazdálkodási területek, ahol korábban is volt erős kockázatmenedzsment szabályozás (pl. vállalati pénzügyek, vagyonbiztosítások, minőségirányítás). Ezek azonban inkább elszigetelődnek, mintsem a saját szintjükre emelik fel a többi funkcionális szervezeti egység, vagy üzleti és technológiai folyamat kockázatmenedzsmentjét. Az sem segít, hogy számtalan kockázatmenedzsment szabvány és ajánlás közül lehet választani és a bőség zavara módszertani segédanyagoknál is jelentkezik. Mielőtt az integráció útjára lépünk, tehát választani kell a lehetőségek közül és ez változásra / változtatásra, valamint tanulásra kényszeríthet sok szervezeti egységet. A kockázatmenedzsment irányítási rendszert pedig a bevezetés után is folyamatosan tesztelni, használni és fejleszteni szükséges.

EGYSÉGES VÁLLALATI KOCKÁZATMENEDZSMENT RENDSZER HIÁNYA

A kockázatmenedzsment vállalati keretének kialakításához és magának a kockázatelemzéshez és -kezeléshez sok támogatást szabvány és ajánlás elérhető [10]. A most felsorolásra kerülő dokumentumok nem felelnek meg a teljesség igényének és inkább csak azok kerültek ide, amelynek fő profilja a funkcionális vagy a teljes szervezeti működést átfogó kockázat-menedzsment.

- ISO/IEC 310XX-es szabványcsalád [24] [28],
- ISO/IEC 27005-ös információbiztonsági kockázatok kezelésére készült útmutató [23],

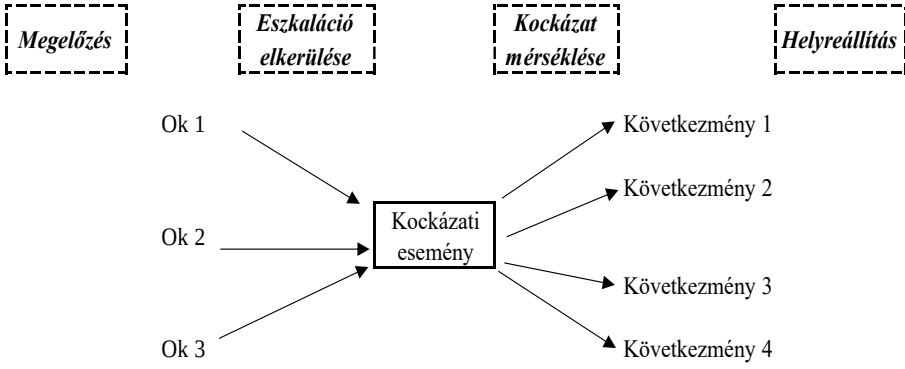
- ALARP alapelv (As Low As Reasonable Practicable a lehető legkisebb, még észszerűen megvalósítható kockázati szint elérésére történő törekvés) [39],
- COSO ERM (Comitte of Sponsoring Organisations of Treadway Comission) vállalati kockázatkezelő (Enterprise Risk Management) keretrendszer, amely a Governance-Risk-Complience (GRC) modellen alapszik [2] [16] [20] [36] [38],
- MIL-STD 882E amerikai katonai szabvány a kockázatmenedzsmentre [34],
- CRAMM modell (CCTA Risk Analysis and Management Method) elsősorban információbiztonsági kockázatok elemzésére és kezelésére szolgáló modell [14] [22],
- FMEA (Failure Mode and Effect Analysis) Hibamód és hibahatás elemzés elsősorban a minőségirányításban [13] [35].

Ezek általában nem kötelező jelleggel szabják meg, hogy milyen kockázatelemzési és -kezelési módszertani hátteret használ egy vállalat. Így azok gyakran nem integráltak és nem egységesek (ráadásul a kockázat értékelés eltérő mérési skálákon történik…).

Az integrált kockázatkezelés szükségességét az 1. ábra alapján is igazolhatjuk. A kockázatkezelés jellemző szakmai területeinek (következményeinek) egy lehetséges felosztása a következő [5]:

- pénzügyi és finanszírozási kockázatok (pl. árfolyamváltozás, alapanyagárak, vevők likviditásának romlása, jegybanki alapkamat változás),
- stratégiai kockázatok (pl. szabályozási vagy politikai környezet megváltozása, vevők ás beszállítók hosszútávú döntései, szervezet külső megítélése),
- működési kockázatok (humán erőforrás, Információs és kommunikációs technológia, termelőeszközök működőképessége),
- projektkockázatok (beruházások és innovációk kockázatai).

Számos ok hozhatja el adott kockázati esemény bekövetkezését, ami azután több szakmai területen is egymást erősítő következményt eredményez.



1. Ábra: Kockázati esemény okai és „nem kívánt" következményei („bow tie" diagram ISO/IEC 31010 szabvány alapján) [24]

Példaként vegyük kockázati eseménynek az elkészült és leszállított termékre vonatkozó számla kibocsátás megakadását. Ennek lehet információtechnológiai oka (a számlázó program nem működik, nem tud a vevő és az adóhatóság által elfogadott, sorszámozott, megfelelő adat-tartalmú bizonylatot előállítani. Ok lehet még a nem megfelelő teljesítés (a

vevő mennyiségi és minőségi átvétele hibát és / vagy hiányosságot észlelt). Elképzelhető okként egy kalkulációs probléma, amely a számla végösszegét kérdőjelezi meg. A következmények több vállalati területet is érinthetnek; romlik a cég reputációja és csökken a vevői bizalom, elmaradó vagy késő bevétel likviditási problémákat okoz. A számlázó program verzió-váltása után a becsült kockázati szint nőhet.

A szervezeten belüli, egy-egy területet izoláltan érintő kockázat elemzés, -értékelés és -kezelés nem fogja a kívánt mértékben emelni a vállalat biztonsági szintjét [9].

Az ISO/IEC 27005-ös szabvány [23] „A" melléklete például számos mintapéldát ad kvalitatív kockázatelemzéshez (a valószínűségek és a kockázati következmények, valamint a kockázatkezelést eldöntő kockázat nagyságának osztályba sorolásához). De ugyanitt találhatunk olyan értékelési mintákat (szempontokat), amelyek a kvantitatív elemzés irányába mutatnak (pl. kockázati események bekövetkezésének várható gyakorisága vagy az angol fontban (£), sávosan kifejezett kockázati következmények, károk osztályai.

Az 1. táblázat az ISO/IEC 27005-ös szabvány mellékletében javasolt (!) kvalitatív kockázati szint mátrixot mutatja. Öt valószínűségi szintből és a lehetséges öt következményből öt kockázati szint jöhet ki (nagyon magas – very high, magas – high, közepes – medium, alacsony – low és nagyon alacsony – very low…).

	Következmény				
Valószínűség	Katasztrófális	Kritikus	Súlyos	Jelentős	Mérsékelt
Majdnem biztos	Nagyon magas	Nagyon magas	Magas	Magas	Közepes
Nagyon valószínű	Nagyon magas	Magas	Magas	Közepes	Alacsony
Valószínű	Magas	Magas	Közepes	Alacsony	Alacsony
Kissé valószínűtlen	Közepes	Közepes	Alacsony	Alacsony	Nagyon alacsony
Valószínűtlen	Alacsony	Alacsony	Alacsony	Nagyon alacsony	Nagyon alacsony

1. Táblázat: Ajánlás kockázati szint mátrixra ISO/IEC 27005 szabvány „A" melléklete alapján [23]

A MIL-STD-882-E amerikai szabvány [34] egy hasonló mátrixot ad meg, amelyet katonai kockázatelemzés során „kötelező" használni. A 2. táblázatban azonban hat valószínűségi szint van és négy következmény alapján kapjuk meg az ötféle lehetséges kockázati szintet (elhanyagolható – eliminated, alacsony - low, közepes - medium, súlyos - serious, magas – high).

	Következmények súlyossága			
Valószínűség	1 - Katasztrofális	2 - Kritikus	3 - Nem jelentős	4 - Elhanyagolható
A - Gyakori	Magas	Magas	Súlyos	Közepes
B - Valószínű	Magas	Magas	Súlyos	Közepes
C - Alkalmi	Magas	Súlyos	Közepes	Alacsony
D - Csekély	Súlyos	Közepes	Közepes	Alacsony
E - Valószínűtlen	Közepes	Közepes	Közepes	Alacsony
F - Lehetetlen	Elhanyagolható	Elhanyagolható	Elhanyagolható	Elhanyagolható

2. Táblázat: Kockázati szint mátrix a MIL-STD-882E szabvány alapján [34]

A 2. táblázat tanúsága szerint B3 mező ugyanolyan kockázati szintet mutat, mint az D1 mező. A kockázati szint megállapítása után a valószínűségnek és a következmények súlyosságának továbbra is szerepet kellene játszani a kockázatkezelés módjának meghatározásában (elfogadás, kockázati szint csökkentése, megosztás, áthárítás vagy kockázatkerülés). Példánkban a D1 mezőbe eső kockázati eseménynél a következmények súlyosságát

javaslom preventív módon csökkenteni (D1 => D2), míg az B3 mezőbe kerülő kockázati eseménynél a valószínűség mérséklése lehet a preferált (B3 => C3).

A széles körben elterjedt FMEA módszer (Failure Mode and Effect Analysis; Hibamód- és Hibahatás Elemzés) három tényezőt vizsgál [13] [35];

- kárérték, súlyosság foka (Effect, 1 – alig észrevehető hiba, 10 – nagyon súlyos kár),
- bekövetkezés valószínűsége (Occurance, 1 – nagyon kis valószínűség, 10 – biztosan várható a hiba előfordulása),
- felderíthetőség (hiba esetén milyen gyorsan válik az felismerhetővé; Detection, 1 – jó hatásfokkal jelezhető a hiba, 10 – a hiba nem észrevehető, csak a későbbi káresemény jelzi…).

Ebből a három tényezőből számolunk egy „kockázat-prioritási számot" (RPN – Ratio Priority Number), ami valójában egy kockázati szintet mutat.

$$RPN = súlyosság\ foka \times bekövetkezési\ valószínűség \times felderíthetőség$$

Az RPN tehát egy 1-től 1000-ig terjedő diszkrét skálán mozoghat. A hibajavítás (és kockázat értékelés valamint -kezelés célja a magas RPN értékek csökkentése. Ilyenkor a 3 tényező közül a legnagyobbat javasolt kockázatkezeléssel lejjebb vinni. Az FMEA termelő és szolgáltató cégeknél nagyon elterjedt és konstrukciós tervezés hibáinak kiküszöbölése mellett használják technológiai folyamatoknál, infrastruktúrákhoz köthető rendszer-üzemeltetésben (pl. épületgépészet) és szervíztevékenységek kockázatkezelésében is.

A kockázatok, kockázati események (bekövetkezési valószínűség x következmények súlyossága) összegyűjtése és feldolgozása nehezen megvalósítható egy integrált kockázatmenedzsment rendszerben. Vannak olyan területek, amelyekben a valószínűség és a következmény majdnem pontosan meghatározható vagy kiszámolható esetleg mérhető (pl. árfolyam-ingadozás), más esetekben (pl. korábban nem tapasztalt természeti katasztrófák bekövetkezése, ill. azok következményei) ezek a paraméterek inkább csak becsülhetők. Integrált rendszerekben tehát az előbb bemutatott kvalitatív, osztályba soroláson alapuló kockázati esemény-minősítés lehet a végcél. Természetesen, ameddig lehetséges próbáljunk meg a számszerűsíthető, kiszámolható adatoknál maradni. Kvantitatív elemzés számszerű eredményeiből könnyebb kvalitatív kockázati szinteket meghatározni, mint fordítva…

Számos olyan szabvány és ajánlás van, amely érinti a kockázatmenedzsmentet és ösztönzi alkalmazását, de nem ez a fő profiljuk (Horváth – Szlávik, 2011a). Néhány a teljesség igénye nélkül;

- MSZ ISO 14001 Környezetközpontú irányítási rendszerek. Követelmények és alkalmazási irányelvek [32],
- MSZ 28001 (BS OHSAS 18001) A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR). Követelmények [27],
- MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Információbiztonság irányítási rendszerek. Követelmények [17],
- CObIT 5 verzió (Control Objectives for Information and related Technology magyar változata Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések) [14] [37],
- MSZ ISO/IEC 20000-1 Informatika. Szolgáltatásirányítás. 1. rész. Előírás [29],

- MSZ ISO/IEC 20000-2 Informatika. Szolgáltatásirányítás. 2. rész: Alkalmazási útmutató [30],
- MSZ ISO 22301 Üzletmenetfolytonossági irányítási rendszerek. Követelmények [33],
- MSZ EN ISO 9001 Minőségirányítási rendszerek. Követelmények [31],
- ISO/IEC 3300X Többrészes szabványcsomag a folyamatok értékelési lehetőségeiről folyamatcélok és várható eredmények tekintetében [25],
- ISO/IEC 38500 Corporate Governance of Information Technology IT vállalaton belüli irányítását szolgáló keretrendszer [26],
- SCOR Supply Chain Operations Reference modell, ellátási láncok működésére vonatkozó folyamatszervezési ajánlás [42],
- Project Management Body of Knowledge (Projektmenedzsment Útmutató) [40].

Az integrált vállalati kockázatmenedzsment (ERM – Enterprise Risk Management) kialakítása és működtetése jelentős lépés lehet egy szervezet életében. A hagyományos, szigetszerű kockázatkezelés töredezett, egymástól független intézkedéseket hozhat, amelyeknél nem ismerik fel kockázati esemény következményeinek összefüggéseit [6]. Az ERM ezzel szemben egy holisztikus megközelítés, amely integrálja kockázatkezelési gyakorlatot az egész szervezetre kiterjedően. Az üzleti és technológiai környezet állandó változása és bonyolultsága igényli a kockázatok átfogó, folyamatos azonosítását, elemzését és kezelését (mérséklését) [15].

Az ISO/IEC 31010-es szabvány [24] több mint 30 kockázatértékelésben és kezelésben alkalmazható eszközt és technikát sorol fel és értékeli használhatóságukat a Monte-Carlo módszertől, a hiba-fa analízisen át egészen a költség-haszon elemzésig. Természetesen egy integrált vállalati üzleti és technológiai folyamatokra fokuszáló kockázatmenedzsment rendszer esetében össze kell válogatni azokat, amelyek együttesen alkalmasak a kockázatok azonosítására, elemzésére, értékelésére és kockázatkezelés támogatására [1].

FOLYAMATOK KOCKÁZATKEZELÉSE

A kockázati események bekövetkezésének szervezeti működésre gyakorolt hatásának elemzése gyakran elmarad. A kockázatelemzés (akár előzetes, akár utólagos) a lokális káreseményre és annak nagyságára fókuszál az üzletmenetfolytonosság biztosítása helyett [20]. Nagyon ritka a vállalat számára előnyös „pozitív” kockázati események számbavétele [4].

Az ISO/IEC 33004-es (korábban ISO/IEC 15504) folyamat-felméréssel foglalkozó szabvány bevezetett hat „folyamatképességi szintet” [25];

0. hiányos folyamat (incomplete process; a folyamat célja nem, vagy csak részben teljesül),
1. végrehajtott folyamat (performed process; a folyamat célja teljesül, de időt és erőforrásigényt nem vizsgálunk…),
2. irányított folyamat (managed process; a folyamat és eredménye is megfelelően kézben tartott…),
3. kialakított folyamat (established process; a folyamat minta és/vagy szabvány alapján megtervezett és végrehajtott),

4. kiszámítható folyamat (predictable process; a folyamat végrehajtása mérhető és ellenőrizhető),
5. optimalizáló folyamat (optimizing process; a folyamatot folyamatosan fejlesztik az előre meghatározott üzleti célok elérése érdekében, megjelenik a visszacsatolás is…).

A folyamatok értékelésével és kimeneteik minősítésével a kockázatértékelést is érintjük [43]. A „végrehajtott" és az „irányított" folyamatok magas és közepes kockázatot hordozhatnak, míg a „kialakított" (3. szint) és a „kiszámítható" (4. szint) folyamatokhoz közepes és alacsony kockázati szint társulhat. Az „optimalizáló" folyamat csak alacsony kockázatú lehet. A megállapított kockázati szint természetesen függ attól is, hogy a tényleges folyamat a valóságban mennyire tér el az előre megadott / besorolt képességszinttől.

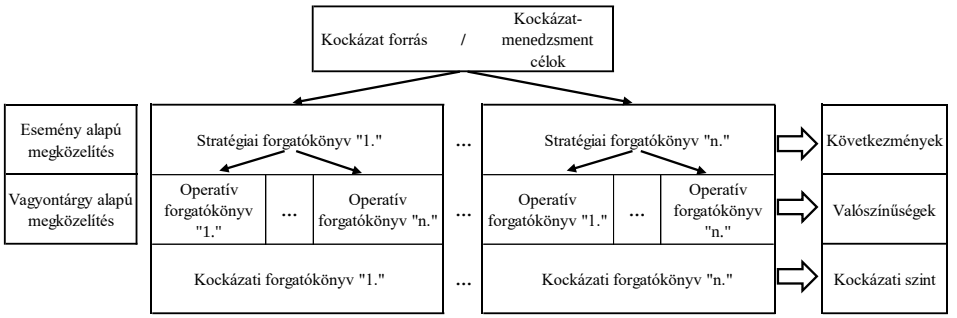
A folyamatok kockázatelemzése a kockázati források (fenyegetések) összegyűjtésén és azok hatásainak elemző vizsgálatát kívánják. Ebben a vizsgálatban szempont lehet folyamatelemek pontos meghatározása, a végrehajtásukhoz szükséges erőforrások rendelkezésre-állása. Gyakorlatilag a folyamatok sebezhetőségeinek strukturált gyűjteménye [7].

BIZONYTALANSÁG A KOCKÁZATELEMZÉSBEN

Ismeretek és tapasztalatok hiányában nem megoldott a korábban még nem bekövetkezett kockázati események kockázat becslése és kezelése. A kockázat leltárban megfogalmazott kockázati események helyett gyakran csak veszélyeket, fenyegetettségeket, gyengeségeket, bizonytalanságokat vagy biztonsági problémákat nevezünk meg bekövetkezési valószínűség és a kár nagyságának megadása, mérése vagy becslése nélkül. A bizonytalanság információhiányt is jelent és a kockázat nem létezik bizonytalanság nélkül [4].

A kockázatelemzés vagyontárgy- (A.2.4) és eseményalapú (A.2.5) az ISO/IEC 27005-ös szabvány szerint [23]. A vagyontárgy alapú megközelítés a jelentős értékű, vagy más szempontból fontos vagyontárgyak sérülékenyégeit, ill. az ezt kihasználni képes fenyegetéseket veszi számba. Az esemény alapú megközelítés a kockázatok forrásából indul ki (elsősorban szándékos károkozók motiváció és az általuk elérni kívánt célok). Előbbi valószínűségeket is tartalmazó operatív forgatókönyveket (operational scenario), míg utóbbiak következményeket megadó stratégiai forgatókönyveket (strategic scenario) eredményeznek. Minden operatív forgatókönyv összeköthető legalább egy stratégiai forgatókönyvvel, ill. egy stratégia forgatókönyvhöz tartozhat több operatív forgatókönyv (2. ábra). Ezeknek a kapcsolatoknak a folyománya a kockázat szintjét (risk level) is meghatározó kockázati forgatókönyv (risk scenario). Kétségtelen, hogy ha stratégiai forgatókönyvekhez nem tudunk minden fontos operatív forgatókönyvet hozzárendelni, akkor a kockázatelemzésünk hiányos lehet.

A szervezet, vállalat dolgozói és vezetői, üzleti partnerei gyakran szubjektív módon látják a várható kockázati eseményeket. Ezek sokszor befolyásolják a folyamatos, „együttfutó" csoportos kockázatértékelés eredményét. Nevezzük ezeket a kockázatokat „érzékelt" kockázatnak. A kockázatmenedzsmentben járatos szakemberek által, a folyamatok indítása előtt elvégzett tapasztalat alapú kockázatelemzés adja az „azonosított" kockázatokat. A két halmaz nem mindig fedi egymást, sőt általában nem egyezik a nem mindig feltárt „valós" kockázatokkal. A kockázat-érzékelés alapvetően meghatározhatja a szervezet tagjainak tevékenységeit és viselkedését is [21].



2. Ábra: Kockázati forgatókönyveken alapuló kockázatértékelés (ISO/IEC 27005 szabvány„A" melléklete alapján) [23]

KÖVETKEZTETÉSEK

Egységes, azonos mérési skálán történő kockázatértékelés javasolt minden üzleti- és technológiai folyamatot figyelembe véve [6].

A „funkcionális", részterületekre fókuszáló kockázatmenedzsment helyett alkalmazott integrált, folyamatalapú kockázat elemzés és -kezelés növelheti vállalati biztonsági szintjét [8].

Jó, ha az integrált kockázatmenedzsment a szervezeti erőforrások rendelkezésre állásán, annak elemző és előrejelző vizsgálatán (is) alapszik. Fontos a kockázatmenedzsment rendszer kialakításakor, hogy az ide vonatkozó ajánlások és szabványok közül melyeket akarjuk alkalmazni (mit vár el a környezetünk?), azokat hangoljuk össze a szervezet új, integrált kockázatkezelési gyakorlatával.

FELHASZNÁLT IRODALOM

[1] A. Balogh, Kockázatmenedzsment és kockázatértékelés. *Magyar Minőség*, XX. évf. 03. szám, 2011., pp. 6-25.

[2] H. Cendrowski and W.C. Mair, *Enterprise risk management and COSO. A Guide for Directors, Executives and Practitioners.* New York, John Wiley & Sons, 2009.

[3] Sz. Farkas és J. Szabó, *A vállalati kockázatkezelés kézikönyve.* Dialog Campus Kiadó, Budapest – Pécs, 2005.

[4] I. Fekete, Integrált kockázatmenedzsment a gyakorlatban. *Vezetéstudomány*, XLVI. évf., 1. szám, 2015., pp. 33-46.

[5] I. Fekete, Folyamat alapú működési kockázatfelmérés - kockázatelemzés alapú belső ellenőrzés. *Egészségügyi Gazdasági Szemle*, 2009/6., pp. 5-10.

[6] Zs. Horváth, A kockázatkezelés alkalmazási területei. Magyar Minőség, XX. évf., 03. szám, 2011., pp.15-24.

[7] Zs. Horváth, Kockázatmenedzsment a vállalati sikeresség érdekében. *Magyar Minőség*, XXVI. évf. 01. szám, 2017., pp. 16-24.

[8] Zs. Horváth és P. Szlávik, Vállalati integrált kockázatkezelés I. *Magyar Minőség,* 2011/3., pp. 124-129.

[9] Zs. Horváth és P. Szlávik, Vállalati integrált kockázatkezelés II. *Magyar Minőség*, 2011/4., pp. 219-226.

[10] T. Jenei, Leggyakrabban használt kockázatkezelési modellek összehasonlítása. *International Journal of Engineering and Management Sciences*, Évf. 1., 1. szám, 2016., p.11, doi: 10.21791/IJEMS.2016.1.22
[11] Á. Kemendi, Integrált kockázatkezelés. *Biztonságtudományi Szemle*, IV. évf., 1. szám, 2022., pp. 43-61.
[12] F.H. Knight, *Risk, Uncertainty, and Profit*, Boston and New York, Houghton Mifflin Co., The Riverside Press. 1921. [on-line] Elérhető: www.econlib.org/library/Knight/knRUP.html?chapter_num=9#book-reader
[13] A. Koncz and L. Pokorádi and Gy. Szabó, Failure Mode and Effect Analysis and Its Extension Possibilities. *Repüléstudományi Közlemények*, 30. évf., 1. szám, 2018., pp. 247-254.
[14] Tné. Mógor és Z. Rajnai, Elektronikus adatkezelő rendszerek kockázatelemzése, kockázati módszerek bemutatása. *Bolyai Szemle*, XXIII. évf. 2. szám, 2014., pp. 43-59.
[15] M. N. Mupa and F. R. Chiganze and T. I. Mpofu and R. M. Mubvuta, The Role of Enterprise Risk Management (ERM) in Supporting Strategic Decision-Making Processes in the Energy Sector. *IConic Research and Engineering Journals*. Vol.8. Issue 2., 2024., pp. 826-848.
[16] N. Racz and E. Weippl and A. Seufert, A process model for integrated IT governance, risk, and compliance management. Proceedings of the Ninth Baltic Conference on Databases and Information Systems, 2010., p.15.
[17] S. Répás és I. Dalicsek, Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében. *Pro Publico Bono - Public Administration*. Vol. 3 No. 4, 2015., pp. 22-33.
[18] K. S. Shrader-Frechette, Kristin, *Risk analysis and scientific method*. D. Reidel Publishing Company, 1985., p.232.
[19] M. K. Starr, Rendszerszemléletű termelésvezetés, termelésszervezés. Közgazdasági és Jogi Könyvkiadó, 1976., p. 619.
[20] S. Takács and A. Tóth, Folyamatmenedzsment a fizikai biztonság területén. *Magyar Rendészet*. 2024/2. pp.105-120. doi:10.32577/mr.2024.2.6
[21] T. Vasvári Tamás, Kockázat, kockázatészlelés, kockázatkezelés - szakirodalmi áttekintés. *Pénzügyi Szemle.* 2015/1. pp.29-48.
[22] Z. Yazar, A Qualitative Risk Analysis and Management Tool - CRAMM. Global Information Assurance Certification Paper Version 1.3. SANS Institute (InfoSec Reading Room), 2000-2005. p.14. [on-line], Elérhető: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysis-management-tool-cramm/103133
[23] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks.
[24] ISO/IEC 31010:2019 Risk management - Risk assessment techniques
[25] ISO/IEC 33004:2015 Information technology - Process assessment - Requirements for process reference, process assessment and maturity models
[26] ISO/IEC 38500:2024 Information technology - Governance of IT for the organization
[27] MSZ ISO 28001:2024 Az ellátási lánc biztonságirányítási rendszerei. Az ellátási lánc biztonságának, felméréseinek és terveinek megvalósítására vonatkozó legjobb gyakorlatok. Követelmények és útmutató (Security management systems for the supply chain.

Best practices for implementing supply chain security, assessments and plans. Requirements and guidance)
[28] MSZ ISO 31000:2018 Kockázatmenedzsment. Irányelvek.
[29] MSZ ISO/IEC 20000-1:2019 Informatika. Szolgáltatásmenedzsment. 1. rész: A szolgáltatásirányítási rendszer követelményei.
[30] MSZ ISO/IEC 20000-2:2024 Informatika. Szolgáltatásmenedzsment. 2. rész: Útmutató a szolgáltatásirányítási rendszerek alkalmazásához (Information technology. Service management. Part 2: Guidance on the application of service management systems)
[31] MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények (ISO 9001:2015)
[32] MSZ EN ISO 14001:2015 Környezetközpontú irányítási rendszerek. Követelmények alkalmazási útmutatóval (ISO 14001:2015)
[33] MSZ EN ISO 22301:2020 Társadalmi biztonság és rugalmasság. Üzletmenetfolytonossági irányítási rendszerek. Követelmények (ISO 22301:2019, angol nyelvű)
[34] MIL-STD-882E, System Safety. Department of Defense. Standard Practice. USA, 2012.
[35] AIAG & VDA, *Hibamód és Hatás Elemzés - FMEA Kézikönyv*, 2019
[36] Belső Ellenőrök Magyarországi Közhasznú Szervezete, Ajánlás a COSO kockázatkezelési keretrendszer alkalmazására, 2023., p.20.
[37] CObIT 5, Vállalati IT irányítás és menedzsment üzleti keretrendszere. ISACA 2012., p. 104.
[38] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management* (Compliance Risk Management: Applying the COSO ERM Framework), 2020., p. 48.
[39] Institution of Mechanical Engineers, *ALARP for Engineers*: A Technical Safety Guide. Report, 2024., Version: 1.1.
[40] Project Management Institute, *Projektmnedzsment Útmtató* (Project Management Body of Knowledge - PMBOK Guide. Akadémiai Kiadó, 2006.
[41] AIRMIC - Association of Insurance and Risk Managers, ALARM - The National Forum for Risk Management, IRM - Institute of Risk Management, *A Risk Management Standard*, 2002.
[42] Supply Chain Council. *Supply Chain Operations Reference (SCOR) Model. Overwiev*. Version 10.0, 2010. [on-line], Elérhető: https://pessolutions.com/wp-content/uploads/2018/02/SCOR10-Overview.pdf
[43] Trusted Business Partners Kft. (szerk. Iványos János): *Kockázatkezelési kézikönyv v.2.1.* (Irányítási forgatókönyvek alkalmazása az integrált vállalati kockázatkezelés megvalósítására), 2014., p.93.

DOI: https://doi.org/10.12700/btsz.2025.7.1.35

A BRIEF OVERVIEW OF OF BODY CAMERA APPLICATIONS (PART 1)

A TESTKAMERA ALKALMAZÁSÁNAK RÖVID ÁTTEKINTÉSE (1. RÉSZ)

ILLÉS Mihály[1] – SZŰCS Endre[2]

Abstract

As part of security processes, surveillance and its results have always played an important role in human life. The Police must process and interpret the significant amount of information generated as a result of surveillance and action processes within the framework of the highest degree of objectivity that can be expected. The new surveillance tool is the body camera, which, as a result of technological development and the opportunity provided by miniaturization, has appeared in the Police's equipment as part of everyday service wear. The reasons for striving to use it included increasing the transparency of the action process, supporting the evidentiary process and public trust in law enforcement agencies. With the development of technology, the initial technical and data recording problems, as well as the processes for processing, using and managing the generated data, have been significantly reclassified in many respects. Our overview covers the countries that were the first to use body cameras.

Keywords

security, camera, development, observation, police action, data recording

Absztrakt

A megfigyelés és annak az eredménye mindig fontos szerepet töltött be az ember életében. A Rendőrség munkavégzése során a megfigyelési és intézkedési folyamatok eredményeként keletkezett jelentős mennyiségű információ feldolgozását és értelmezését az elvárható legnagyobb mértékű objektivitás keretein belül kell, hogy teljesítse. A megfigyelés új eszköze a testkamera, ami a technikai fejlődés, a miniatürizálás nyújtotta lehetőség eredményeként, a mindennapi szolgálati viselet részeként jelent meg. Alkalmazására való törekvés indokai között az intézkedési folyamat átláthatóságának növelése, bizonyítási eljárás és a rendvédelmi szervek felé irányuló lakossági bizalom támogatása is szerepelt. A technológia fejlődésével a kezdeti technikai és adatrögzítéssel kapcsolatos problémák, valamint a keletkezett adatok feldolgozására, felhasználására és kezelésére létrejövő folyamatok sok tekintetben jelentősen átminősültek. Az áttekintésünk a testkamerákat elsőként alkalmazó országokra terjed ki.

Kulcsszavak

biztonság, kamera, fejlődés, megfigyelés, rendőri intézkedés, adatrögzítés

[1] illes.mihaly@bgk.uni-obuda.hu | ORCID: 0009-0002-0307-3136 | assistant lecturer, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi tanársegéd, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

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

BEVEZETÉS

A testkamera, vagy helyesebben testen viselhető kamera (Body Worn Camera, a továbbiakban: BWC) olyan videó-, hang- vagy fényképrögzítő eszköz, amit úgy terveztek, hogy azt a ruházathoz rögzítve törzsön, sisakon, vagy esetleg szemüvegbe építve lehessen viselni. Egyes típusok élő közvetítésre is képesek, illetve felhőtárhelyre tudják felölteni a felvételeket, míg mások csak saját belső tárhelyre (pl. SD-kártya) rögzítenek. Vannak modellek, amik GPS helymeghatározást is tartalmaznak, és olyanok is, amelyek maguktól aktiválódnak, illetve a beépített intelligenciájuk révén automatikusan betartják a használó szervezet képrögzítési szabályzatát. A testkamerák számos felhasználási területtel és kialakítással rendelkeznek. Eredetileg a rendőrök számára fejlesztették ki ezeket az átláthatóság és az elszámoltathatóság növelése érdekében. A rendőrségi alkalmazás az elmúlt évtizedben széles körben elterjedt, és ez a legismertebb, de ma már számos hivatal és szakma alkalmazza az eszközt. Például közterület-felügyelet, biztonsági szolgálatok, közlekedési ellenőrök, egészségügyi dolgozók, mentők, tűzoltók, az intézkedések rögzítésére, a szabálysértések dokumentálására, az agresszív helyzetek kezelésére, és az erőszakos támadások visszaszorítására. Az egyéb felhasználási területek közé tartoznak a közösségi és szabadidős célokra szolgáló kamerák, a katonai sisakkamerák, orvosi, kutatási stb. eszközök.

A rendőrségi testkamerák legnyilvánvalóbb előnye az lehet, hogy javítja az átláthatóságot, könnyebbé teszi a bizonyítást úgy az eljáró rendőr, mint az állampolgár viselkedésének tekintetében, és ezzel növeli a lakosság rendvédelmi szervekbe vetett bizalmát. A kamerák felvételei főleg az Amerikai Egyesült Államokban (United States of America, a továbbiakban: USA) az afroamerikaiakkal szembeni intézkedéseknél bizonyultak hasznosnak, és ennek köszönhető, hogy az amerikai rendőrök támogatják a kamerák viselését. A BWC-k alkalmazását azonban sokan kritizálják a költségek miatt. A kezdeti kis hardverberuházás hamar eltörpül az adminisztrációs és az adattárolási költségek mellett. Főleg ezek a költségek okozzák azt, hogy a testkamerák terjedése az utóbbi időben lelassult.

Egyesek felhívják figyelmet, hogy a kamerák rendőrök és civilek viselkedésére gyakorolt hatását vizsgáló kutatások vegyes eredményeket hoztak. Mások úgy vélik, hogy ez a technológia nem olyan, mint egy villanykapcsoló, amit csak meg kell nyomni, és máris jelentkezik a várt hatás, hanem idő kell, amíg elérik a kívánt eredményt, és sok múlik a szabályozáson és a végrehajtáson. Az eszközök elterjedése adatvédelmi aggályokat is felvet, hiszen a rögzített felvételek kezelésére szigorú szabályokat kell alkalmazni. Ráadásul a legújabb készülékek már automatikus arcfelismerést is alkalmaznak, és a felvételek tömeges elemzésére és adatbázisokkal való összekapcsolására alkalmas mesterséges intelligenciát (Artifical intelligence, a továbbiakban: AI) használó technológiát. Emiatt a legtöbb kritika eddig a Google Glass headsetet érte.

A közvélemény és a sajtó gyakran kérik a felvételek kiadását a nagy horderejű eseményekről, például rendőri fegyverhasználatról, hogy megnézzék magukat az incidenseket, és levonhassák saját független következtetéseiket. A videók közzétételét azonban különböző személyek eltérően értelmezhetik. Ahhoz, hogy ezt a jelenségkört jobban megértsük, érdemes áttekinteni a testkamerák történetét és alkalmazásának tapasztalatait. A külföldi alkalmazások tapasztalatait irodalomkutatás és feldolgozás módszerével végezzük el.[1][2]][3][4]

ELŐZMÉNYEK

Bár a testkamerák koncepciója viszonylag modern, az ötlet nem új. A Rendőrség és a katonai szervek már az 1950-es és 60-as években kísérleteztek hordozható kép- és hangrögzítőkkel, de a technológia túl nagy és nehézkes volt. Az 1980-as években jelentek meg az USA-ban a járőrautók műszerfalára szerelt kamerák (dashcam-ek), hogy rögzítsék a rendőri intézkedéseket. Ezeket az eszközöket bizonyos szempontból a testkamerák előfutárainak tekinthetjük. Az 1990-es években a technológia egyre kisebb és könnyebb lett, de még mindig nem terjedt el széles körben. Csak 2005-ben kezdődtek meg a testkamerák alkalmazására az első nagyobb kísérletek az Egyesült Királyságban (United Kingdom, a továbbiakban: UK és az Egysült Államokban, hivatalos bevezetésükre pedig az UK-ban 2007-ben, az USA-ban pedig 2010-ben került sor. Az első kísérletek biztató eredményeket hoztak, például Devon és Cornwall megyében (UK), 2005-ben, a program első 10 hetében 8%-kal csökkent az erőszakos incidensek száma. Hasonlóan pozitív tapasztalatokkal járt Arizona és Kalifornia három önkormányzatának kísérleti programja, ahol az eljáró rendőrökkel szembeni panaszok drasztikus csökkenését figyelték meg.

A kezdeti biztató tapasztalatok ellenére nem terjedt el széles körben a technológia. A fordulópontot az USA-ban a 2014-es Ferguson-eset hozta el. Amikor a missouri rendőrtiszt, Darren Wilson megölte a 18 éves afroamerikai Michael Brownt és emiatt Fergusonban zavargások törtek ki, hatalmas társadalmi nyomás nehezedett a Rendőrségre, hogy átláthatóbbá tegyék intézkedéseiket. Az Obama-kormányzat 23 millió dolláros támogatást biztosított testkamerák bevezetésére a Rendőrség számára, ezzel elérve, hogy a bűnüldöző szervek közel felénél 2016-ra általánosan alkalmazzák ezeket. Ettől kezdve a testkamerák gyors ütemben terjedtek világszerte, nemcsak a rendőrségnél, hanem más hatóságoknál és szervezeteknél is.

A fokozott átláthatóság iránti igény ellenére a Rendőrségnek és a civil polgárjogi aktivistáknak is aggályai voltak a BWC-k alkalmazásával kapcsolatban. Egyes rendőrök attól tartottak, hogy a kamera aláássa a civilekkel való jó kapcsolatot, azok nem lépnek kapcsolatba a rendőrökkel, ha tudják, hogy felveszik őket. Mások arra kérdeztek rá, hogyan védik meg a tanúk személyazonosságát, ha a felvételeket nyilvánosságra hozzák. Az aktivisták eközben aggodalmukat fejezték ki azzal kapcsolatban, hogy kinek van mérlegelési jogköre a rendőrségi testkamerák aktiválása felett, és a felvételek által felvethető esetleges adatvédelmi aggályok miatt. [5][6]

Technikai problémák is előfordultak. Az első generációs kamerákat a műszak végén dokkolni kellett a videó letöltéséhez, ami órákig is eltarthatott. Ez késleltette a jelentésírási folyamatot azon tisztek számára, akik át akarták nézni a videót, hogy a lehető legpontosabb jelentést készítsék. A korai kamerák gyakran leestek a rendőrökről, különösen a gyanúsítottakkal folytatott viták, dulakodások során. A hardver karbantartási költségei gyorsan növekedtek, és a rendőri szerveknek szembesülni kellett az adattárolási és selejtezési munkák költségeivel is. Azóta a technológia hatalmasat fejlődött. A felhőalapú tárolásnak, megnövekedett akkumulátor-üzemidőnek és az egységes rögzítési stratégiák fejlődésének köszönhetően a testkamerák egyre biztonságosabbak, áramvonalasabbak, hatékonyabbak és megfizethetőbbek.

Ahogy a rendőrségi testkamerák egyre általánosabbakká váltak, a fejlesztők elkezdtek kísérletezni azzal, hogy a mesterséges intelligencia hogyan egészítheti ki a meglévő

technológiát. Az egyik jelentős és sokat vitatott terület az arcszkennelés és felismerés: az AI a testkamerák felvételei között keresi az arcokat, rögzíti a jellemzőiket, és összehasonlítja őket egy arcadatbázissal, hogy azonosítsa a személyeket. A technológia egyelőre rendkívül ellentmondásos, adatvédelmi aggályokat vet fel, és gyakran hamis pozitív azonosításokat generál a vizsgálatok során, különösen az afroamerikai és ázsiai férfiak azonosításakor. Ezért sok arcfelismerő szoftvert fejlesztő cég nem támogatja vagy egyenesen tiltja termékük rendőrségi környezetben történő használatát. Más AI alkalmazások ígéretes lehetőségeket biztosítanak az etikus felhasználás mellett. Például az AI azon képessége, hogy lehetővé teszi a beszéd azonnali átírását a testkamerás videóból, ezáltal elősegíti az érintettek gyorsabb kihallgatását és a hatékonyabb jegyzőkönyvkészítést. Családon belüli erőszak esetén különösen fontos lehet ez, hiszen azonnal lehetővé teszik az intézkedést a bántalmazók ellen ahelyett, hogy az áldozatokat előbb berendelnék egy másnapi kihallgatásra.[7][8][9][10][11]

TESTKAMERA HASZNÁLATA KÜLFÖLDÖN

A testkamerák bár nem tekinthetők csodaszernek, és egyes kezdeti várakozások ma már túlzónak tűnnek, bebizonyosodott, hogy a rendőri intézkedések során hasznosak, és különösen a kisebb súlyú bűncselekmények gyorsabb elbírálását is segítik, megkönnyítik a vádemelést, és felgyorsíthatják a bűnösség bizonyítását. Ennek ellenére a testkamerák alkalmazásában országonként jelentős eltérések vannak. A következőkben néhány országon keresztül megvizsgáljuk tesztelésüket és bevezetésüket, majd következtetéseket vonunk le az alkalmazásuk sikerességével kapcsolatban.

Egyesült Királyság

Mint már említettük, az UK-ban a videórendszer alkalmazását kis léptékben a Devon és Cornwall Rendőrsége kezdte meg 2005-ben. Az első eszközök egyike látható az alábbi képen. Érdemes megfigyelni az alábbi képen, hogy a fejre elhelyezhető (fül fölött hordható) videókamera itt még külön egység, és kábellel csatlakozik a különálló, monitorral is felszerelt rögíztőegységhez.

1. ábra Olly Tayler rendőr őrmester a devoni és cornwalli egység tagja videókamerával és a különálló monitorral és rögzítő egységgel, https://www.nbcnews.com/id/wbna19750278#.VN-wl_nF8y4

A testkamerák első jelentős országos bevetését 2006-ban a Rendőrségi Szabványügyi Egység (Police Standards Unit, a továbbiakban: PSU) végezte a családon belüli erőszak elleni kampányuk során. A kedvező tapasztalatok hatásra a Belügyminisztérium jelentést tett közzé, amelyben megállapították, hogy „a bizonyítékok gyűjtése ezzel a berendezéssel radikálisan javíthatja a rendőrség teljesítményét." Belügyminisztérium kiemelte, hogy a kamerát viselő rendőrökkel szembeni panaszok nullára csökkentek, és 22,4%-kal csökkentették a papírmunkára fordított időt, ami 9,2%-kal növelte a járőrözéssel töltött időt. A testkamerák jól szerepeltek, a közvélemény is kedvezően fogadta. A Biztonsági Ipari Hatóság (Security Industry Authority, a továbbiakban: SIA) arra jutott, hogy a korábbi közterület-felügyeleti térfigyelő rendszerek (CCTV) jogi szabályozása kiterjeszthető a testkamerákra is, így lényegében a jogi keretek is adottak voltak.

A pilot projektet követően 2008-ban a Hampshire-i Rendőrség elkezdte használni a technológiát a Wight-sziget és a szárazföld egyes részein. Öt évvel az első tesztek megkezdése után, 2010-ben már 40 rendőri egységnél jelen volt a testkamera, ami immár egy egységben tartalmazta a videókamerát és az adattárolót is.

2013-ban a Belügyminisztérium kiadott egy gyakorlati kódexet kamerák használatára vonatkozóan. Eszerint a brit rendőrségi testkamerák nem rögzítenek folyamatosan, hanem a tisztviselők manuálisan aktiválják őket az intézkedések során. A kamera bekapcsolásáról az érintett személyeket lehetőség szerint tájékoztatni kell. A kamerák képet és hangot is rögzítenek, ami bizonyítékként felhasználható bírósági eljárások során. A rögzített felvételek az adatvédelmi törvények szerint kezelendők, és csak meghatározott ideig tárolhatók (általában 31 nap).

2014-ben a UK legnagyobb rendőri egysége, a Metropolitan Police Service nagyszabású testkameraprogramot indított Londonban. A kedvező tapasztalatok, a rendőri intézkedésekkel kapcsolatos panaszok továbbá az agresszív viselkedés csökkenése, és a használható bizonyítékok miatt úgy döntöttek, hogy 22.000 kamerát osztanak ki a rendőreik között. A következő nagyobb beszerzést az Észak-Írországi Rendőrszolgálat hajtotta végre.

A brit kormány további forrásokat biztosított, így az Egyesült Királyság legtöbb rendőri egysége testkamerákat kapott. Mára a testkamera alapvető felszerelési eleme az Egyesült Királyság rendőreinek, széles körben elfogadott és bizonyítottan hasznos eszköz a rendfenntartásban. [12]]13]

Finnország

A finn Rendőrségénél viszonylag későn kezdték meg a testkamera alkalmazásának tesztelését. Az első tesztprogramokat Helsinki rendőrsége végezte 2015-2017-ben, s csak 2018-ban kezdték bevezetni országosan, főként közrendvédelmi és tömegrendezvényeken szolgálatot teljesítő egységeknél.

A pilot projekt alapján arra a következtetésre jutottak, hogy a rendőrök biztonsága javult, csökkent a Rendőrséggel szembeni ellenállás, és javult az intézkedések átláthatósága. Ugyanakkor Finnországban a felvételek készítésére és tárolására nagyon szigorú adatvédelmi szabályok vonatkoznak. A testkamerák otthonokon belüli használata általában nem megengedett, csak ha bűnügyi nyomozás részeként engedélyezik azt. A felvételeket titkosí-

tani kellett, és csak meghatározott szoftverrel lehetett hozzáférni. A rögzített képeket a magánélet védelme miatt 24 óra után törölték, illetve automatikusan felülírták újabb adatfolyammal, kivéve, ha bűncselekményt rögzítettek.

Finnországban a testkamerák használata még nem olyan elterjedt, mint az UK-ban vagy az USA-ban, de folyamatosan fejlődik, és egyre inkább a modern rendészeti eszköztár részévé válik. A kormány által kijelölt munkacsoport szerint indokolt lenne a jogi keretek átgondolása, például a 24 órás korlát legalább 96 órára növelése, illetve annak tisztázása, hogy ki és mikor törölheti a felvételeket. Álláspontjuk szerint a felvételek kezelése nem különbözik a többi rendőrségi dokumentáció kezelésétől.[14]

Hollandia

Holland Királyi Rendőrség különleges egysége a Lovasrendőrség. Általában párban járőröznek a közterületeken, tengerpartokon, ilyenkor a feladataik megegyeznek a gyalogos járőrökével. Hivatalos alkalmakkor, állami rendezvényeken reprezentatív feladatokat látnak el. Bevetéseken ritkán vesznek részt, felvonulásokon, futballmérkőzéseken adnak támogatást a rohamrendőri fellépéshez. Ekkor fontos, hogy az intézkedések minden részlete pontosan dokumentálható legyen. Ennek érdekében már 1997-ben videókamerákat kaptak a lovas rohamrendőrök. A korszerűbb testkamerákkal végzett első, kis léptékű kísérletek 2008-ban kezdődtek, ezekről értékelhető eredményt nem közöltek. Ezt követően 2009 és 2011 között négy nagyszabású kísérletet végeztek, amelyek eredményeit már nyilvánosságra hozták. Ezek alapján az Igazságügyi Minisztérium úgy találta, hogy még nem időszerű a testkamerák bevezetése. A kamerák nem csökkentették a Rendőrséggel szembeni erőszakot és agressziót a várt mértékben, főleg a technikai problémák, és a viselhetőség nehézkessége miatt. A jelentésben azt is megállapították, hogy a felhasznált testkamerák által készített felvételek nem teljes értékűek.

A következő nagyszabású kísérletre 2015-ben került sor, amikor 12 hónapra a Rendőrség számos egysége kapott testkamerát, a legtöbben – mintegy 1500 rendőr – Amszterdamban. A használatot a lehető legmagasabb minőségű módszertani normák szerint, randomizált kontrollált vizsgálatként értékelték ki, és egyértelműen megállapítást nyert, hogy jelentősen csökkent a rendőrökkel szembeni erőszak és agresszió. Ennek alapján már a rendszeresítés mellett döntöttek, de a tényleges alkalmazásra 2019-ig várni kellett és akkor is csak a járőrök és a konkrét bevetéseken résztvevők számára biztosítottak testkamerákat.

A Rendőrségen kívül használja a testkamerát a városi rendészet, a mentők, a tűzoltók, a biztonsági őrök és a tömegközlekedési ellenőrök.[15][16]

Svédország

Svédországban az első testkamerás kísérletek 2017-ben kezdődtek kisebb léptékben, olyan városokban (Göteborgban, Södertäljében és Stockholm külvárosaiban, Rinkebyben és Botkyrkában), ahol a rendőri intézkedésekkel szembeni panaszok magasabb számban jelentkeztek. A tesztidőszak célja az volt, hogy megvizsgálják, milyen hatással van a testkamera használata a rendőri munka hatékonyságára és az állampolgári bizalomra. Speciális célokra használták őket, eleve nem látták szükségesnek, hogy rendőri intézkedést nagy részét dokumentálják.

A kezdeti próbálkozások pozitív benyomásokat hoztak, különösen az agresszió csökkentése és a panaszok tisztázása terén. Az első tudományos igénnyel a Svéd Bűnmegelőzési Tanács által kiértékelt tesztre 2018–19-ben került sor stockholmi rendőrségnél. Ennek értékelése során arra jutottak, hogy a testkamerák alkalmazásakor viszonylag szerény mértékben jelentkeznek a pozitív hatások. Az erőszak bizonyos formái, a zaklatás, a fegyveres erőszak, a nők szexuális megfélemlítése csökkent, a rendőrökkel készült interjúk szerint a velük szemben tanúsított verbális agresszió is ritkábban fordult elő. Az intézkedés alá vont személyek részéről a fizikai erőszak viszont nem csökkent ugyanilyen mértékben. Ennek magyarázata az, hogy Svédországban a közbiztonság kiemelkedően jó, ilyen típusú erőszakos cselekményeket főleg ittas vagy zavart elméjű személyek követtek el. A felvételeket ritkán használták bizonyítékként a bíróságokon, és akkor is az esetek felében végül kivették azokat a bizonyítékok közül. Megfigyelték azt is, hogy a kísérletben résztvevő rendőröknél a testkamerák aktivitása szélsőségesen változatos volt. A kutatók szerint a rendőrök nem kaptak egyértelmű utasítást arra, hogy milyen esetekben kell az eszközt használni. Ha ez megtörtént volna, akkor jobb eredmények születtek volna.

A kísérleteket követően 2018-ban a svéd kormány jóváhagyta a testkamerák szélesebb körű bevezetését. Először a nagyvárosokban, például Stockholmban, Göteborgban és Malmöben alkalmazták őket. A 2020 augusztusában kezdődött Korán-lázadások során bebizonyosodott, hogy ha nagyobb számban álltak volna rendelkezésre a testkamerák, több elkövetőt letartóztattak volna. Ez nagyot lendített a testkamerák egész országra történő alkalmazásának kiterjesztésére.

Az egyik legfontosabb kérdés továbbra is az adatvédelem és a személyes jogok védelme. Svédország szigorú adatvédelmi törvényeket alkalmaz, és folyamatosan felülvizsgálják a testkamerás rendszerek működését annak érdekében, hogy azok ne sértsék az állampolgárok jogait. A testkamerák technológiája folyamatosan fejlődik, és egyre inkább integrálják őket más rendszerekkel, például mesterséges intelligenciával működő arcfelismerő programokkal. Svédországban azonban az arcfelismerés rendőrségi használata egyelőre erősen korlátozott jogi és etikai okokból.

Más területeken is alkalmazásba vették a testkamerákat 2018-ban, mint a vagyonőrök, a vasúti vendéglátó személyzet, valamint a tömegközlekedési ellenőrök.[17][18][19][20][21]

ÖSSZEFOGLALÁS

Összességében megállapítható, hogy a testkamerák bevezetése egy átgondolt és fokozatos folyamat eredménye volt a vizsgált országok esetben. Az eszközök használata hozzájárult az agresszív helyzetek csökkentéséhez, a rendőri munka átláthatóságának növeléséhez és a bizonyítékgyűjtés hatékonyságának javításához. A rendőri munkavégzés biztonságához is hozzájárul a testkamera alkalmazása, melynek a hatékonysága is nő. Bár vannak még megoldásra váró kihívások, főleg a magánélet védelméről szóló aggályok miatt. A bemutatott országok közül az USA-ban, a UK-ban a testkamerák egyértelműen a modern rendfenntartás egyik fontos eszközévé váltak.

FELHASZNÁLT IRODALOM

[1] N. P. Institute, „National Policing Institute,” 2025.01.25. június 2020. [Online]. Elérhető: https://www.policinginstitute.org/publication/police-body-cameras-what-have-we-learned-over-ten-years-of-deployment/.

[2] C. Lum, C. Koper, D. Wilson, M. Stoltz, M. Goodier, E. Eggins, A. Higginson és L. Mazerolle, „Body-worn cameras' effects on police officers and citizen behavior: A systematic review,” Campbell Syst Rev., 2020 Sep.

[3] J. Doleac, „Do Police Body-Worn Cameras Reduce the Use of Force?,” Econfact, 17 11 2017. [Online]. Elérhető: https://econofact.org/do-police-body-worn-cameras-reduce-the-use-of-force.

[4] T. Brewster, „The Many Ways Google Glass Users Risk Breaking British Privacy Laws,” Forbes, 30 05 2014. [Online]. Elérhető: https://www.forbes.com/sites/thomasbrewster/2014/06/30/the-many-ways-google-glass-users-risk-breaking-british-privacy-laws/.

[5] „CSE Crosscom,” 20 09 2022. [Online]. Elérhető: https://csecrosscom.co.uk/when-were-body-worn-cameras-first-introduced/.

[6] „Police Use Body Worn Video, A Brief History,” 18 01 2018. [Online]. Elérhető: https://americanpoliceofficersalliance.com/police-use-body-worn-video-brief-history/.

[7] M. Roig-Franzia, D. L. Brown és W. Lowery, „In Ferguson, three minutes — and two lives forever changed,” The Washington Post, 16 08 2014. [Online]. Elérhető: https://www.washingtonpost.com/politics/in-ferguson-three-minutes--and-two-lives-forever-changed/2014/08/16/f28f5bc0-2588-11e4-8593-da634b334390_story.html.

[8] O. Johnson és E. Smith, „Boston brass, police union fear body cams on cops,” Boston Herald, 03 12 2014. [Online]. Elérhető: https://www.bostonherald.com/2014/12/03/boston-police-brass-union-wary-of-cameras-on-cops/.

[9] J. Dombkowski, „The Body-Worn Camera Evolution—Increase Security with Uniform Integration and Eliminating Docking Stations,” Police Chief, [Online]. Elérhető: https://www.policechiefmagazine.org/the-body-worn-camera-evolution/. [Hozzáférés dátuma: 10 12 2024].

[10] C. M. Natasha Singer, „Many Facial-Recognition Systems Are Biased, Says U.S. Study,” The New York Times, 19 12 2019. [Online]. Elérhető: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

[11] „Axon Case Study Reveals the Power of Police Body Camera Footage for Prosecuting Domestic Violence,” PR Newswire, 14 11 2017. [Online]. Elérhető: https://www.prnewswire.com/news-releases/axon-case-study-reveals-the-power-of-police-body-camera-footage-for-prosecuting-domestic-violence-300555113.html.

[12] J. Cooper, „Smile! Police will soon be filming you as body worn cameras are introduced,” Plymouth Live, 01 09 2018. [Online]. Elérhető: https://www.plymouthherald.co.uk/news/plymouth-news/smile-police-soon-filming-you-1954506.

[13] P. Jacques, „MPS to issue latest BWV cameras to frontline officers,” Police Professional, 25 11 2015. [Online]. Elérhető: https://policeprofessional.com/news/mps-to-issue-latest-bwv-cameras-to-frontline-officers/.

[14] H. Kallio, „Haalarikamerat tulevat – poliisit haluavat oikeuden poistaa nauhoilta todisteet virkavirheistään," Turun Sanomat, 12 12 2022. [Online]. Elérhető: https://www.ts.fi/uutiset/3486995.
[15] S. Flight, De mogelijke meerwaarde van bodycams voor politiewerk; een internationaal literatuuronderzoek, Reed Business Amsterdam ISBN: 978-90-3524-946-7, 2017.
[16] S. Flight, „Evaluatie pilot bodycams Politie Eenheid Amsterdam 2017-2018," Politie en Wetenschap, 28 04 2019. [Online]. Elérhető: https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2019/focus-evaluatie-pilot-bodycams-politie-eenheid-amsterdam-329/#files.
[17] K. Wettre, „Stockholm police to start using body cameras," Sveriges Radio, 10 03 2017. [Online]. Elérhető: https://www.sverigesradio.se/artikel/6649196.
[18] „Minskad utsatthet för poliser med kroppsburna kameror," Brå, 19 02 2020. [Online]. Elérhető: https://web.archive.org/web/20200220163150/https:/www.bra.se/om-bra/nytt-fran-bra/arkiv/press/2020-02-19-minskad-utsatthet-for-poliser-med-kroppsburna-kameror--pressmeddelande.html.
[19] K. Nyberg, „Brist på kroppskameror för poliser i yttre tjänst," Sveriges Riksdag, 16 05 2022. [Online]. Elérhető: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/skriftlig-fraga/brist-pa-kroppskameror-for-poliser-i-yttre-tjanst_h9111598/.
[20] L. Klint, „Kroppskameror införs i hela landet," Polis Tidningen, 29 11 2022. [Online]. Elérhető: https://polistidningen.se/2022/11/kroppskameror-infors-i-hela-landet/.
[21] P. Pettersson, „Bärbar kamera ökar säkerheten i utsatta jobb," ARBETARSKYDD, 30 09 2015. [Online]. Elérhető: https://www.arbetarskydd.se/arbetsmiljo-overvakning/barbar-kamera-okar-sakerheten-i-utsatta-jobb/1463022.

DOI: https://doi.org/10.12700/btsz.2025.7.1.45

APPEARANCE OF DIGITAL COMPETENCES IN THE COMMUNICATION AND MOBILE USING HABITS OF PARTICIPANTS IN THE HONVÉD CADET PROGRAM

DIGITÁLIS KOMPETENCIÁK MEGJELENÉSE A HONVÉD KADÉT PROGRAMBAN RÉSZTVEVŐK KOMMUNIKÁLÁSI ÉS MOBILHASZNÁLÁSI SZOKÁSAIBAN

KISS Csaba[1]

Abstract

IT applications common in the civilian field have also appeared in the military field, the best example of which is the digital soldier. We equip the soldier with IT tools so that the data necessary to fight the battle is immediately available to him. In this way, you get a screen and a camera on the practitioner's clothes, which, when connected to a system, become part of an IT network. Communication can be done through the microphone or the touch screen, just like on home computers or as the society that grew up using mobile phones is used to. Can everyone become a digital soldier? The publication analyzes the existence of the digital soldier's digital competencies based on a large-scale questionnaire among military cadets.

Keywords

digital soldier, ability, digital competence

Absztrakt

A civil területen megszokott informatikai alkalmazások megjelentek a katonai területen is, a legjobb példa erre a digitális katona. A katonát felszereljük informatikai eszközökkel, hogy a harc megvívásához szükséges adatok rögtön azonnal elérhetőek legyenek a számára. Így egy képernyőt és kamerát is kap a gyakorló ruhájára, amit egy rendszerbe kötve egy informatikai hálózat része, eleme lesz. A kommunikáció a mikrofonon vagy az érintős képernyőn keresztül is történhet, ugyan úgy, mint az otthoni számítógépeken vagy ahogy a mobiltelefon használatán nevelkedett társadalom megszokta. Lehet-e mindenkiből digitális katona? A publikáció elemzi a digitális katona digitális kompetenciáinak a meglétét a katonai kadétok között végzett nagymintás kérdőív alapján.

Kulcsszavak

digitális katona, képesség, digitális kompetencia

[1] kiss.csaba@uni-nke.hu |ORCID: 0000-0002-7265-8704 | PhD student, National University of Public Service, National, Doctoral School of Military Engineering | doktorandusz, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola

INTRODUCTION

The XXI. In the 20th century, the increase in the number of armed conflicts prioritized the modernization of the technical equipment of the armies and the education and training of their operators and personnel. Armies increase their numbers either through their own school system or by recruiting and training the civilian population.

Applicants for armed service bring with them the knowledge and skills they have learned in civil society, under controlled conditions, in the classroom or during independent training. This knowledge enables them to have skills that help them successfully integrate into society and adapt flexibly to changes in the labor market.

The rapid development of information and communication technology tools in the world affects all areas of life and unknowingly changes our daily way of life. Recently, these processes require faster and faster adaptation from both users and manufacturers.

Newer and newer smart devices that appear provide help and support to their users, and in many cases save them time. Without them, we would no longer be able to book an appointment, shop online, talk to our friends across the continent, study, and if we are sick, we would need the IT tools to get our medicine. Knowledge of the use of basic IT tools is already expected at workplaces, and it is also good to have an Internet mail account in case of complaints and requests for information from service providers.

Recognizing this technical change taking place in the world, IT training also appeared in education, and we can get used to interacting with machines and robots almost from preschool age. At school, computers are already a basic tool in education, and almost every student has access to or owns a personal computer, and more and more students are using smartphones, some even tablets.

The demands for the use of IT tools present humanity with new challenges. New challenges make it necessary for users to have new competencies in order to be able to properly adapt to today's requirements. The national defense is no exception to the digital revolution, so the digital soldier appeared as a means of exploiting digital opportunities, along with the competencies necessary for its use.

The recommendation (2018/C 189/01) issued by the Council of the European Union in 2018 [1], which talks about the key competences required for lifelong learning, is aligned with these requirements, as well as the recommendation adopted by the Hungarian Government on June 11, 2019 the government decision "On the development and implementation steps of the Digital Competence Framework" submitted by the Ministry of Innovation and Technology.

Of course, the acquisition of these competencies can be achieved through a learning process. The learning process is strengthened by practical application. The main elements of the digital soldier are already present in civil society. For example, the displays are similar to smartphones, and the communication devices are copies of the usual headphones. The tools of the digital soldier can therefore be identified with the digital tools used in the civilian field, so the use of existing digital tools in the civilian field contributes to the acquisition, i.e. development, of the competencies of the digital soldier.

DIGITAL SOLDIER

Hungary's Artificial Intelligence Strategy [4] was completed in 2020, which defines the introduction and development of AI for a period of 10 years. Based on this, the National Military Strategy of Hungary [5] was published in 2021, which brought with it the appearance of the digital soldier.

The main elements of the structure of the digital soldier:

1. Elements involved in communication: earphones, microphone, radio
2. Elements involved in displaying data: portable computer, displays
3. Elements involved in data collection: sensors, cameras
4. Power supply devices: batteries, energy distributors

In the era of digital communication, it is necessary to be able to provide soldiers with all the information they need to fight. The data received by the driver through the reconnaissance system is processed and then sent to the tablet placed on the arm of the combat soldier. [7] This is how the soldiers see their own situation in the current military maneuver. Digital soldier systems can even be connected to a network, so management can operate at battalion and brigade level. The flow of information also works backwards, because the signal from the sensors (camera) worn by the soldier is connected to a transmitting device, the transmission of which is received by a centrally located receiver, so the commander sees everything that the soldier sees.

It is easy to see that the soldier, with the technical devices on him, has become one of the outsourced data users and data collectors of the management's central computer. It is not possible to receive, process and interpret the data arriving on the devices without digital competences.

DIGITAL COMPETENCES OF A DIGITAL SOLDIER

Competence should be understood as based on knowledge, experience, values and dispositions that can be acquired during learning.[3] According to Zoltán Kerber: "Competence is characterized by the level of autonomy and responsibility that appears during the completion of the task, and the concept includes the use of knowledge, cognitive and practical abilities".

According to the EU's recommendation, digital competence is also among the key competences required for lifelong learning, the reference model of which describes everything that digital competence includes in 5 competence areas as follows:

1. Information and data management
2. Communication and cooperation
3. Creating digital content
4. Security
5. Problem solving

Regarding the device system of the digital soldier, we can say that there is a user (soldier) who only manages the IT device and there is a programmer who programs the device. The user and the programmer are two separate persons, but they can also be the

same person. As a result, since the digital soldier does not create digital content, he only uses the device, so the digital soldier is covered by the 1st and 2nd competence areas, while the programmer is mostly covered by the 3rd area, while cyber defense belongs to the 4th area, the area 5 for education.

Interpretation of the reference model from a military point of view:

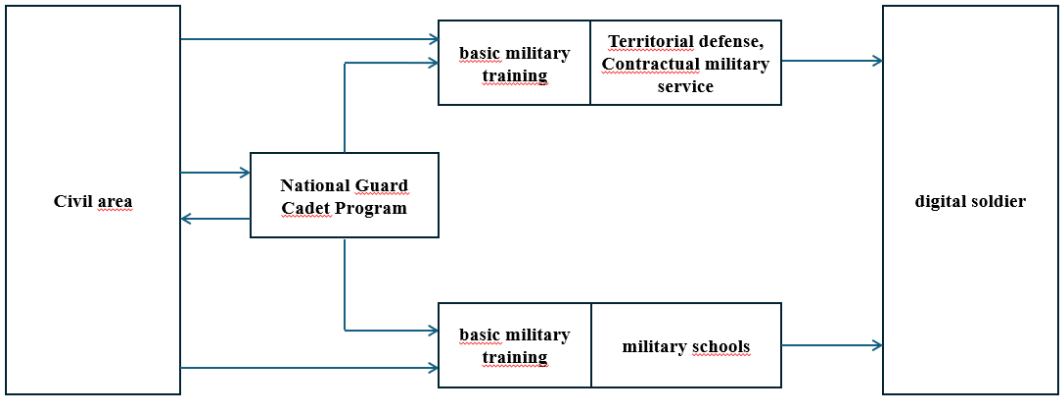
1. Information and data management: Formulation of information needs, search and retrieval of digital data, military information and content. Assessment of the authenticity of the data source and content. Storage, management and organization of digital data, military information and content according to military regulations.

2. Communication and cooperation: Interaction, communication - with superiors and subordinates - cooperation using tools using military digital technologies. Participation in military digital services.

Of course, the acquisition of these competencies can be acquired and deepened during military exercises. The learning process is supervised by military instructors and they help to master the processes necessary for practical application. The used devices can already be found in civil society, as the displays are similar to smartphones, for example, and the communication devices are copies of the usual headphones. For the soldiers to be trained, the tools will not be new, only the usage environment and the method will be different compared to what is usual in the civilian field, so we can say that the use of digital tools in the civilian field contributes to the acquisition of the competencies of the digital soldier. The existence of these was examined by a survey among the cadets of the national defense using a large sample questionnaire.

SURVEY AMONG PARTICIPANTS IN THE NATIONAL GUARD CADET PROGRAM

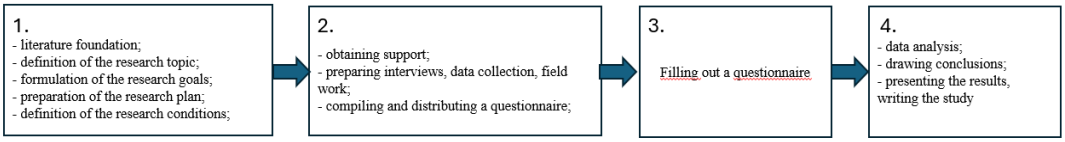
Participants in the National Guard Cadet Program come from the civilian area, and at the end of the training either return to the civilian area or have the opportunity to continue their studies in the military area. Those who apply from the civilian area to become a territorial defense reservist or contract soldier can take part in military training, which can also be done after the cadets of the national army have graduated. Everyone who fulfills the application conditions has the opportunity to apply to a military school, so the cadets of the National Guard also have the opportunity to choose a military career. Those who return to the civilian field after completing the national defense cadet program have the opportunity to continue their work in the military field. Everyone who chooses a military field first participates in military training, so we can say that the path to the digital soldier leads through military training, as shown in Picture 1.



Picture 1.: Connection diagram of participants in the National Guard Cadet Program, own editing

Potential applicants mostly acquire the digital competences required for the digital soldier in the civilian field or in the National Guard Cadet Program.

The research of the digital competencies of the participants in the cadet program took place according to Picture 2.



Picture 2.: Flow chart of research, own editing

The research was supported by the National Defense Sports Association, which gave me a letter of support signed by the general vice-president Dr. György Nébald. This letter of support was a good offer to the school principals, who accepted my request with confidence. I hereby thank the National Defense Sports Association for its support.

Since the National Guard Cadet Program (HKP) in Hungary has 3 levels: HKP I., HKP II. and HKP III., and for interviewing HKP I. and HKP II. was selected because this level of training is offered by civil secondary schools. Mikszáth Kálmán Technikum és Szakképző Iskola was selected from among secondary schools teaching according to the HKP I. program, with a location in Balassagyarmat, while HKP II. among secondary schools that teach according to Than Károly Ökoiskola and Technikum with a location in Budapest.

In both secondary schools, the person in charge of national defense education was appointed by the school principals as the subject of the interview. The areas that stood out during the interviews were the following:

- the interviewees said that there is no longer an IT class in the classical sense, but instead a digital culture class, which is not equivalent to an IT class

- the biggest problem is that students take all the information they find while browsing the Internet as authentic, not they are critical of the information they receive
- the students use social media well, but word processing and spreadsheet management are less successful
- students use the smartphone mostly for communication, they cannot be separated from the smartphone, they can also use the phone during class under the guidance of the teacher
- it is very difficult for the students to transfer the competences needed to create their own portfolio
- the poorer students do not have a laptop, tablet or PC only they have mobile phones
- students are increasingly using artificial intelligence to solve their homework
- the schools have a good relationship with the Hungarian Defense Forces, students go to military demonstrations and the Defense Sports Center
- students' willingness to further study or work in the armed forces is greatly influenced by the amount of salary appearing in military recruitment advertisements in the media
- they like to wear cadet clothes both at school and on the street
- taking the ECDL exam is not mandatory for students
- many students do not participates in the ECDL exam because their scholarship does not increase if they pass the exam
- at the graduation exam students solve a word processing task, a presentation task, a spreadsheet task, a database management task, as well as an algorithmization and programming task from the digital culture subject

Based on the interviews, I prepared the questionnaire with the help of Google Forms, I processed the data obtained with Google Sheets on the one hand, and Libre Office Calc, an alternative to Microsoft Excel, on the other hand, while during the deeper analyzes I used the free software PSPP instead of SPSS. I used the works of Klára Tóthné Lőkös [8], [9], among others, to explore the connections and formulate the conclusions.

The questionnaire was sent to 150 schools where the National Guard Cadet Program was launched. The questionnaire was available from 22.04.2024 until midnight on 12.05.2024. The filling in was completely anonymous, so it is not possible to infer the person filling it in. Schools can access the results of the research through the National Defense Sports Association.

The questions of the questionnaire are grouped around the following topics:

1. Demographic questions (8 questions)
2. Communication (9 questions)
3. Technology (10 questions)
4. Sport-leisure (8 questions)
5. Education (6 questions)

The questionnaire was returned by 808 national defense cadets. The number of questionnaires received corresponds to the statistically determined number of items, on the basis of which my findings can be extended to all participants in the National Guard Cadet Program:

$$n = \left(\frac{\sigma * z}{D}\right)^2$$

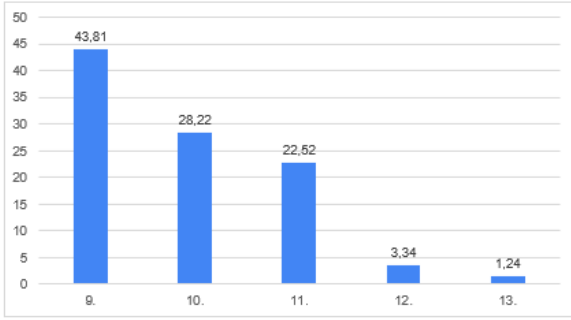
where D (accuracy) =± 5%, CL (confidence level) = 95%, Z = 1.96, σ = between 50-55 (in this case 50), based on the formula n (minimum sample size) = 385

Mandatory responses were not set in the questionnaire, so you could skip the questions or go back to correct the answer you had already given. Due to the non-mandatory response, I interpreted the answers received, which was 808, in percentage distribution.

SURVEY DATA AMONG PARTICIPANTS IN THE NATIONAL GUARD CADET PROGRAM

1. Demographic questions

A total of 808 military cadets returned the questionnaire. Among the respondents, 61.76% are boys and 36.88% are girls. The ratio of women to men in the Hungarian Armed Forces is approx. 20% according to "Data on the Hungarian Armed Forces" published by the Parliamentary Office. The percentage distribution of the respondents according to the Honvéd Cadet Program HKP-I. cadet 60.52% while HKP-II. cadet 31.44% while HKP-III. cadet 3.47%. 9.9% of the respondents live in the capital, 8.17% in the county seat, 45.3% in the city, 35.27% in the village, village, or farm. Picture 3 shows the % distribution of the respondents by year.



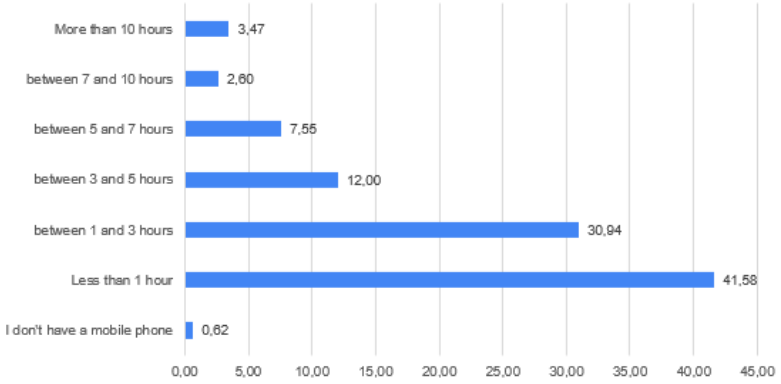
Picture 3.: Percentage distribution of respondents by class, own editing

Distribution of respondents according to residence: 17.08% college students, 23.27% live locally, but not college students, 28.47% do not live locally, the walk (round trip) takes less than 45 minutes, 30.20% not local resides, the walk (round trip) takes more than 45 minutes. 23.51% of the respondents answered that they have a soldier among their close relatives, while 75.5% answered that they do not. Based on the 3rd picture, it can be

seen that the 12th grade took part in filling out the questionnaire in low numbers, this can be explained by the fact that they were preparing for the graduation.

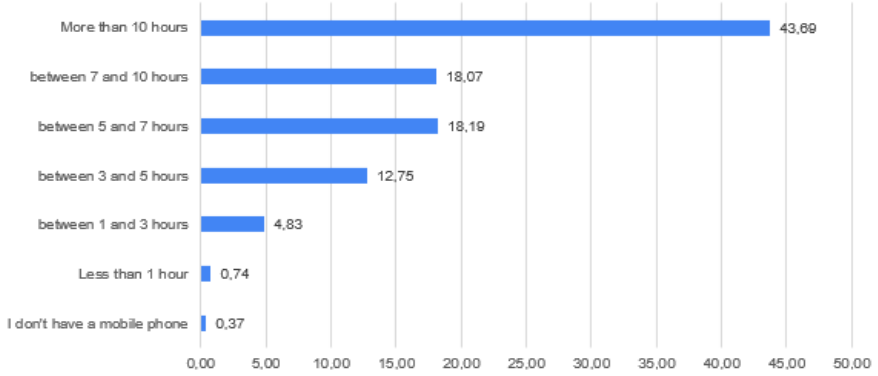
2. Communication

Respondents to the question "How do you keep in touch with your friends?" 4.83% answered the question on the Internet, 23.89% answered in person rather than on the Internet, 1.11% answered with a mobile phone rather than in person, and 69.43% responded equally in person, on the Internet, and with a mobile phone. The respondents to the question "How do you keep in touch with your friends?" to the question, where the respondent could select more than one answer option, 40.84% by video call, 75.99% by chat, 2.85% by e-mail, 6.44% by SMS, 27.6% by Facebook, 1.86% by blogging, 4.33% by Viber, 2.6% by Twitter, 59.03% by phone call, 81.06% chose a conversation, 25% chose another method. Picture 4 shows the respondents' mobile phone calling time in weekly average and percentage form.



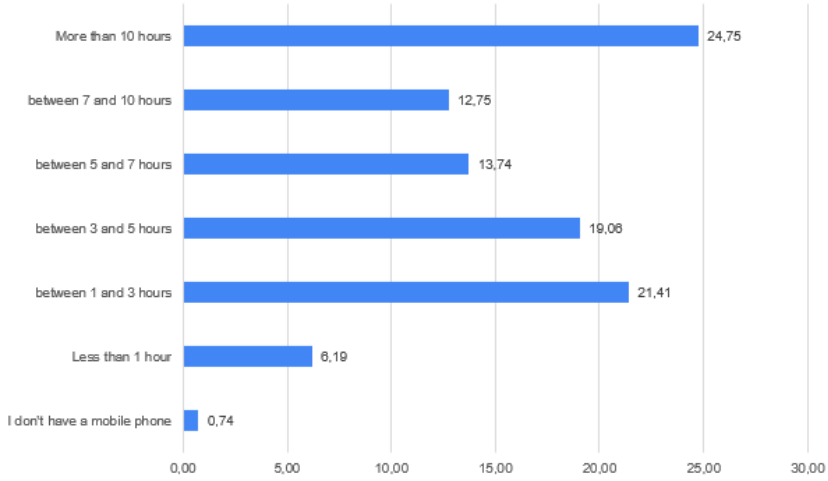
Picture 4.: Average weekly telephone time of the respondents divided into %, own editing

Picture 5 shows respondents' mobile phone use time in weekly average and percentage form.



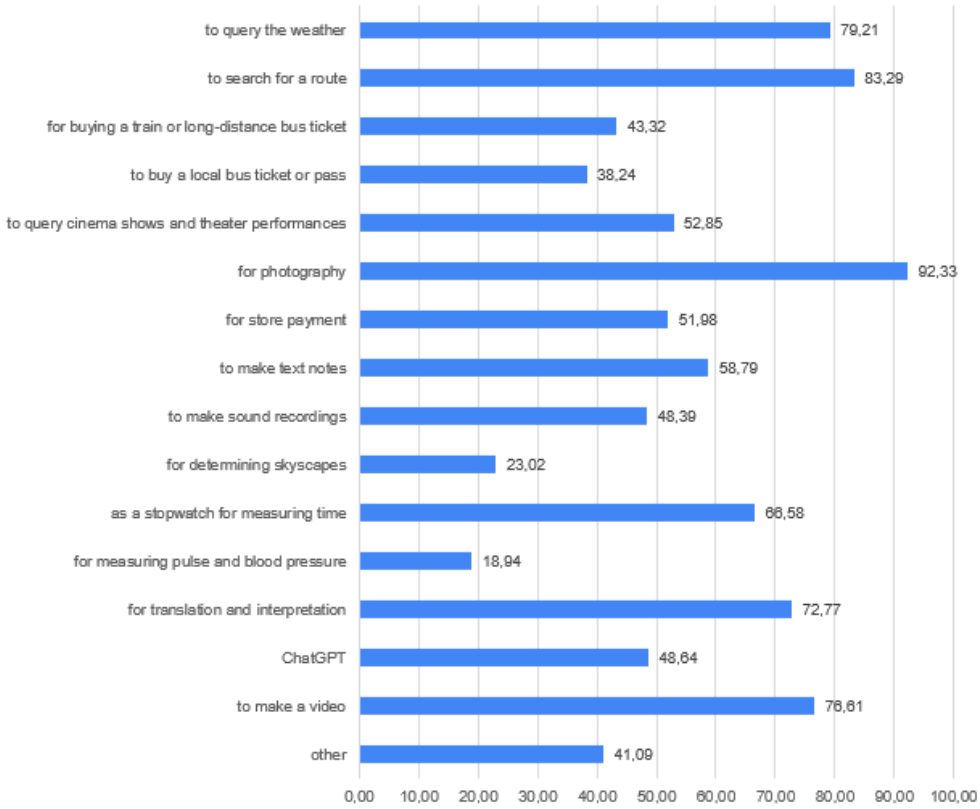
Picture 5.: Respondents' mobile phone usage time per week on average, broken down into %, own editing

Picture 6 shows respondents' time spent listening to music on a mobile phone device in weekly average and percentage form.



Picture 6.: It shows the respondents' time listening to music on their mobile device in weekly average and percentage breakdown, own editing

Respondents to the question "How do you most like to listen to music?" to the question, where the respondent could select more than one answer option, 37.38% answered hands-free, 75.74% with earphones, 36.26% with headphones, 24.88% with a mobile phone, 14.23% -a, 9.78% with a computer, 14.11% chose another answer. 45.79% of respondents only listen to music, 47.15% do sports, 38.24% do their hobbies, 34.41% play computer games, 44.43% do housework, 31, 68% solve homework, 33.79 do other activities while listening to music. The answers of the respondents to the question "What have you used your mobile phone for?" to the question entitled, where the respondent could indicate more than one answer option, is shown in picture 7.



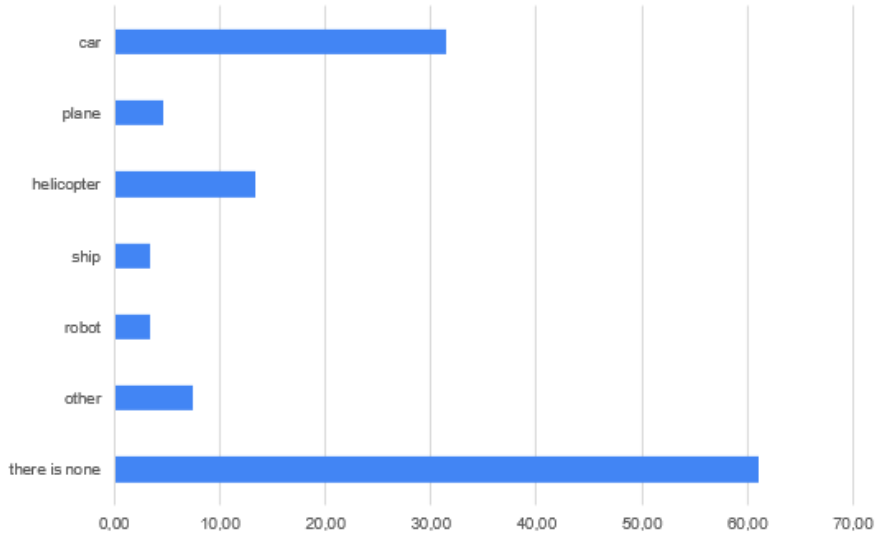
Picture 7.: The scope of use of the mobile phone in percentage breakdown, own editing

Respondents to the question "What does the term 'deepfake' mean?" to the question, 62.38% chose an image or video falsified by artificial intelligence, 36.14% did not know, I have not heard this before, and 0.5% chose the group name of new video games.

3. Technology

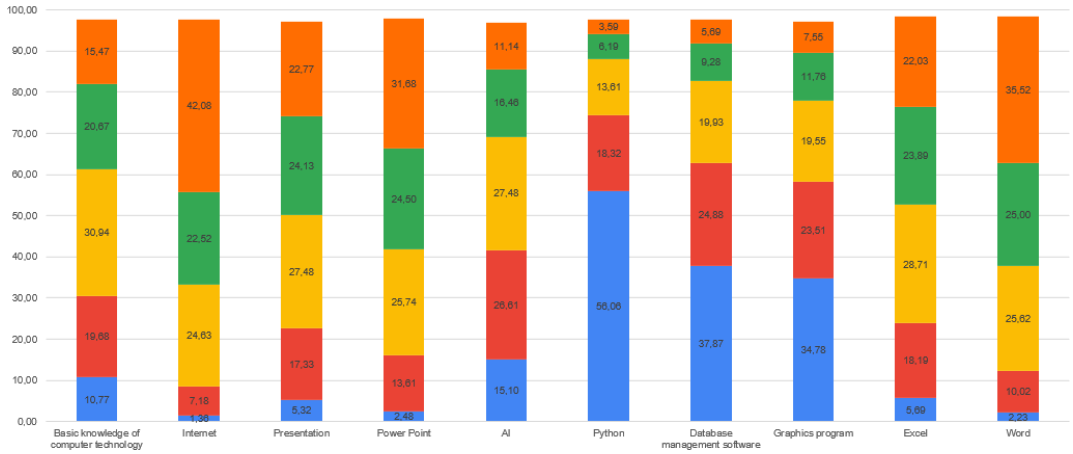
For Technical questions, I was curious about what devices are used to control another device, or, for example, whether mobile phones are used for remote control and programming of devices.

The first remote control question is "Have you ever flown a drone?" was a question where 30.69% said yes, but not mine, 20.54% said yes, I also have it, 23.02% said no, 24.05% said no, but I would like an answer. Respondents' answers to the question "What kind of remote control toy do you have?" to the question entitled, where the respondent could indicate more than one of several answer options, is shown in picture 8.



Picture 8.: The remote control games are broken down by percentage, own editing

58.54% of the respondents answered that they do not have a game that can be played together with a mobile phone, 12.75% have 1 game, 12% have 2 games, 2.72% have 3 games have games, 12.62% have more than 3 games that can be used together with a mobile phone. 79.08% of respondents know a device with artificial intelligence, 6.81% do not and 12.75% do not know which device has artificial intelligence. 45.17% of the respondents want to learn more about artificial intelligence, 24.13% do not want to learn more, and 29.46% have not yet decided to learn more about artificial intelligence. 87.87% of the respondents would like to try the simulation driving of the Leopard-2 tank, while 10.77% would not try the simulation driving. The respondents in the question "Have you ever been to a presentation day organized by the national defense, where military equipment was presented?" to the question, 22.77% chose yes once, 60.27% yes several times, 6.6% no, 9.46% no, but I would like to answer. Regarding writing a program, 15.10% of the respondents have already written a simple program, 9.65% are now learning and can write a simple program after that, 46.41% are not able to write, but 26.73% are not able, but would like to learn how to program. Respondents' answers to the question "How well do you know the following computer programs/applications?" for the question, where you could score your own knowledge from 1 to 5, as shown in picture 9.



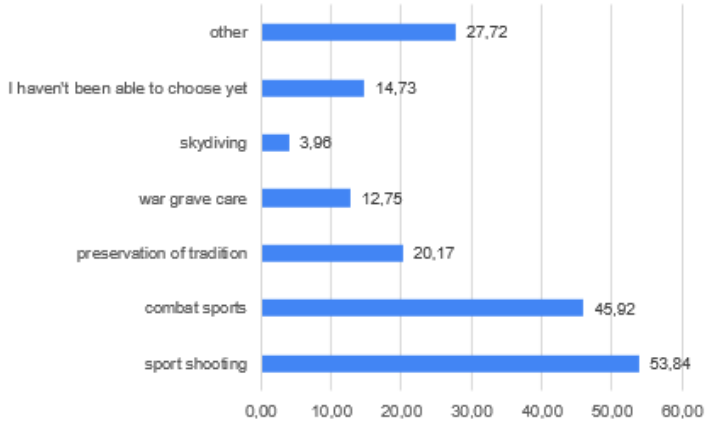
(1-blue, 2-red, 3-yellow, 4-green, 5-orange)

Picture 9.: Knowledge of computer programs broken down by percentage, own editing

Picture 9 clearly shows the four and five evaluations of Excel, Word, and Power Point, which are required for the ECDL exam, which in turn increases digital competence. The lowest ratings were given to Python, Database management programs and Graphics programs, which are mostly related to programming. 10.4% of the respondents indicated that they had already taken the ECDL exam, 13% wanted to take the ECDL exam, 5.57% were currently studying, 20.79% did not want to take the ECDL exam, 10.27 % are not interested in the ECDL exam and 38.49% do not know what the ECDL exam is.

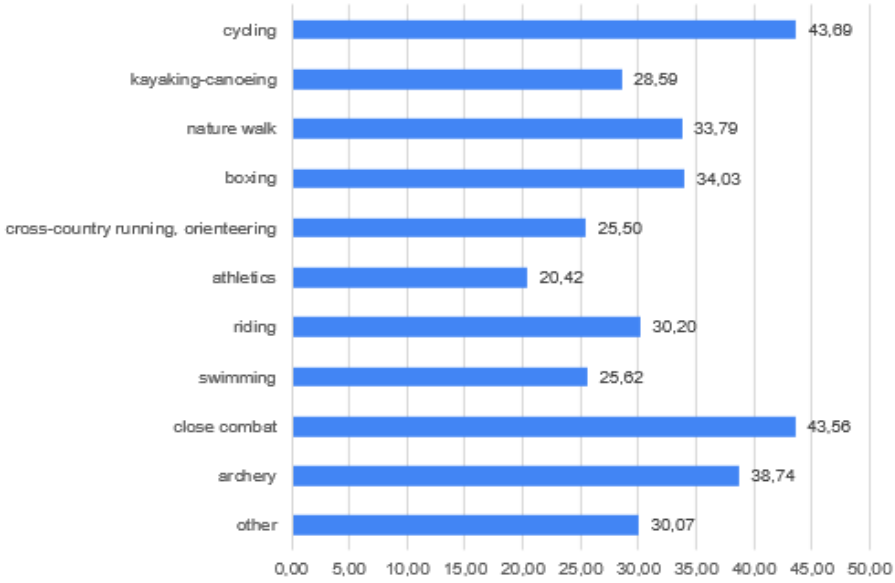
4. Sport-leisure

Respondents to the question "Who do you spend most of your free time with?" to the question, 9.41% prefer to be with their family, 17.08% prefer to be with friends, 9.03% prefer to be alone, 60.64% are equally family-friendly, 2.97% I don't have free time you chose an answer. Picture 10 shows the leisure activities chosen by the respondents.



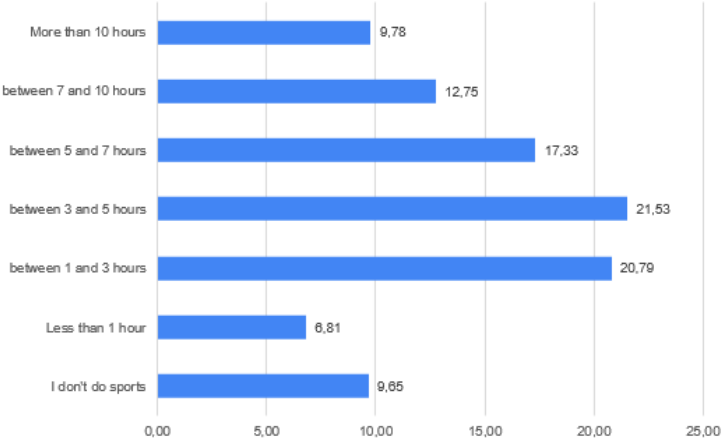
Picture 10.: Leisure activities in percentage distribution, own editing

Among the selected activities, sports shooting tops the list, which is also due to the fact that in recent years there has been a large development in this area, i.e. National Defense Sports Centers have been handed over. The respondents had the opportunity to choose which activity they would like to participate in, the result is shown in percentage form in Figure 11.



Picture 11.: Wish list of leisure activities, broken down by percentage, own editing

Based on picture 11, the respondents would most like to choose cycling and close combat as leisure activities. The answer of the respondents was based on the question "How many hours a week do you play sports outside of the compulsory physical education class?" picture 12 shows the question.

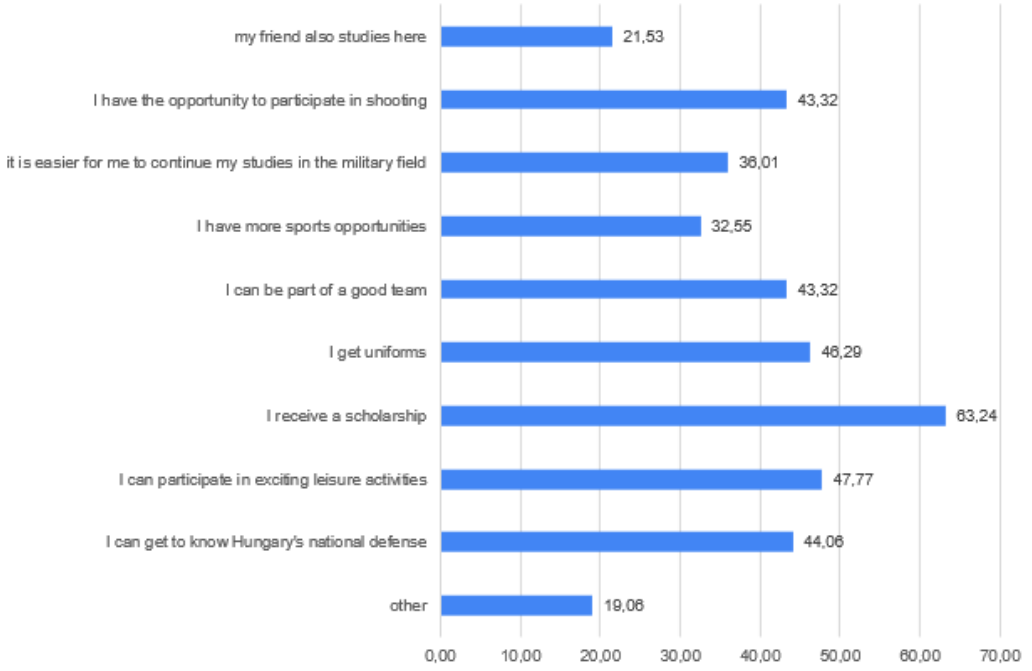


Picture 12.: Length of sports time, broken down as a percentage, own editing

Based on picture 12, it can be clearly seen that more than 40% of the respondents spend 1 to 5 hours a week doing physical education in their spare time. 37% of the respondents have already visited the National Defense Sports Center, 57.55% have not yet and 3.71% are just about to go to the Sports Center. The following question aims to advertise sports centers: "Would you take your friends to the National Defense Sports Center?". 31.56% of the respondents said yes, 11.01% said yes, we have already been there, 0.87% yes, it is being organized now, 1.36% say we go there regularly, 53.71% not yet I thought about it, he chose an answer. Among the respondents, 9.03% have participated in the National Martial Arts Tournament once, 4.33% have participated several times, 59.41% have not yet participated, and 25.87% have not participated, but would like to participate. Regarding competitive sports, 31.31% of respondents answered yes, 41.96% answered no, and 25.12% answered no, but I would like to.

5. Education

11.63% of respondents heard about the Honvéd Cadet Program from their parents, 36.26% from their class teacher, 15.47% read about it on the Internet, 12.38% heard about it from friends, 1.73% heard from his brother, 0.62% heard about it on TV and 20.54% learned about the program in other places. The answers of the respondents in the "What attracted you to the Honvéd Cadet Program?" to the question titled, where the respondent could indicate more than one answer option, can be seen in picture 13.



Picture 13.: Arguments in favor of the National Guard Cadet Program, broken down by percentage, own editing

On the basis of the 13th picture, it is clear that the first place is the answer "I will receive a scholarship", this could even represent a representation of our money-centered world. The respondents to the question "How have you experienced the attitude of other students towards the cadets of the National Guard in the city, at your school?" to the question, where the respondent could choose more than one answer option, 22.9% are proud of us, 18.94% envy us, 17.82% look up to us, and 17.95% want to being them, 46.16% of them nothing special, not noticing anything, 30.82% of them chose the answer after us. 67.7% of the respondents have already thought about further education, 18.32% are still thinking about it and 12.5% have not yet thought about further education. Among the respondents, 37.38% want to choose a military career, 37.13% do not know yet, and 23.89% do not want to choose a military career.

If we examine the relationship between the ECDL exam and the scholarship among the respondents based on Table 1, it can be seen that according to the first column, a total of 234 cadets want to take the ECDL exam and a total of 562 do not want to take the exam.

Answer option	Do you want to take the ECDL exam?	What attracted you to the National Guard Cadet Program? (I receive a scholarship)
yes	105	57
I've already done it	84	44
I'm still studying	45	27
Total (yes)	**234**	**128**
not	168	111
I'm not interested in ECDL	83	54
I don't know what it is	311	216
Total (not)	**562**	**381**

Table 1. The relationship between the ECDL exam and the scholarship, in the person breakdown, own editing

Based on Table 1, according to the second column, 128 of the 234 cadets indicated that they applied to become a cadet because of the scholarship, while 381 of the 562 cadets indicated this. Compared to the 808 respondents, 381 cadets is a significant number (47.15%) that needs to be addressed. I see that the 381 cadets could be encouraged to take the ECDL exam through financial appreciation. This would be beneficial for several reasons: on the one hand, people who already have an ECDL exam would apply to the national defense, so they would not have to be sent for education, and on the other hand, the cadet would also have a recognition, which would have financial implications. A similar system is already in place in the Hungarian Armed Forces, and the rank and qualification exam of the staff also has financial implications in the case of a successful exam.

If we examine the relationship between the number of siblings and the scholarship among the respondents based on Table 2, it can be seen (the first column shows the number of siblings, the second column shows how many people nominated the scholarship as an argument in favor of the cadet program, the third column and shows their percentage), that the percentage does not increase greatly with the number of siblings.

Answer option	Number of siblings	What attracted you to the National Guard Cadet Program? (I receive a scholarship)	Percentage
More than 3	56	33	58,93
3	99	60	60,61
2	220	142	64,55
1	311	199	63,99
I don't have a brother	114	76	66,67

Table 2. Number of siblings and the relationship of the scholarship, in person division, own editing

Based on Table 2, we can state that the number of people who choose the scholarship does not depend to a large extent on the number of siblings. So, approximately 6 out of 10 applicants will choose the scholarship regardless of the number of siblings when deciding on the National Guard Cadet Program.

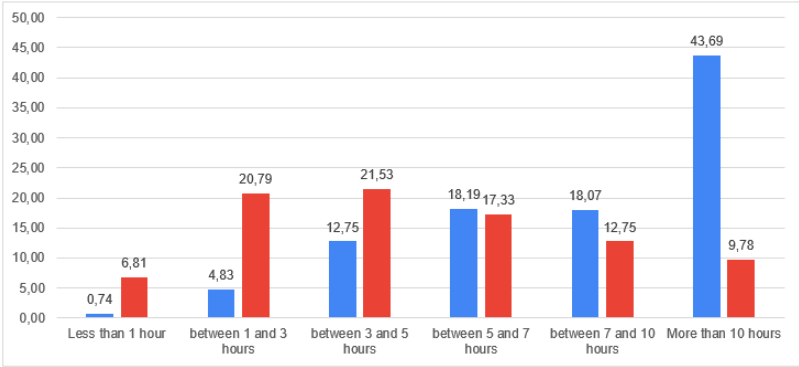
If we examine the influence of a close relative in the military on the cadets' willingness to choose a military career, we get Table 3.

Is there a soldier among your close relatives?	Where did you first hear about the Honvéd Cadet Program? (from my parents, brother)	Where did you first hear about the Honvéd Cadet Program? (on TV, from my class teacher, on the Internet, from other places, from my friends)	Would you like to choose a military career?	Percentage
190	35		24	68,57%
		155	77	49,67%

Table 3.: The influence of a close military relative on the choice of a military career, in person breakdown, own editing

The first column of Table 3 shows the number of respondents who have a soldier among their close relatives. The second column shows the number of respondents who learned about the National Guard Cadet Program from a close relative. The third column shows the number of respondents who did not learn about the National Guard Cadet Program from a close relative. The fourth column shows the number of people from columns two and three who would like to be soldiers. The fifth column shows the ratio according to columns two-four and three-four. Among those who were introduced to the National Guard Cadet Program by a close soldier's relative, 68.57% would gladly become a soldier, while only 49.67% of those who learned about the National Guard Cadet Program from another source would gladly become a soldier. Based on Table 3, we can say that it is more beneficial if a close military relative introduces the National Guard Cadet Program to the applicant, because more of them would choose the military career. It is possible to communicate better information and transfer more personal experiences also play a role in the decision.

If we compare the time spent playing sports and the time spent using mobile phones on average per week, we get the 14th picture below.

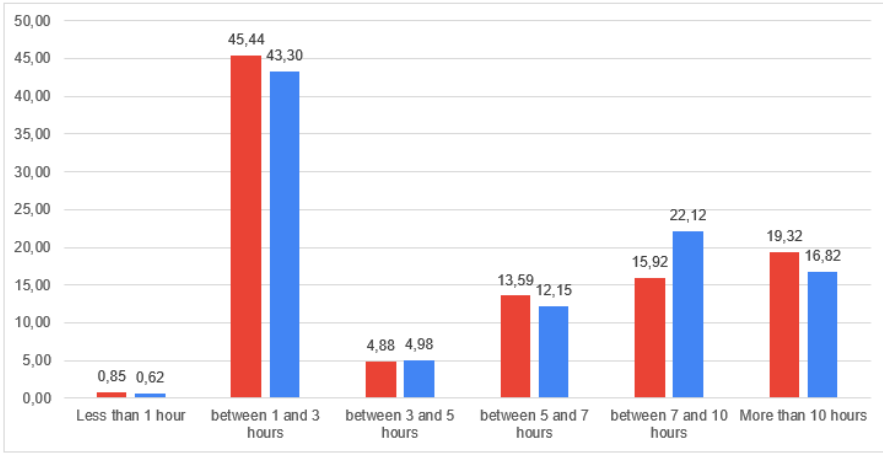


(red - duration of sports, blue - duration of mobile use)

Picture 14.: Comparison of mobile phone use and time spent playing sports, divided by percentage, own editing

On the basis of picture 14, it can be seen that in the interval of 'more than 10 hours', those who choose sports are drastically behind mobile users. Interestingly, the respondents chose the interval 'between 5 and 7 hours' in the same way for the question about the length of time using a mobile phone and the length of time playing sports.

If we examine the length of time spent using a mobile phone among respondents who have and those who do not have a toy or device that can be used with a mobile phone, we get the 15th picture.



(red - there is no such device, blue - there is such a device)

Picture 15: Duration of mobile phone use between those who have and those who do not have a device that can be used together with the mobile phone, in percentage breakdown, own editing

On the basis of picture 15, we can see that the blue column, which shows those who have a device that can be used with a mobile phone, uses a mobile phone in a lower percentage on

average than those who do not have such an option. An exception is the time interval "between 7 and 10 hours", where several people chose this option among those who have a device that can be used together with a mobile phone. The result is surprising because we would expect that the more opportunities we give our child to use his mobile phone, the more time he spends using it. The result shows otherwise. We can say that the time spent on games and free time is constant among the respondents, so the time they spend using devices that can be used together with a mobile phone is included in this time interval, so the time spent using mobile phones does not increase dramatically.

The device system of the digital soldier includes the communication system responsible for maintaining contact and which can be integrated into the helmet, which delivers the instructions, questions, and information received on the radio to the soldier's ears. According to the questionnaire, 86.88% of the respondents use earphones or headphones when listening to music, which means that the younger generation is already used to the device that can be used to input information through the ear. 43.69% of the respondents indicated that they listen to music with earphones or headphones during sports, so they do physical work while also listening to the music coming to their ears and moving to its rhythm. This activity is compatible with the activities of the digital soldier in the military field, since while moving in the field, which is physical work, he must also pay attention to the radio, through which information can come from his peers or superiors. Among those who listen to music with earphones or headphones and do sports, 19.55% of the respondents indicated that they would like to choose a military career, this means 158 cadets.

SUMMARY

Every army strives to protect its soldiers from enemy attacks as best as possible. The probability of personal injuries and losses can be reduced by various measures, but cannot be completely excluded. This is the reason for the need to develop the digital soldier, which can be supported by the use of already well-proven AI in the civilian field.

Digital competence is necessary for learning digital technologies, for the confident and responsible use of AI technology, and for the commitment related to them. The national defense cadets are on the right track in acquiring skills in data management, communication and cooperation, and media literacy. The questionnaire showed the interest of military cadets in AI.

According to the data obtained on the basis of the questionnaire, devices that can be used together with the mobile phone do not drastically increase the usage time of the mobile phone. So parents should not be afraid of buying such devices, because with these options they can only increase the connection between man and machine.

The number of people taking the ECDL exam could be increased among those participating in the National Guard Cadet Program, if they paid for a successful exam in the same way as in the Hungarian Armed Forces after the rank or qualification exam.

Since women can also apply to be digital soldiers, their training and education requires more attention, because according to EU statistics, there are fewer women among those employed in digital technology.

Due to the rapidly changing and renewing digital techniques, it is important that the cadet of the National Guard be open and curious about today's emerging technologies and applications. The half-measurement also confirms that cadets enthusiastically participate in military demonstrations and are interested in new techniques.

It is important that with the digital soldier system, the soldier is not only a part of the central server as an external speaker, but a conscious user, with a critical attitude and appropriate digital competence, an active part of military operations. The National Guard Cadet Program provides an opportunity to develop these competencies and acquire knowledge.

REFERENCES

[1] 2018/C 189/01 Az Európai Tanács ajánlása az egész életen át tartó tanuláshoz szükséges kulcskompetenciákról. Az Európai Unió Hivatalos Lapja. 2018.6.4.
[2] 1341/2019. (VI. 11.) Kormány Határozat a Digitális Kompetencia Keretrendszer fejlesztéséről és bevezetésének lépéseiről. Online: 1341/2019. (VI. 11.) Korm.határozat - Nemzeti Jogszabálytár (njt.hu)
[3] Kerber Zoltán et al. (2006): Hidak a tantárgyak között. Országos Közoktatási Intézet. ISBN 963 682 572 6
[4] 1573/2020. (IX. 9.) Kormány határozata Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről; Magyar Közlöny 2020 (202)
[5] 1393/2021. (IV.24.) Kormány határozata Magyarország Nemzeti Katonai Stratégiájáról. Magyar Közlöny 2021 (119)
[6] Digital Economy and Society Index (DESI) 2022. Online: https://digital-strategy.ec.europa.eu/hu/policies/desi
[7] Szűcs László (2021): A digitális katona program - Beszélgetés dr. Böröndi Gábor altábornaggyal. Online: https://matasz.com/hun/a-digitalis-katona-program-a-magyar-honvedseg-teljes-gondolkodasmodjat-meg-fogja-valtoztatni/
[8] Tóthné Lőkös Klára 2009. Következtetés statisztika. Gödöllő: Gödöllői Innovációs Központ Kft.
[9] Tóthné Lőkös Klára 2009. Összefüggés vizsgálatok. Gödöllő: Gödöllői Innovációs Központ Kft.

DOI: https://doi.org/10.12700/btsz.2025.7.1.65

ANALYSIS POSSIBILITIES OF THE TOOLSET OF INFORMATION SECURITY

AZ INFORMÁCIÓBIZTONSÁG ESZKÖZTÁRÁNAK ELEMZÉSI LEHETŐSÉGEI

KÁRÁSZ Balázs[1]

Abstract

Regarding the limited availability of comprehensive Hungarian literature on this topic, this paper aims to collect tools of information security utilised by all involved parties and present them to the professional audience in a structured manner. Involved parties consist of users of information infrastructures who are exposed to threats, defence personnel contributing to the maintenance of security level, and attackers that probe the effectiveness of security systems. Tools are widely mapped, including concepts that belong to the logical layer of cybersecurity, as well as physically manifested devices, systems, networks and programs. The objective of the research presented in this paper is to describe the tools by main dimensions and detailed characteristics in a way that, according to these attributes, a comprehensive analysis of comparison can be performed. As a result of the analysis – since tools are collected both from military and civil background – the author makes efforts to determine ways of classification of information security tools, in order to facilitate more successful targeting of further researches of the topic both within military, administrative (public service) and civil context.

Keywords

information security, security awareness, technical, logical and administrative tools,

Absztrakt

Tekintettel a korlátozottan elérhető magyar szakirodalomra, mely átfogó megközelítésből tárgyalná az információbiztonság eszköztárának kérdéskörét, e tanulmány célja, hogy az érintett felek által alkalmazott információbiztonsági eszközöket összegyűjtse, majd strukturált formában bemutassa a szakmai közönség számára. Az érintett felek az információs infrastruktúrák fenyegetéseknek kitett felhasználói, a biztonsági szint fenntartásában közreműködő védelmi oldal, valamint a támadók, akik a biztonsági rendszerek hatékonyságát próbára teszik. Az eszközök széles körűen kerülnek feltárásra, ideértve a kiberbiztonság logikai rétegéhez tartozó koncepciókat, valamint a fizikailag megfogható eszközöket, rendszereket, hálózatokat és programokat egyaránt. A kutatás célja, hogy főbb dimenziók és részletes tulajdonságok mentén jellemezze az eszközöket, és átfogó, összehasonlító jellegű elemzés készüljön. Az elemzés eredményeképpen – köszönhetően annak, hogy az eszközök köre védelmi és polgári környezetre egyaránt kiterjed – a szerző kísérletet tesz ezek klasszifikációs lehetőségeinek megfogalmazására. Mindez hozzájárul a téma további kutatásában a célok megfelelőbb kitűzéséhez katonai, közszolgálati, valamint polgári kontextusban.

Kulcsszavak

információbiztonság, biztonságtudatosság, technikai, logikai, adminisztratív eszközök

[1] karaszb@gmail.com | ORCID: 0000-0003-2065-4928 | Former PhD Student, National University of Public Service, Doctoral School of Military Engineering | Volt PhD hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

INTRODUCTION AND RESEARCH DETAILS

Regarding current and possible future trends in the evolution of threats on information society, as well as the increasing pace of technical knowledge development concerning cyberattacks, organisations have to dispose of a diverse toolset of information protection they can easily reach out to. Thanks to the recent dynamic technological improvement of the affected areas, such as IT security, physical security, human risk management (in terms of awareness training), the variety of tools is constantly widening up till today. The year 2020 also brought the entire society an information environment that shortens distance between people thanks to technology in times of social distancing.

Browsing through relevant literature, the author has found no up-to-date systematic overview of the entire toolset of information protection and security, which would enable every kind of users to easily find the most suitable and appropriate solution when facing a particular information security problem. Even in studies that analyse the aspects of tools people currently use for conducting private or business life, keeping in touch and maintaining the information flow, no reference can be found to a comprehensive analysis of the toolset of information security. The above-mentioned approach means the main motivation for the author to construct an appropriately structured overview.

Scientific research problem

Based on the above-mentioned issues, the following question arises: what are the main dimensions, according to which, information security tools can be clearly classified, and how can such a classification system contribute to solving ad-hoc occurring or recurring security issues thanks to its transparency and applicability?

Research objective

The objective of this research is, firstly, to collect all currently available information security tools describing their main features and characteristics, and secondly, outline and define at least three dimensions of at least two attributes, according to which, each of the enlisted tools can be classified. As a third step, various ways of classification are to be determined in order for the expected results to be successfully targeted to further research in military context.

Research methods

The author used theoretical and empirical research techniques, partly with the method of grounded theory. Related scientific literature from Hungary, as well as abroad, from professional of both technical approach and military background are widely mapped and elaborated, in terms of review papers, monographs, conference publications, internet sources.

LITERATURE REVIEW

In this chapter, the author enlists concepts on the role of security as viewed by organisations in general, and how handling information and awareness development relate.

One might think for the first view that there is a lack of relevant, up-to-date literature available in Hungary to analyse the toolset of information security. Researches are

based mostly on international literature published in countries that have a developed security culture, information security and cybersecurity knowledge and defence capacity both in civil and military environment. However, if we dig deep in the content of papers, monographs and conference publications, plenty of references can be found that lead to the tools used as part of information security on the side of users, defence forces and attackers, as well.

Definitions of concepts applied within this research

As of today, in everyday conversations, the most common usage of the terms 'data protection' and 'data security' (as well as information privacy/protection and information security) is that they are synonyms. Firstly, the author aims to make a distinction by pointing to the correct understanding of that in the background, behind the action of protection lie massive legal documentation and measures to protect personal data, pointing at exact steps to be taken in order to *achieve* a secure state, while aspects of security aim to *maintain* an already secure environment in a technical sense (that is, within and across information systems) and on the human level of the entire information society, too. Moreover, information security is a wider concept than IT security, since it would also include protecting all forms of information – not exclusively electronic –, also including information services and supporting systems. [1]

The risk itself – as introduced above in the context of information security management – refers to the possibility of not being able to fully protect – or building an attack surface for a potential invader to take advantage of – the information of the organisation, and therefore causing loss, which can theoretically be quantified in every case. By theoretically I mean, in several cases the quantification process might be clear and easy, while in other ways, the organisation might not have the suitable method, time, money or willingness to manage risks in this depth in spite of it being worth from many aspects. [2]

Security in information society

The evolution process of information society throughout the past decades and centuries shows a clear picture of how security became more crucial step-by-step, as some examples follow. Physical passive security systems, such as fences, have always been serving to defend territories or borders against invaders. Physical active security devices, including automatic weapons applied in military defence operations, became necessary to be ameliorated to have dominance over the enemy. [3] By deeper investigation, one can discover parallelisms between concepts of ancient times and security measures of nowadays. Passive information security features firewalls as defence against malicious or intrusive entries, while active information security is equipped with intelligence methods like OSINT or simply AI-based extensions, improving both effectivity and reliability. [4]

Today's information society features intelligent tools, connected to each other via internet, which people use in their everyday life to deal with their duties, responsibilities, and keep in touch with each other – especially true for 2020, when the world-wide Covid-19 pandemic deeply influenced and changed our regular life in many aspects. Humans continue to realise that without connection, or without functional devices, we cannot survive these types of highly influential challenges. [5]

Adding up to the fastening pace of digitalisation, it has always mostly been crises with global impact that implied a next evolutionary step in digitalisation and automatisation. [6] These steps in both fields came across as fast as mankind could not imagine earlier. The specialty of Covid-19 pandemic can be found in that our global approach to commerce, production, consumption was strictly limited in short of time in terms of not allowed to socialise, to work from the office, to attend school for an uncertain time period or to travel abroad or to farther destinations within one's own country of residence. On the other hand, security has turned into a state of uncertainty when global economy, together with local economic processes (proven also by the trends of indexes [7]), started to regress due to restrictions in various industry sectors, but still, everyday duties of most people (including employed and just unemployed), such as taxes, heating or insurance kept on waiting to be paid just as before.

Significance of information security awareness

Obviously, using the internet, smartphones and connected devices daily, everyone should think about what sorts of information is used and shared via these tools. This is the point when we might forget about the security guidelines, the responsibility of the usage. Consequently, without responsibility on the user's side, the risk of loss or theft of data is increased. There is no question about the importance of security awareness, although it is rather relevant to clarify what it is. As we have shortly described above, one will not be able to avoid living without the continuous necessity of up-to-date tools and devices. Therefore, we must understand and learn this process, using which, we will make successful efforts in favour of keeping our private data/information secure. [8]

Information security is required to protect organisation data/information from threats, which can be classified according to being external or internal. External threat is implied by outsiders from the point of view of the organisation and theoretically, it should not make up a major issue, since by 2020, most of the organisations ought to have implemented advanced security technologies at various levels of the security system. [8] Until recently, internal threat has become the main critical information security issue identified, where threat and therefore risk is caused by internal factors, mainly deriving from the poor user behaviour of the employees such as carelessness, omission, and user errors.

Based on the above-mentioned aspects, apart from the technical part of information security, the toolset serving as the basis of our analysis should also include human behaviour the elements of which strongly influence efficiency and reliability rate of operating technical security layers either to protect data or to handle them securely. [9] Human behaviour and decision-making can be driven by rational and emotional reasons, both implying a certain rate of risk of performing under 100%. When it comes to rational decisions and behaviour of the user, the risk lies in the following three major factors: unawareness (together with carelessness), undereducation (related also to omission), and human error. [10] On the other hand, emotion-driven decisions and behaviour are unpredictable because of the irrationality in thinking, vulnerability and misguidance of the user, or simply the personality pattern the user has, therefore carrying a certain measure of risk (to be further defined in the second next paragraph).

After organisations realised that human behaviour influences the effectivity of all steps made to secure the IT and information systems, consulting firms, IT service providers,

and security experts all have been endeavouring the elaboration of courses and development programs (such as trainings and workshops), which are tailored to the unique needs of the organisation, in order to overcome either undereducation or unawareness of employees. [11] In the first case, the main goal is broadening technical knowledge primarily on basic levels, while in the second case, various techniques are at disposal to train the users realise threats and risk-incurring situations and take appropriate actions and reactions.

From the point of view of our analytic research, we consider the above-described side aspects also as crucial contributors to the whole toolset of information security. Within any area considered in the discussion, the triad of the parties affected by the processes of information security serves as a basis of our discussion, since we collect tools of not only the users' side, but also those of the defence personnel and the attackers. The users mean any person dealing with the information to be protected excluding defence personnel, while the term 'defence personnel' covers in our use all users dedicated to protection or maintaining security, and finally, attackers are affected parties aiming to obtain information without authorisation (mainly for criminal purposes).

DISCUSSION

In this chapter, the author collects concepts and specific tools of information security categorised according to their technical, influential, and protective characteristics, aiming to outline ways of building clusters in order to achieve higher effectivity in applying the tools within the organisational context.

Tools of information security

Referring to the literature reviewed in the Chapter 2, we have seen that many papers discuss various solutions and tools of security, although they do not define or describe the tools themselves or organise these into groups. What all pieces of literature certainly affirm is: the effectiveness of taking any sort of information security measures depends on the complexity of execution. For the structured discussion and analysis of the topic, we discern the following three main areas of information security: technical, logical and administrative – according to which, tools are enlisted by naming their important characteristics.

Technical tools of security

By technical security, the author means all security tools and measures that are physically manifested or can be implemented to serve active or passive protection – this way contributing to security directly, by action, in the physical space. Technical tools aim to protect confidential or sensitive information from unauthorised access – confidential or sensitive from the point of view of its owner or its addressee (in case of communication). For example, should documentation of an organisation be held in either electronic or paper-based, the stored or communicated information has to be protected. As for the location of the information, we can enlist buildings, premises, meeting rooms, cabinets, and storage media (paper-based – printed or handwritten, phonographic, magnetic, optical, electronic, digital – computer-based).

Passive technical security includes passive fire protection, water protection, protection against mechanic vibrations, and electromagnetic compatibility. Active technical security features external and uninterruptible power supply, air conditioning, active fire protection, cable management. The tools at the users' disposal when talking about technical security are limited. This circle includes simple solutions to serve the work-related or everyday life-related information need in a user-friendly way. To have authorised access to the information, walls can be overcome only through doors, and locks are to be unlocked by appropriate keys.

As for the tools applied by the defence personnel, entry points to office buildings have security guards requiring self-identification from arriving guests to let them in and in cases, baggage check/car trunk check when somebody is leaving the building, while highly protected areas can also feature armed guards. Perceptibly forwarded information can be secured by surveillance systems (image and voice recording, closed-circuit television), intrusion detection systems (based on electromagnetic technologies such as infrared vision or radar), DECT phones, electromagnetic shielding, acoustic vibration or barrier film layers (the latter two tools serve for avoiding eavesdropping in case of respective indications).

Attacks aiming at a technical security measure or solution share the objective to find and make use of flaws in either its preparation (design) or its implementation (execution). Forging, deception, and force are the main methods at the attackers' disposal to encompass the flaws or overcome security lines, therefore making it possible to obtain protected information – and at a later point, to use them for malicious intentions. While at first hearing, attack imply something coming from the outside, it would be a mistake not to observe the inside threats including human risk of inappropriate information handling (unintended attack).

Logical tools of security

By logical security, we would like to include all concepts or methodologies that have significant role in actively or passively maintaining a secure environment.

Recently, with the growing importance of work from home, it has become more difficult to keep all information secured when in home office – partly due to the usage of user-owned devices (UOD) and take some of the sensitive documentation with us. At home one feels safe, while having guests that use their devices on these home networks, all sharing the same level of safety. These can easily open the possibility for unauthorised access or vulnerability in the event of an attack. Tools we can use are virus protection, firewall, regulations, awareness of information security better to say conscious protection, software control. To summarise these, we can say logical security.

End-to-end encryption is a logical tool encoding content within digital communication, connected to both ends of communication. The principle is based on using a pseudo-random encryption key, which is generated by an algorithm, provided to authorised recipients. [12] This way, it features numerous but limited number of possibilities to decrypt the content without possessing the key by applying brute force, although only with notable computational capacity. In everyday life, one can encounter the principle at messaging applications, which vary storing the key at the operator or the source/recipient within the communication. The second option provides the user higher level of security and privacy, since this way, even the service provider cannot access the content in a decrypted form.

Key management is strongly linked to encryption where (usually referring to a system) the logic behind the handling of encryption keys is administered – also meaning a domain where keys are generated, distributed, stored, refreshed, recalled or annulled. [13] The crucial points of a successfully operating key management include scalability – capability of managing a large number of encryption keys, security – elimination of vulnerabilities exposed to outside hackers or malicious insiders, availability – ensuring data accessibility for authorised users, heterogeneity – support of multiple databases, applications and standards, as well as governance – definition of policy-driven access control and protection for data.

Folders, domains of storage, virtual protection barriers such as firewalls and other logical units of systems and networks are to be unlocked, accessed, or modified by users and administrators possessing the appropriate access rights. Identity and access management (IAM) is a framework of implemented principles and directives as well as technologies that effectively assure to grant access to (sub)systems, (sub)domains partly or entirely to the authorised users only. A correctly operating IAM framework complies to all three attributes to information security: confidentiality, integrity and accessibility, not only from the perspective of the information but also interpreted in the context of the logical structure of the assigned access rights. [14]

Coming to the question of identifying authorised users to data which is secured/encrypted/protected, the key notion is authentication. Authentication methods can be diversified according to several factors – either if one or more of them implemented at the same time. The more factors implemented, the higher level of security the protection features. Factors can vary from knowledge-based (password) through possession-based (token or text message or push notification on mobile device) to character-based (biometrics) solutions, and multi-factor authentication means at least two different methods used within one authentication process. [15]

Administrative tools of security

Administration tasks – to variable extent – accompany all technical and logical tools of security, as stated above even in paper-based form or electronically. Administrative security is based on the rules, laws, policies to follow and covers compliance to technical specifications, principles, as well. Moreover, it's about the people, it's about the human component. The highest level of security risk can be related to human factors. Through manual controls we can ensure that there is no intentional or unintentional act in the process, however this rather detective way of control. These activities could be identified with detective control, but more secure to build security awareness in the people, teach them how to protect the data, information they use. Those rules, laws and policies mentioned in the beginning of this paragraph each person should acquire, who use the clever tools, the internet even in their private or business life.

Bureaucracy cannot be separated from administrative tasks – which from first hearing implies that complicated processes and paperwork (even if digitally documented) are attached to security measures. On the contrary, thoroughly worded, clear, and detailed description of IAM (paired with full compliance) can keep information systems safer from hacker attacks, as shown by the example of the Hungarian school administration system scandal in late 2022. [16] In this recent case, not only the system's source code was retrieved

by the intruder, but personal data and a wider circle of information about potentially all of the users have been compromised. The system was operated with significant deficiencies in IAM, authentication, security awareness and inappropriate corporate communication. If these administrative processes had been better defined and enforced, the vulnerabilities that led to this breach could have been prevented. This highlights the importance of not only technical defences but also the rigorous implementation of administrative controls to strengthen overall security posture.

Additionally, we have places where the topic of meetings holds the risk to get publicity or fall into the wrong hands. Confidential discussions regarding security strategies, vulnerabilities, or potential future threats can inadvertently become a target for malicious actors if not properly managed. In such cases, ensuring that the right people have access to sensitive information is paramount, and any sharing of such details should be handled with extreme caution. Thus, fostering an environment where confidentiality and discretion are prioritised is critical for effective administrative security.

Security awareness training concepts should be elaborated based on precedent case studies, analogy research, simulation and with an emphasis on solution-focused and decisive thinking development. The process management connected to information security measures within organisations can be considered as more and more developed, whereas nowadays, cyberattacks threatening daily operation of corporates are performed more frequently. Regarding this, it is inevitable to incorporate security awareness to corporate training and development, and the maintenance of high level of preparedness in both technical and non-technical fields, especially in order to adequately handle human risk factors.

ANALYSIS

This chapter aims to provide a concise analysis of the collected information security tools, focusing on their classification across multiple dimensions. By examining these dimensions, the author aims to establish a structured framework that enables a better understanding of the tools' applicability, strengths, and limitations. Such a framework can guide both military and civil organisations in selecting the most appropriate tools for their unique contexts.

Impact: direct vs. indirect security

Direct security tools are capable of immediately handling specific vulnerabilities or threats. For instance, the implementation of firewalls in a network system has been proved to be highly effective in preventing unauthorised access and blocking malicious traffic. A frequently occurring example can be a firewall which, during a coordinated phishing attack, successfully filters and flags suspicious links in emails, preventing the users from compromising sensitive systems. Examples can also cover intrusion detection systems, antivirus software, and access control tools. These tools act as a front line of defence, blocking or mitigating risks in real-time.

Indirect security tools focus however on enhancing the overall defence ability of a system. These include awareness training programs, security policies, and compliance mon-

itoring systems, among others. While they do not confront threats directly, they aim to create an environment that reduces the probability of carrying out successful attacks by the means of improving user behaviour, organisational culture, or system configurations.

Contribution: active vs. passive security

Active security tools are based on continuous monitoring, capability of intervention, and are adapted to maintain effectiveness of defence level. List of examples include most importantly intrusion prevention systems, security information and event management systems. These tools often demand a higher level of expertise and resource allocation but provide immediate responses to dynamic threats.

Passive security tools however function in the background or in a fully automated manner, providing basic and ideally continuous support, such as encryption algorithms, hardware security modules, or even physical barriers like locked server rooms. These tools make active security measures complete by providing a stable basis for them to operate effectively. For instance, encryption ensures data integrity, which is critical for intrusion detection systems to accurately analyse information, whereas secure hardware and physical barriers ensure the reliability of active monitoring. While their maintenance needs are typically low, their effectiveness depends on proper implementation and regular updates.

Approach: proactive vs. protective security

Proactive security tools are focusing on risk identification and mitigation before they are effectuated as threats. However, implementing such tools result in higher upfront costs and also, they need specialised configuration and maintenance expertise. Moreover, potential false positives strain resources or desensitise response teams. Additionally, their effectiveness depends on accurate threat intelligence, which can be difficult for seamless integration. Examples cover vulnerability scanning software, penetration testing, threat intelligence platforms, and predictive analytics systems. These tools are critical for reducing the exposure to emerging threats and ensuring resilience of systems and networks.

Protective security tools, in contrast, are designed to detect, or recover from security breaches. Examples include backup and recovery solutions, incident response plans, and endpoint detection and response tools. These tools are indispensable for minimising the damage caused by successful attacks and restoring normal operations.

Control: management vs. operational vs physical security

Management-level tools approach information security from the strategic viewpoint, often serving as a bridge between operational and physical security by ensuring that strategic-level decisions take both technical and tangible aspects of protection into consideration. For example, risk assessments guided by governance standards (e.g., ISO 27001) can influence physical security measures like access zones, and in parallel, also shaping operational strategies, such as automated monitoring protocols. They are essential for aligning security efforts with organisational goals and regulatory requirements.

Operational-level tools are implemented at the tactical level to manage day-to-day security challenges. Monitoring dashboards, automated patch management systems, and user access provisioning tools belong to this layer of control. These tools translate strategic goals into actionable measures.

Physical security tools cover various tangible measures to physically protect technical assets and visible parts of infrastructure. Surveillance systems, biometric access controls, and environmental monitoring sensors are part of this layer, while addressing physical vulnerabilities that could compromise information systems. Major risks mitigated by their presence could cover disruption of critical infrastructure, or undermining of the integrity of digital operations. For example, a physically compromised server room can lead to data breaches or system failures that directly impact virtual systems relying on it.

Integrating these three layers of the dimension of control ensures a holistic security posture, as each layer addresses distinct aspects of organisational security.

Manifestation: virtual vs. physical security

Virtual security tools are solutions that are based on software, and are designed to protect digital assets including information at first place. Firewalls, data loss prevention systems, and secure coding practices are of highest importance to be enlisted within this element. These tools combat cyber threats that seek to exploit vulnerabilities in digital systems and networks.

Physical security tools, on the contrary, aim to protect the tangible components of an information infrastructure. Examples include hardware firewalls, secured server enclosures, and electromagnetic shielding for critical systems. These tools are crucial for defending against threats like unauthorised access, theft, or environmental hazards. While virtual security tools dominate modern cybersecurity discussions, the increasing interconnectivity between digital and physical domains (for instance, in IoT environment) underscores the importance of physical security measures.

CONCLUSION

By analysing information security tools across these five dimensions and their elements or layers (as referred to in the analysis), this paper provides a comprehensive overview for understanding their roles and applications. Organisations can use it, supporting their security objectives, to identify and classify tools effectively and select the most suitable options based on their specific needs. Furthermore, the approach used within this analysis in setting up the five dimensions supports further research into developing integrated security solutions that can relate to complex challenges in both military and civil context.

REFERENCES

[1] R. Von Solms and J. Van Nieker, “From information security to cyber security.” *computers & security*, vol. 38, pp. 97-102, 2013. doi: 10.1016/j.cose.2013.04.004

[2] E. Gelbstein, “Quantifying information risk and security.” in *ISACA Journal*, 2013, no. 4 (access: https://www.isaca.org/resources/isaca-journal/past-issues/2013/quantifying-information-risk-and-security (04.02.2025)

[3] Z. Haig, *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó, 2018. ISBN 978-615-5945-05-2

[4] Cs. Kollár, “A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed.,

Budapest, Hungary: Óbuda University, Doctoral School on Safety and Security Sciences, 2019, pp. 47-61.
[5] K. Härmand, *Digitalisation before and after the Covid-19 crisis,* ERA Forum vol. 22, pp. 39–50, 2021. doi: 10.1007/s12027-021-00656-8
[6] F. Debasa, "Digitalisation, pandemics and current world (2019-2021)", *unio,* vol. 7, no. 1, pp. 18–32, Oct. 2021. doi: 10.21814/unio.7.1.3575
[7] H-J. Trenz, et al., Resilience of public spheres in a global health crisis. *Javnost-The Public,* vol. 28, no. 2, pp. 111-128, 2021. doi: 10.1080/13183222.2021.1919385
[8] Cs. Kollár, "Életünk a digitális korban," in: *Pedagógia a digitális korban*, Cs. Kollár, R. Tóth, Eds., Budapest, Hungary: PREMA Consulting, 2014 pp. 1-30.
[9] R. Klint, 'Cybersecurity in home-office environments : An examination of security best practices post Covid', Dissertation, 2023.
[10] Cs. Kollár, *Az információbiztonság jogi- és humán aspektusai*. Budapest: Szerzői kiadás, 2023.
[11] B. Kárász and Cs. Kollár, "Leadership Responsibilities in Information Security Awareness Development", *AARMS,* vol. 19, no. 2, pp. 79–91, May 2021, doi: 10.32565/aarms.2020.2.6
[12] G. Kovács and J. Hornyacsek, „Korszerű oktatási eszközök és módszerek alkalmazása a polgári védelmi felkészítésben." *Műszaki Katonai Közlöny* vol. 29, no 2, pp. 117-132, June 2019, doi: 10.32562/mkk.2019.2.10
[13] K. Ermoshina, F. Musiani, H. Halpin, (2016). "End-to-end encrypted messaging protocols: An overview." presented at the Internet Science: Third International Conference, INSCI, Florence, Italy, Sept. 12-14, 2016, Proceedings 3, pp. 244-254, Springer International Publishing.
[14] W. Fumy and P. Landrock, "Principles of key management," in *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 785-793, June 1993, doi: 10.1109/49.223881
[15] M. A. Thakur and R. Gaikwad, "User identity and Access Management trends in IT infrastructure- an overview," *2015 International Conference on Pervasive Computing (ICPC),* Pune, India, 2015, pp. 1-4, doi: 10.1109/PERVASIVE.2015.7086972.
[16] B. Kárász, "Social Aspects of Reliability and Security Issues of Authentication Solutions" *Hadtudományi Szemle* vol. 13, no. 2, pp. 111-127, June 2020, doi: 10.32563/hsz.2020.2.9
[17] Telex: 110 milliós bírságot kapott a KRÉTA meghekkelt fejlesztője, súlyos hiányosságokra derült fény. https://telex.hu/techtud/2024/02/21/kreta-hekkertamadas-feltores-szemelyes-adatok-naih-vizsgalat-eredmeny-adatvedelmi-birsag (access: 29.01.2025)

DOI: https://doi.org/10.12700/btsz.2025.7.1.77

ASSESSING WEB SECURITY AWARENESS: A SURVEY ON DEVELOPERS' PRACTICES, TOOLS, AND LEARNING PREFERENCES

FEJLESZTŐK WEBBIZTONSÁGI TUDATOSSÁGÁNAK FELMÉRÉSE: GYAKORLAT, ESZKÖZÖK ÉS TANULÁSI PREFERENCIÁK

ČOVIĆ Zlatko[1] – PAPP Zoltán[2] – ČOVIĆ Emili[3]

Abstract

This research assesses participants' awareness and understanding of OWASP Top 10 vulnerabilities, their real-world experience with security risks, and web security practices. By examining security challenges developers face and risk mitigation strategies, the study identifies knowledge gaps and misconceptions. It also explores the adoption of security testing tools, the role of AI-based security solutions, and their effectiveness. Additionally, it investigates developer interest in security education, participation in training programs, and preferred learning methods. By comparing security awareness across demographics, experience levels, and roles, this study provides insights into designing targeted training initiatives to integrate security awareness into software development education.

Keywords

OWASP Top 10, Web Security, Software Development, Security Awareness, Threats, Vulnerabilities

Absztrakt

Ez a kutatás a résztvevők OWASP Top 10 sérülékenységekkel kapcsolatos tudatosságát, biztonsági kockázatokkal szerzett tapasztalatait, valamint webbiztonsági gyakorlatait vizsgálja. Elemzi a fejlesztők által tapasztalt biztonsági kihívásokat és kockázatcsökkentési stratégiáikat, hogy azonosítsa a tudásbeli hiányosságokat és tévhiteket. Emellett feltárja a biztonsági tesztelő eszközök és AI-alapú biztonsági megoldások alkalmazását és hatékonyságát. A kutatás vizsgálja a fejlesztők érdeklődését a webbiztonsági oktatás iránt, képzési programokban való részvételi hajlandóságukat, valamint preferált tanulási módszereiket. Az eredmények hozzájárulnak a célzott képzési programok kialakításához, elősegítve a biztonságtudatosság integrálását a szoftverfejlesztési oktatásba.

Kulcsszavak

OWASP Top10, Web biztonság, Web fejlesztés, Biztonsági tudatosság, Fenyegetések, Sérülékenységek

[1] zlatko.covic@uni-obuda.hu | ORCID: 0000-0002-1769-1990 | University professor, researcher, Óbuda University Doctoral School on Safety and Security Sciences | egyetemi oktató, kutató, Óbudai Egyetem Biztonságtudományi Doktori Iskola; Professor, Assistant Director for Public Relations and Student Affairs, Subotica Tech – College of Applied Sciences, Subotica | oktató, Közkapcsolatokért és Hallgatói Ügyekért Felelős Igazgatóhelyettes, Szabadkai Műszaki Szakfőiskola, Szabadka
[2] zoltan.papp@magister.uns.ac.rs | ORCID: 0000-0001-9589-6580 | Associate professor, University of Novi Sad, Hungarian Language Teacher Training Faculty Subotica; University of Dunaújváros, Institute of Information Technology |egyetemi docens, Újvidéki Egyetem, Magyar Tannyelvű Tanítóképző Kar, Szabadka; Dunaújvárosi Egyetem, Informatikai Intézet
[3] 28224008@vts.su.ac.rs | ORCID: 0009-0003-1977-3062 | MSc student in Information Technology, Subotica Tech – College of Applied Sciences, Subotica | MSc hallgató Információs technológiák szakon, Szabadkai Műszaki Szakfőiskola, Szabadka

INTRODUCTION

Web applications are an essential part of modern digital infrastructure, supporting a wide range of business, communication, and entertainment services. As the adoption of web technologies continues to expand, so do the risks associated with cyber threats targeting web applications. The increasing number of security breaches highlights the importance of secure web development practices. Studies show that more than 60% of breaches involve vulnerabilities in web applications, with common attack vectors including SQL injection (SQLi), cross-site scripting (XSS), and broken authentication mechanisms [1]. Research on e-commerce security has identified SQL injection (SQLi), cross-site scripting (XSS), and security misconfigurations as some of the most frequently exploited vulnerabilities, often resulting in significant business losses [2].

Despite the availability of security frameworks and best practices, many developers still lack awareness or training in secure coding. Research has indicated that security is often deprioritized in favor of functionality and speed, leading to the deployment of vulnerable applications [3]. While organizations invest in security tools such as static and dynamic application security testing (SAST/DAST) tools, their effectiveness relies heavily on developers' understanding of security risks and proper implementation of secure coding practices [4].

Insecure web applications have a direct financial, operational, and reputational impact on businesses. Cyberattacks targeting web applications result in data breaches, financial fraud, loss of customer trust, and legal repercussions due to non-compliance with regulations such as GDPR and CCPA [5].

To address these issues, it is necessary to assess developers' awareness of web security vulnerabilities, their use of security tools, and their learning preferences. This study aims to evaluate these aspects by surveying developers in Subotica and analyzing the findings to gain insight into current security practices. The results will serve as the foundation for designing targeted security training programs, bridge the knowledge gap, and improve web application security.

The rest of this section provides a background on common web security threats, discusses the importance of security awareness among developers, presents an overview of the OWASP Top 10 vulnerabilities, reviews previous studies on the topic, and outlines the research objectives and structure of this paper.

Background on Web Security Threats

The increasing reliance on web-based systems has led to a rise in security threats targeting web applications. Cyberattacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) remain among the most commonly exploited vulnerabilities [6]. According to a report by Verizon, web applications account for over 43% of security breaches, highlighting the critical need for secure coding practices [7].

The rapid development of web technologies has also introduced new attack surfaces, making traditional security measures insufficient. The emergence of AI-driven cyber threats, automated exploitation tools, and large-scale data breaches further complicates the security landscape [8]. Given these challenges, the role of developers in maintaining web application security has become more crucial than ever.

Importance of Security Awareness Among Developers

Developers play a fundamental role in ensuring the security of web applications. However, multiple studies have shown that developers often lack adequate security training, leading to the introduction of vulnerabilities in the code they write [9]. A survey conducted by NIST found that 79% of developers do not receive formal security training, which increases the risk of security flaws in web applications [10].

Security awareness programs and secure coding training have been proposed as effective strategies for mitigating these risks. However, traditional security training methods often fail to engage developers or align with their real-world development practices. Research suggests that interactive and hands-on training methods, such as hackathons, capture-the-flag (CTF) competitions, and security coding challenges, are more effective in improving developers' security awareness and adoption of best practices [11].

Web applications, as public-facing system components, are vulnerable to attacks. Developers often struggle to grasp the full attack surface. A study found that one-third were unaware clients could intercept and modify HTTP requests, with knowledge mostly limited to XSS and SQL Injection. Using a questionnaire and a Capture the Flag challenge, the study highlighted security knowledge gaps, stressing the need for better training on web threats and defenses [12].

Security awareness is crucial in software development, as insufficient knowledge among developers can lead to poor coding practices and exploitable vulnerabilities. Studies indicate that a significant portion of security vulnerabilities in web applications stem from development errors rather than infrastructure weaknesses [12].

To mitigate these risks, integrating security-by-design principles throughout the Software Development Life Cycle (SDLC) is essential. This approach ensures that security is embedded from the outset, rather than addressed later. Key aspects of security awareness programs include:

- Understanding web vulnerabilities: Familiarity with common threats (e.g., OWASP Top 10) helps developers anticipate and prevent attacks. [13]
- Writing secure code: Adhering to standards from organizations like CERT and NIST ensure robust software security [14].
- Implementing security controls: Measures like input validation, access control, and encryption protect sensitive data and system integrity [15].
- Regular code reviews and security testing: Early detection and remediation of issues enhance software security [13].

Security is a shared responsibility across all roles in software development, including junior developers, testers, and DevOps engineers. By fostering a culture of security awareness and providing comprehensive training, organizations can significantly reduce vulnerabilities and enhance the overall security posture of their software products.

Overview of OWASP Top 10 Vulnerabilities

The Open Web Application Security Project (OWASP) publishes the Top 10 most critical web security risks, serving as an industry standard for secure software development.

[13] The list is regularly updated to address emerging threats, offering key insights for developers, security professionals, and organizations. The latest OWASP Top 10 list includes [16]:

1. Broken Access Control – Unauthorized access resulting from weak or improperly enforced permission policies. This vulnerability is responsible for the highest number of web application breaches.
2. Cryptographic Failures – Improper handling of sensitive data, such as weak encryption algorithms, exposure of passwords, or transmission of confidential information in plaintext, leading to data breaches.
3. Injection Attacks (SQLi, XSS, LDAP, etc.) – Maliciously crafted inputs that exploit poor input validation, allowing attackers to execute unauthorized queries, inject scripts, or manipulate backend systems.
4. Insecure Design – Fundamental flaws in the architecture or logic of an application that introduce security risks, emphasizing the need for security-by-design principles.
5. Security Misconfiguration – Default settings, excessive privileges, and unnecessary features that expose applications to exploitation, making them easier targets for attackers.
6. Vulnerable and Outdated Components – Use of unpatched libraries, outdated frameworks, or unsupported software that increases the risk of exploitation through known vulnerabilities.
7. Identification and Authentication Failures – Weak password policies, improper session management, and lack of multi-factor authentication (MFA) leading to account takeovers and identity theft.
8. Software and Data Integrity Failures – Risks associated with insecure deployment, lack of integrity verification in software updates, and unauthorized modification of critical application data.
9. Security Logging and Monitoring Failures – Insufficient or improperly configured logging mechanisms that prevent timely detection of security incidents, making applications vulnerable to prolonged undetected attacks.
10. Server-Side Request Forgery (SSRF) – Attackers exploiting server-side functionality to access or manipulate internal resources, leading to unauthorized data exposure and system compromise.

To mitigate these vulnerabilities, OWASP recommends implementing the best security practices such as secure authentication mechanisms, strict access control policies, and the use of parameterized queries to prevent injection attacks [17]. Additionally, organizations should adopt secure software development practices, conduct regular security assessments, and integrate automated security testing tools to identify and remediate vulnerabilities throughout the Software Development Life Cycle (SDLC).

Examples of Previous Studies

Several studies have explored developers' security practices, tools, and learning preferences. For example, a systematic review of secure coding practices found that developers often struggle with integrating security measures into their workflow due to time con-

straints and a lack of formal training [18]. Another study analyzed the effectiveness of security tools such as SAST and DAST scanners, revealing that many developers are unaware of how to properly configure and use these tools [19].

Additionally, empirical research has examined the impact of security awareness programs on software development teams. Findings suggest that security culture and peer learning play a significant role in shaping developers' security behaviors [20]. However, gaps remain in understanding how different experience levels and backgrounds affect security awareness, which this study aims to address.

Ensuring secure software development is crucial for maintaining integrity, confidentiality, and availability, yet security is often overlooked in favor of functionality. Research emphasizes the need to integrate security at every phase of the Software Development Life Cycle (SDLC), as many existing methodologies fail to do so effectively. The findings highlight the need for enhanced security practices to overcome adoption barriers and establish a structured approach to secure software engineering [21].

The authors in [19] present a swarm intelligence-based Orchestrated Continuous Vulnerability Assessment (OCVA) scanning tool to address the limitations of traditional security detection methods, such as signature recognition and anomaly detection, which often miss sophisticated cyber threats. [19] highlights the increasing need for continuous vulnerability assessment to improve security monitoring, analysis, and mitigation across networks, assets, and web applications. Comparative case studies show that OCVA outperforms existing vulnerability scanners in detection accuracy, remediation rates, and consistency. These findings suggest that OCVA provides a more efficient and reliable solution for developers and security auditors in mitigating cybersecurity risks.

In the paper [22], the authors emphasize the importance of improving employee security awareness to mitigate cybersecurity risks. They propose the Security Awareness Improvement Tool (SAWIT), designed to assess and enhance individual security practices within organizations. The study highlights the significance of continuous education and proactive engagement in fostering a security-conscious workplace culture, ultimately aiming to minimize security vulnerabilities linked to human factors in cybersecurity.

RESEARCH OBJECTIVES

This article aims to assess developers' awareness of web security vulnerabilities, their security practices, and their learning preferences. Specifically, the research questions are:

Q1: OWASP Top knowledge and experience:

- What proportion of developers are familiar with OWASP Top 10 security risks?
- How do developers perceive their own knowledge of OWASP Top 10 vulnerabilities?
- In real-world development, which OWASP Top 10 categories are encountered by the developers?

Q2: How do developers' education level, experience, seniority, and role influence their awareness and adoption of web security practices and OWASP Top10?

Research Methodology

This study is based on a non-representative online survey conducted in January 2025. The survey aimed to assess software developers' web security awareness, particularly focusing on OWASP Top 10 vulnerabilities, security tools, developers' practices, and AI-based security solutions. Additionally, the research aims to understand their interest in web security education and preferred learning methods. The questionnaire was designed by the authors and distributed via Google Forms.

Variables

To address research questions Q1 and Q2, the authors identified and analyzed a set of independent and dependent variables. These variables represent a specific subset of the questionnaire, designed to directly contribute to answering Q1 and Q2. By focusing on these targeted variables, the analysis aims to provide meaningful insights into the factors influencing web security awareness, OWASP Top 10 knowledge, and the adoption of secure development practices.

The key groups of independent variables used in the analysis pertain to demographics and professional background. These variables help assess whether factors such as education, work experience, seniority, and job role influence knowledge of web security and the OWASP Top 10, as well as the adoption of secure development practices.

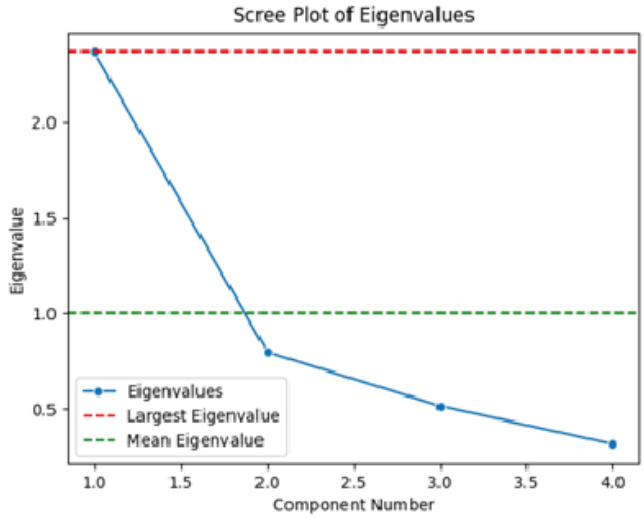
The key dependent variables analyzed in this study include awareness and experience with the OWASP Top 10, responsibility for secure web development, and the frequency of using web security assessment tools. These variables help assess the extent to which developers are knowledgeable about web security best practices, their role in ensuring secure development, and their regular engagement with security evaluation tools.

Internal consistency reliability of the questionnaire

To assess the internal consistency reliability of the questionnaire related to research questions Q1 and Q2, the authors categorized the relevant survey questions into two distinct groups, each designed to measure a specific underlying construct. The first group includes questions related to demographics and professional background, capturing factors such as education, work experience, seniority, and job role, while the second group focuses on OWASP Top 10 knowledge and the adoption of secure development practices, assessing participants' awareness, experience, and engagement with web security principles. Since internal consistency reliability is only meaningful for items measuring the same latent construct, it was evaluated exclusively for the second group, as demographic and background variables represent independent characteristics rather than a unified scale. The analysis was conducted using Python, applying appropriate statistical methods to ensure the reliability of the measured constructs.

For the second question group, McDonald's omega [23], was chosen as the reliability measure due to the mixed nature of the data. This group includes binary, ordinal, and linear scale data, making McDonald's omega a more suitable alternative to Cronbach's alpha [24], which assumes continuous or ordinal data with equal variances. This approach ensures a more accurate assessment of internal consistency across the diverse data types present in the survey. Since many statistical methods do not natively support categorical data, the authors transformed it into numerical form to facilitate analysis [25]. For binary data, such as yes/no responses, they applied the One-Hot Encoding technique in Python.

For ordinal data, where categories have a meaningful order, the authors used the Ordinal Encoding method. By applying these encoding methods, the authors ensured that the data could be effectively analyzed using statistical techniques while maintaining the integrity of the categorical variables. To determine the number of latent factors, the authors conducted an Exploratory Factor Analysis (EFA). However, before performing EFA, they assessed the sampling adequacy of each observed variable in the model using the Kaiser-Meyer-Olkin (KMO) test [26]. The KMO statistic is calculated based on the correlation between variables and ranges from 0 to 1. Higher values, closer to 1, indicate strong correlations among variables, suggesting that the data is well-suited for factor analysis. For the research question group related to Q2, the KMO value was $KMO = 0.7942$, indicating an acceptable level of sample adequacy, which is considered average to good for factor analysis. Additionally, the authors conducted Bartlett's test of sphericity [27] to determine whether the correlation matrix was significantly different from an identity matrix. A significant result from Bartlett's test suggests that there are sufficient correlations among the variables, justifying the application of factor analysis. In this study, Bartlett's test for the Q2 research question group yielded significant results ($p \approx 0.$), confirming that the variables were adequately correlated to proceed with factor analysis. The scree plot generated from the EFA is presented in Fig. 1 and indicates the presence of a single latent factor.



1. Figure: Number of latent factors for the second question group

A scree plot is a graphical representation of eigenvalues associated with each factor or principal component, with eigenvalues plotted on the y-axis and factors/components on the x-axis, arranged in descending order. The primary goal of this visualization is to identify the "elbow" point, where the slope of the curve significantly levels off. This point suggests a natural cutoff for the number of factors or components to retain in the analysis. Given the presence of a single latent factor, the authors calculated McDonald's omega ($\omega = 0.6925$) to assess internal consistency reliability. This value indicates moderate reliability—acceptable for exploratory research but with room for improvement.

Sample

To ensure a broader reach and higher response rate, the survey link was initially sent to company directors, who were requested to share it with their employees. Recognizing the multilingual environment of Subotica, the questionnaire was made available in both Serbian and Hungarian, allowing respondents to complete it in their preferred language. A total of 51 programmers, all employed by software development companies in Subotica, Serbia, participated in the study. All developers responded to every question in the questionnaire. The collected data contains no missing values.

The sample distribution across variables related to demographics and professional background is presented in Table 1.

Variable		Count	Percentage
education	high school	6	11.76
	BSc	36	70.59
	MSc	9	17.65
experience (year)	<1	3	5.88
	1-3	11	21.57
	4-6	9	17.65
	7-10	10	19.61
	10>	18	35.29
seniority	junior	9	17.65
	mid-level	18	35.29
	senior	24	47.06
role	frontend developer	11	12.09
	backend developer	23	25.27
	full stack developer	15	16.48
	mobile app developer	6	6.59
	software architect	7	7.69
	tech lead	11	12.09
	project manager	7	7.69
	DevOps	6	6.59
	other	5	5.50

1. Table: Sample distribution related to demographics and professional background

Table 2 presents the distribution of the sample across variables related to awareness and experience with the OWASP Top 10, responsibility for secure web development, and the frequency of using web security assessment tools.

Variable		Count	Percentage
OWASP Top 10 self assessment	I'm not sure	25	49,02
	superficial	20	39,22
	good	6	11,76
OWASP Top 10 experiences in projects	no	22	43.14
	yes	29	56.86
Responsibility for the web secure development	I'm not sure.	3	5.88
	Only security experts.	1	1.96
	The entire team.	47	92.16
Frequency of using security tools.	Never	18	35.29
	Rarely	20	39.22
	Occasionally	10	19.61
	Regularly	3	5.88

2. Table: Sample distribution related to awareness and experience with the OWASP Top 10 and secure web development

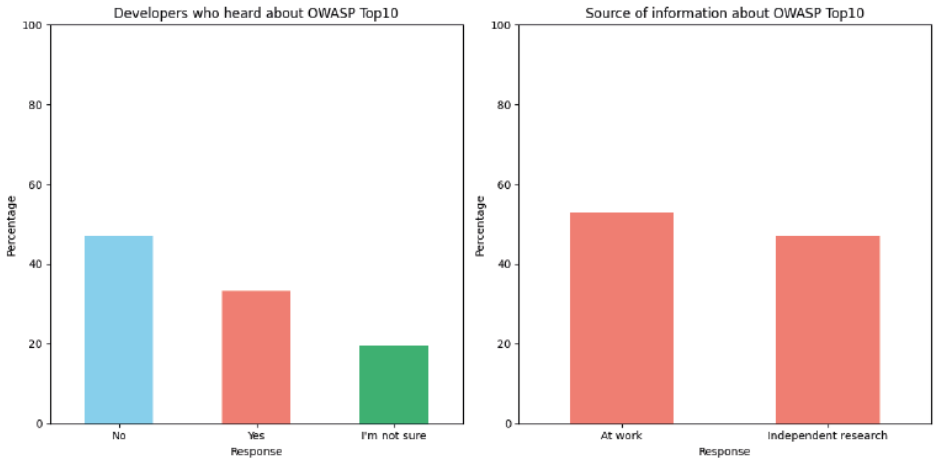
Plan of analysis

For the quantitative analysis of the collected data, the authors utilized the Python programming language. To preprocess the data obtained from the questionnaire, they employed One-Hot Encoding and Ordinal Encoding methods. To calculate internal consistency reliability, the authors first determined the number of latent factors through EFA and scree plot analysis. To justify the application of EFA, they conducted the KMO test and Bartlett's test of sphericity. For measuring internal reliability, the McDonald's omega coefficient was used. To answer the research questions, the authors employed descriptive statistics and correlation. This comprehensive approach ensured the robustness and validity of their findings.

RESULTS

Research question Q1

Fig2. presents the distribution of answers to the question: "What proportion of developers are familiar with OWASP Top 10 security risks?



2. Figure: Developers' awareness of OWASP Top10 and source

Fig. 2 illustrates whether developers have heard about the OWASP Top 10. Approximately 45% of developers have not heard about the OWASP Top 10, about 30% have heard about it, and around 25% are unsure if they have heard about it. Among those who have heard about the OWASP Top 10, approximately 55% learned about it at work, while about 45% gained their knowledge through independent research.

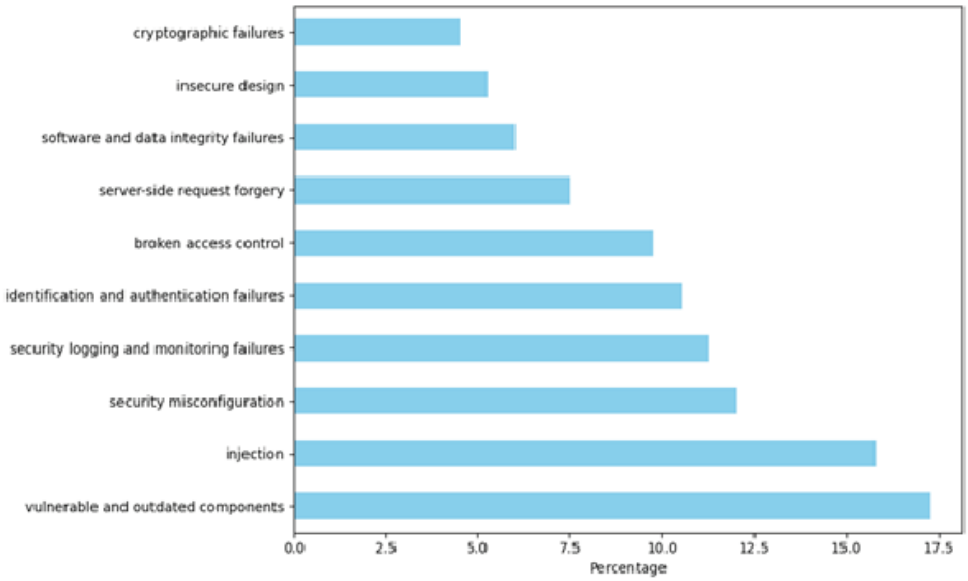
Table 3. gives an answer on the research question "How do developers perceive their own knowledge of OWASP Top 10 vulnerabilities? "

Independent variable		**Count**	**Percentage**
OWASP Top 10 self-assessment	I'm not sure	25	49,02
	superficial	20	39,22
	good	6	11,76

3. Table: Sample distribution related to OWASP Top 10 related security issues in real projects

Most developers are uncertain about their knowledge of OWASP Top 10 vulnerabilities. Additionally, 39.22% of developers assess their understanding as superficial, while only 11.76% believe they have a good grasp of these vulnerabilities.

The research question "In real-world development, which OWASP Top 10 categories are encountered by the developers?", could also help the authors to assess the OWASP Top10 awareness of the developers. Understanding which OWASP Top 10 categories are most encountered in real-world development is crucial for several reasons. By identifying the most frequently encountered security risks, developers and organizations can prioritize their efforts and resources to address the most critical vulnerabilities first. Fig. 3 provides a detailed breakdown of the specific OWASP Top 10 security vulnerabilities that developers have faced in real-world projects. The most prevalent vulnerabilities are related to the use of vulnerable and outdated components, injection flaws, and security misconfigurations.



3. Figure: Source of OWASP Top 10 security issues in real-world development

Research question Q2

Understanding how developers' education level, experience, seniority, and role influence their awareness and adoption of web security practices, including OWASP Top 10, is important for several reasons. By identifying how these factors affect web security awareness, organizations can develop targeted training programs. These programs can be tailored to address the specific needs and gaps of different groups, ensuring that all developers are adequately equipped with the necessary knowledge and skills. Insights into how these factors influence security practices can help organizations allocate resources more effectively.

As a measure of the developers' awareness and adoption of web security practices, including OWASP Top 10 the authors considered the following variables.

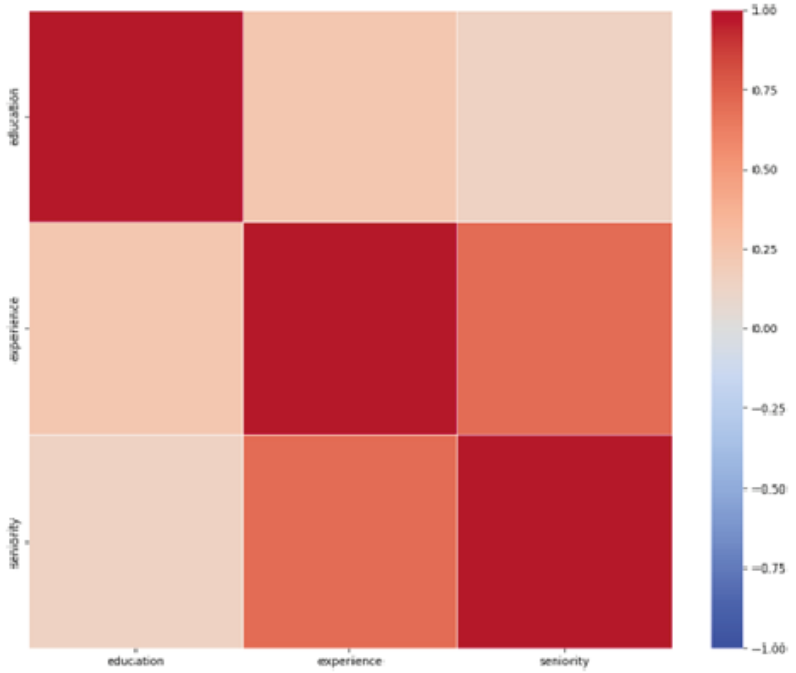
- Awareness of OWASP Top10: ordinal variable. The variable's sample distribution is presented in Fig. 2.
- Encountering OWASP Top10 security issues: categorical variable, with the possibility of selecting multiple options. The variable's distribution is presented in Fig. 3.
- Responsibility for secure web development: ordinal variable. The distribution of this variable is presented in Table 2.
- Frequency of using security testing tools: ordinal variable. The distribution of this variable is presented in Table 2.

Before performing statistical analysis, the authors preprocessed the data by converting binary and categorical variables to numerical values.

To avoid analyzing all possible pairs of dependent-independent variables, the authors opted to construct a single dependent variable by index construction method which

consists of standardization of variables and aggregation of standardized variables. aggregating the dependent variables [28]. This method is particularly useful when measuring complex constructs, such as developers' awareness and adoption of web security practices

The authors initially conducted a correlation analysis and calculated variance inflation factors (VIF) [29] on demographic variables, including developers' education level, experience, and seniority. VIF values greater than 5 are considered indicative of problematic multicollinearity. To prevent potential multicollinearity issues, the authors excluded highly correlated independent variables. The VIF values were calculated, and the Spearman correlation coefficient was employed due to the categorical nature of the data and its non-normal distribution. Fig. 4 presents the correlation matrix using a heatmap. Shades of red indicate a positive correlation. Darker red signifies a stronger positive correlation, closer to 1.00. Shades of blue indicate negative correlations. Darker blue signifies a stronger negative correlation, closer to -1.00. Seniority and experience are highly correlated, which implies multicollinearity. To avoid multicollinearity, the authors excluded experience.



4. Figure: Spearman correlation matrix for demographics data

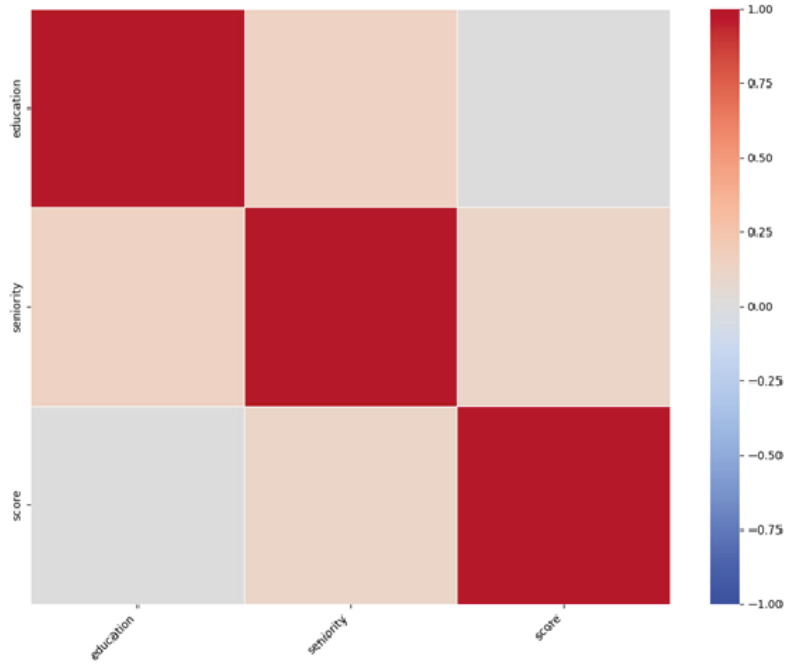
Correlation analysis is employed on dependent variables to identify and exclude variables that don't contribute meaningful information to the index and can even dilute its accuracy. These are variables with weak or no correlation to other dependent variables and are essentially noise. The Spearman correlation matrix is presented in Table 4. The variable representing the frequency of using security testing tools has a low correlation with both the awareness of OWASP Top 10 and the variable measuring encounters with OWASP Top 10 security issues. This suggested the authors exclude this variable.

	OWASP Top10 awareness	Encountering OWASP Top11 security issues	Responsibility for secure web development	Frequency of using security testing tools
OWASP Top10 awareness	1.00	0.27	0.12	0.03
Encountering OWASP Top11 security issues	0.27	1.00	0.33	0.05
Responsibility for secure web development	0.12	0.33	1.00	0.24
Frequency of using security testing tools	0.03	0.05	0.24	1.00

4. Table: Spearman correlation matrix for dependent variables

After excluding experience as an independent variable and the frequency of using security testing tools from the calculation of the composite index score, a correlation analysis was performed. The Spearman correlation matrix in Fig. 5 reveals that there are no strong correlations between any of the independent variables and the dependent composite index score. However, the correlation between seniority and the composite index score is relatively higher. Possible reasons for low correlation could be that education level, years of experience, or seniority may not necessarily translate into better security awareness. Security responsibilities often belong to dedicated security teams, meaning general developers (regardless of seniority) may not engage deeply with security practices.

The authors conducted a correlation analysis using developers' roles as independent variables and the composite index score as the dependent variable. To avoid multicollinearity, they calculated the Spearman correlation matrix and VIF values. The heatmap presented in Fig. 6 revealed some higher correlation values. Based on these findings, the authors decided to exclude the roles of tech lead, head of software development, mobile app developer, and project manager.



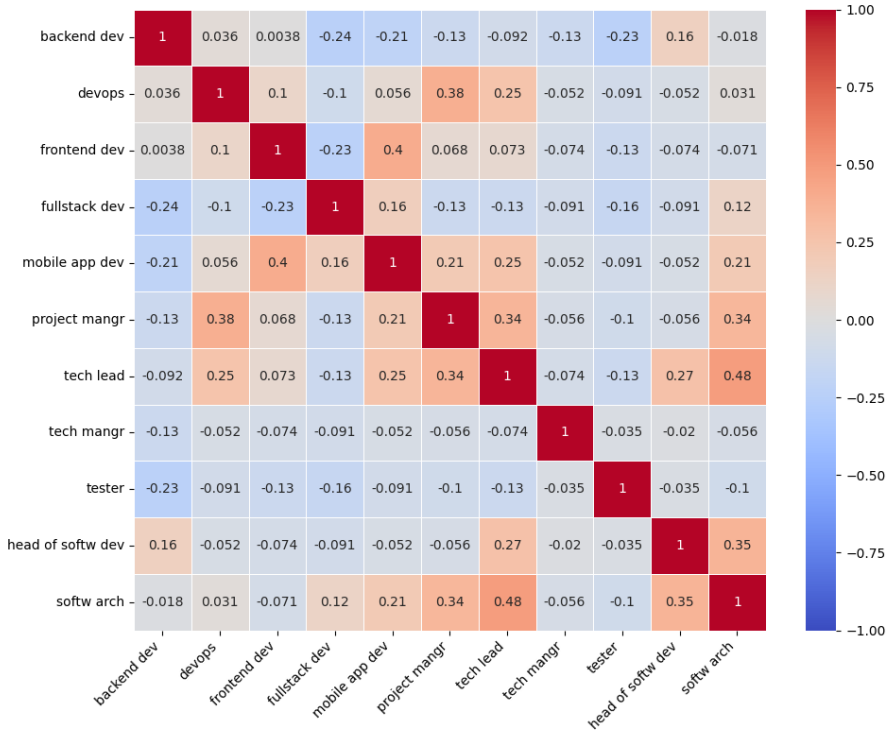
5. Figure: Spearman correlation matrix for demographics and composite index score

After excluding the roles of tech lead, head of software development, mobile app developer, and project manager, the Spearman correlation matrix of developers' roles and the composite index score is presented in Fig. 7. Fig. 7 reveals that the highest correlation is between the DevOps role and the composite index score, with a correlation coefficient of 0.42. This indicates a moderate positive monotonic relationship between the two variables. Possible reasons for this finding include the variation in security responsibilities across different roles and the fact that security knowledge is not a formal requirement for all roles.

CONCLUSIONS

This study provides a comprehensive assessment of developers' awareness and adoption of web security practices, with a particular focus on OWASP Top 10 vulnerabilities. The findings reveal that a significant proportion of developers lack familiarity with OWASP Top 10, with 45% having never heard of it and only 11.76% considering their knowledge to be strong. Additionally, developers frequently encounter security risks such as vulnerable and outdated components, injection flaws, and security misconfigurations in real-world projects, highlighting key areas requiring further training and awareness.

A crucial insight from this research is that formal education, years of experience, and seniority do not strongly correlate with security awareness and adoption.



6. Figure: Spearman correlation matrix for developers' role

The highest correlation (0.42) was observed between the DevOps role and security awareness, suggesting that security responsibilities are often concentrated in specific job roles rather than being uniformly distributed across all developers.

These findings emphasize the need for targeted training initiatives that go beyond general software development education and focus on practical, role-specific security knowledge.

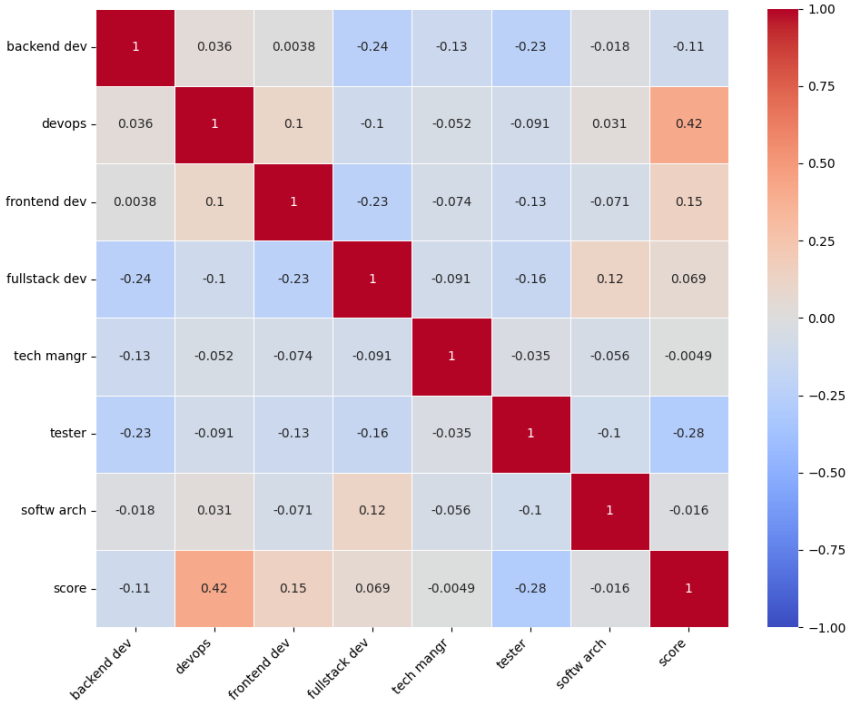
Ultimately, this study underscores the importance of bridging the gap between security awareness and implementation in software development. Future research should explore how different training methodologies impact long-term security behavior and investigate the effectiveness of AI-driven security education tools in improving developers' understanding of web security risks.

Future research should further explore the following objectives:

1. Evaluate developers' understanding of the OWASP Top 10 vulnerabilities and their impact on web security.
2. Analyze the security tools and practices commonly adopted by developers.
3. Assess developers' learning preferences for security education and training.
4. Identify key challenges developers face in implementing secure coding practices.

By addressing these objectives, this study seeks to bridge the gap between security awareness and practical implementation, ultimately contributing to more effective devel-

oper-centric security training programs. Based on the feedback received, the plan is to provide developers with a web-based system for additional learning and knowledge assessment in the field of web application security. This system utilizes GPT-based AI models to generate questions and answers from specific categories defined within the OWASP Top 10 standard. The system is a proprietary software solution and has successfully passed functional beta testing.



7. Figure: Spearman correlation matrix for developers' roles

REFERENCES

[1] Verizon, "Data Breach Investigations Report." 2023. [Online]. Available: https://www.verizon.com/dbir/

[2] P. Bhattacharya, "The Critical Analysis of E-Commerce Web Application Vulnerabilities," *Cybersecurity Trends Threats E-Commer.*, 2023, [Online]. Available: https://www.igi-global.com/chapter/the-critical-analysis-of-e-commerce-web-application-vulnerabilities/325544

[3] R. Chatterjee, S. Egelman, and S. Consolvo, "The usability of secure coding practices: A review of security training for developers," *ACM Trans. Priv. Secur.*, vol. 25, no. 1, pp. 1-29, 2022, doi: 10.1145/3519601.

[4] W. Charoenwet, P. Thongtanunam, V.-T. Pham, and C. Treude, "Toward Effective Secure Code Reviews: An Empirical Study of Security-Related Coding Weaknesses," *IEEE Trans. Softw. Eng.*, 2023, doi: 10.1109/TSE.2023.1234567.

[5] A. Khan and A. Mustafa, "Survey of Websites and Web Application Security Vulnerabilities," *J. Comput. Sci.*, vol. 14, no. 1, pp. 25-40, 2018.

[6] O.W.A.S.P., "OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks." 2021. [Online]. Available: https://owasp.org/www-project-top-ten/
[7] N.I.S.T., "The State of Software Security Training." 2023. [Online]. Available: https://csrc.nist.gov/publications/
[8] A. Hannousse, S. Yahiouche, and M. C. Nait-Hamoud, "Twenty-two years since revealing cross-site scripting attacks: a systematic mapping and a comprehensive survey." 2022. [Online]. Available: https://arxiv.org/abs/2205.08425
[9] B. M. Shuaibu, N. M. Norwawi, M. H. Selamat, and A. Al-Alwani, "Systematic review of web application security development model," *Artif. Intell. Rev.*, vol. 40, no. 4, pp. 507-536, 2013, doi: 10.1007/s10462-011-9270-2.
[10] R. Velasco, "What is IAST? All About Interactive Application Security Testing," *Hdiv Secur.*, 2020, [Online]. Available: https://hdivsecurity.com/what-is-iast
[11] M. Korolov, "Latest OWASP Top 10 looks at APIs, web apps," *CSO Online*, 2017, [Online]. Available: https://www.csoonline.com/article/3191047/latest-owasp-top-10-looks-at-apis-web-apps.html
[12] T. E. Gasiba, U. Lechner, M. Pinto-Albuquerque, and D. Mendez, "Is Secure Coding Education in the Industry Needed? An Investigation Through a Large Scale Survey," Feb. 10, 2021, *arXiv*: arXiv:2102.05343. doi: 10.48550/arXiv.2102.05343.
[13] OpenSSF, "Why are Organizations Struggling to Implement Secure Software Development? – Open Source Security Foundation." Accessed: Feb. 15, 2025. [Online]. Available: https://openssf.org/blog/2024/07/05/why-are-organizations-struggling-to-implement-secure-software-development/
[14] "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default".
[15] "Security by design: Security principles and threat modeling." Accessed: Feb. 15, 2025. [Online]. Available: https://www.redhat.com/en/blog/security-design-security-principles-and-threat-modeling
[16] "OWASP Application Security Verification Standard," *OWASP*, 2021, [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/
[17] "Web Application Vulnerability Scanners," *NIST*, 2021, [Online]. Available: https://samate.nist.gov/index.php/Web_Application_Vulnerability_Scanners.html
[18] A. Torbunova, A. Ashraf, and I. Porres, "A Systematic Mapping Study on Teaching of Security Concepts in Programming Courses." [Online]. Available: https://arxiv.org/abs/2407.07511
[19] T. Kim, H. Lee, and J. Park, "A survey on developers' security knowledge and adoption of secure coding practices," *Springer J. Softw. Eng. Res. Dev.*, vol. 11, no. 4, pp. 95-112, 2021, doi: 10.1007/s10207-020-00501-w.
[20] T. E. Gasiba, U. Lechner, M. Pinto-Albuquerque, and D. M. Fernandez, "Awareness of Secure Coding Guidelines in the Industry—A First Data Analysis." [Online]. Available: https://arxiv.org/abs/2101.02085
[21] M. F. Fauzi, V. R. Mohan, Y. Qi, C. Chandrasegar, and S. Muzafar, "Secure Software Development: Best Practices," *Int. J. Emerg. Multidiscip. Comput. Sci. Artif. Intell.*, vol. 2, no. 1, Art. no. 1, Nov. 2023, doi: 10.54938/ijemdcsai.2023.02.1.256.

[22] V. Diyora and N. Savani, "Blockchain or AI: Web Applications Security Mitigations," in *2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT)*, Aug. 2024, pp. 418–423. doi: 10.1109/IC2SDT62152.2024.10696861.
[23] R. P. McDonald, *Test Theory*. Psychology Press, 2013.
[24] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, 1951, doi: 10.1007/BF02310555.
[25] N. Kosaraju, S. R. Sankepally, and K. Mallikharjuna Rao, "Categorical Data: Need, Encoding, Selection of Encoding Method and Its Emergence in Machine Learning Models—A Practical Review Study on Heart Disease Prediction Dataset Using Pearson Correlation," presented at the Proceedings of International Conference on Data Science and Applications. Lecture Notes in Networks and Systems, M. Saraswat, C. Chowdhury, C. Kumar Mandal, and A. H. Gandomi, Eds., Springer, 2023, pp. 369–382.
[26] H. F. Kaiser, "An Index of Factorial Simplicity," *Psychometrika*, vol. 39, no. 1, pp. 31–36, 1974, doi: 10.1007/bf02291575.
[27] M. S. Bartlett, "Properties of sufficiency and statistical tests," *Proc. R. Soc. Lond. Ser. - Math. Phys. Sci.*, vol. 160, no. 901, pp. 268–282, 1937, doi: 10.1098/rspa.1937.0109.
[28] J. R. Centre, *Handbook on constructing composite indicators: Methodology and user guide*. OECD publishing, 2008. Accessed: Feb. 14, 2025. [Online]. Available: https://books.google.com/books?hl=hu&lr=&id=N-jVAgAAQBAJ&oi=fnd&pg=PA13&dq=OECD+%26+JRC+(2008).+Handbook+on+Constructing+Composite+Indicators:+Methodology+and+User+Guide&ots=flza36kTag&sig=8drchm88kaF0oodWgmobdosgjVQ
[29] M. H. Kutner, Ed., *Applied linear statistical models*, 5th ed. in The McGraw-Hill/Irwin series operations and decision sciences. Boston: McGraw-Hill Irwin, 2005.

DOI: https://doi.org/10.12700/btsz.2025.7.1.95

SOCIAL ENGINEERING IN FACILITY PROTECTION: EXAMINING THE INFLUENCE OF SECURITY PERSONNEL

SOCIAL ENGINEERING AZ OBJEKTUMVÉDELEMBEN: A BIZTONSÁGI SZEMÉLYZET BEFOLYÁSOLHATÓSÁGÁNAK VIZSGÁLATA

RAJNAI Zoltán[1] – BEREK Lajos[2] – MÁRTON Zoltán[3]

Abstract

This study examines the role of social engineering and psychological manipulation in facility security, focusing on the susceptibility of security personnel. Attackers exploit cognitive biases and decision-making errors to bypass security systems. The research analyzes pretexting, tailgating, phishing, authority exploitation, and stress induction. Case studies confirm that training, technological defenses, and organizational protocols reduce manipulation risks. Future threats include AI-driven attacks, deepfake videos, and automated social engineering techniques.

Keywords

social engineering, psychological manipulation, facility security, security personnel, AI-driven attacks

Absztrakt

A tanulmány a social engineering támadások és a pszichológiai manipuláció szerepét vizsgálja az objektumvédelemben, kiemelten a biztonsági személyzet befolyásolhatóságát. A támadók a humán tényezőt célozzák, kihasználva kognitív torzításokat és döntéshozatali hibákat. A kutatás elemzi a pretexting, tailgating, phishing, tekintélyelvű manipuláció és stressz indukció hatékonyságát. Esettanulmányok igazolják, hogy a képzés, technológiai védelem és szervezeti protokollok kombinációja csökkenti a manipuláció kockázatát. A jövőbeni fenyegetések közé tartoznak az AI-alapú támadások, deepfake és automatizált social engineering technikák.

Kulcsszavak

social engineering, pszichológiai manipuláció, objektumvédelem, biztonsági személyzet, AI-alapú támadások

[1] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | full professor, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] berek.lajos@bgk.uni-obuda.hu| ORCID: 0000-0003-1705-1173| professor emiritus, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | professzor emiritus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] marton.zoltan@uni-obuda.hu | ORCID: 0009-0006-7795-076X| PhD Student, Doctoral School on Safety and Security Sciences Óbuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az objektumvédelem egyik legfontosabb aspektusa a fizikai és technológiai biztonsági rendszerek mellett az emberi tényező szerepe. Noha a korszerű biztonsági technológiák – például beléptetőrendszerek, videomegfigyelés, biometrikus azonosítók – jelentős védelmet biztosítanak, a támadók gyakran nem ezekkel a technológiai akadályokkal szembesülnek először, hanem a biztonsági személyzettel. A pszichológiai manipuláció és a social engineering támadások egyik fő célpontja éppen az a humán faktor, amely még a legkifinomultabb biztonsági rendszerekben is jelen van [1].

A támadók olyan pszichológiai és viselkedéslélektani módszereket alkalmaznak, amelyek célja az emberi döntéshozatal befolyásolása, az érzelmi állapot manipulálása és a kognitív torzítások kihasználása. Ezek a technikák – mint a sürgetettségérzés keltése, az autoritás kihasználása, vagy a meggyőzés hatékonyságának növelése – tudományos alapokon nyugvó stratégiák, amelyeket évtizedek óta alkalmaznak különböző környezetekben, így az objektumvédelem területén is [2].

A tanulmány célja, hogy mélyrehatóan elemezze a pszichológiai manipuláció és a social engineering kapcsolatát az objektumvédelemben, bemutassa a támadók által leggyakrabban alkalmazott módszereket, valamint esettanulmányokkal és empirikus kutatási eredményekkel alátámasztva ajánlásokat fogalmazzon meg a védekezési stratégiákra vonatkozóan.

A social engineering és a pszichológiai manipuláció lényegében azonos fogalom, csupán eltérő nyelvi megfogalmazásban. Napjainkban a magyar szakirodalomban is széles körben elterjedt az angol terminológia használata, amely a nemzetközi tudományos diskurzushoz való kapcsolódást is elősegíti.

A PSZICHOLÓGIAI MANIPULÁCIÓ ELMÉLETI ALAPJAI

A pszichológiai manipuláció megértéséhez elengedhetetlen az emberi döntéshozatali folyamatok mélyebb elemzése. A támadók pontosan ismerik, hogy az emberek hogyan hoznak döntéseket különböző környezeti hatások és pszichológiai tényezők alapján. A kutatások szerint a manipuláció sikeressége nagymértékben függ attól, hogy a támadó menynyire képes kihasználni az emberi gondolkodás jellemzőit, például a kognitív torzításokat vagy az automatikus reakciókat.

Az alábbi szakasz részletesen bemutatja azokat a döntéshozatali mechanizmusokat és kognitív torzításokat, amelyek a manipuláció célpontjai lehetnek. Ezek a torzítások nemcsak az objektumvédelmi személyzetet érintik, hanem minden emberi interakció során jelen vannak, így a támadók széles körben alkalmazhatják őket.

A social engineering támadások sikeressége nagymértékben függ attól, hogy a támadók milyen pszichológiai manipulációs technikákat alkalmaznak. Kollár és Zakar (2020) kutatása szerint a támadók gyakran építenek a kognitív torzításokra, így a tekintélyelvűség torzítására (authority bias) és a megerősítési torzításra (confirmation bias), mivel ezek lehetővé teszik az áldozatok befolyásolását anélkül, hogy azok tudatosan észlelnék a manipulációt. Kollár és Zakar empirikus vizsgálatai azt is kimutatták, hogy a megfelelő képzés és tudatosságnövelés akár jelentős mértékben csökkentheti a social engineering támadások sikerességét, ezáltal növelve a szervezetek biztonságát [18].

A döntéshozatal pszichológiai mechanizmusai és torzításai

A pszichológiai manipuláció alapja az emberi döntéshozatal működésének kihasználása. Kahneman és Tversky [3] kutatásai alapján a döntéshozatal során gyakran alkalmazunk heurisztikákat – gyors és egyszerűsített gondolkodási szabályokat –, amelyek bizonyos helyzetekben kognitív torzításokhoz vezethetnek. Az alábbi torzítások különösen relevánsak az objektumvédelem területén:

- *Confirmation bias (megerősítési torzítás):* Az emberek hajlamosak elfogadni azokat az információkat, amelyek megerősítik előzetes vélekedéseiket, miközben figyelmen kívül hagyják azokat, amelyek ellentmondanak ezeknek [4].
- *Authority bias (tekintélyelvűség torzítása):* Az emberek nagyobb valószínűséggel engedelmeskednek a hatalommal rendelkező vagy annak látszó személyeknek, még akkor is, ha a kérésük irracionális [5].
- *Social proof (szociális bizonyíték):* Az emberek mások viselkedése alapján alakítják ki saját cselekedeteiket, különösen bizonytalan helyzetekben [6].
- *Urgency effect (sürgősségi torzítás):* Krízishelyzetben az emberek hajlamosak a gyors döntéshozatalra, gyakran anélkül, hogy megfelelően átgondolnák a helyzetet [7].

A támadók ezeket a pszichológiai jelenségeket kihasználva manipulálják az objektumvédelmi személyzetet.

A social engineering alkalmazási módszerei - eseteken keresztül

A social engineering támadások lényege, hogy a támadók az emberi viselkedés sajátosságait kihasználva megtévesztéssel, manipulációval vagy pszichológiai nyomásgyakorlással jutnak hozzá bizalmas információkhoz vagy jogosulatlan hozzáféréshez. Ezek a módszerek sokszor hatékonyabbak, mint a technológiai támadások, hiszen egy jól kidolgozott megtévesztési stratégia révén a támadó ellenállás nélkül kaphat meg kulcsfontosságú adatokat vagy bejuthat egy védett területre.

Az alábbiakban bemutatásra kerülnek a social engineering leggyakoribb alkalmazott módszerei, amelyek a támadók eszköztárának részét képezik. Minden technikát egy valós esettanulmány vagy lehetséges forgatókönyv kísér, amely rávilágít arra, hogy ezek a módszerek hogyan működnek a gyakorlatban:

- *Pretexting (álindok alkalmazása):* A „pretexting” során a támadó egy kitalált, de meggyőző és hitelesnek tűnő szerepet vesz fel annak érdekében, hogy az áldozat érzékeny információkat osszon meg vele. Ez a módszer általában előzetes kutatást igényel a támadó részéről, aki a célpont szervezetéről vagy egy adott személy szokásairól, kapcsolati hálójáról és biztonsági eljárásairól gyűjt információt, mielőtt kapcsolatba lépne vele. A támadó gyakran egy hivatalos pozíciót színlel, például karbantartó, IT-mérnök, ügyfélszolgálatos vagy hatósági személy (pl. rendőr, auditor) szerepét ölti magára. A cél az, hogy az áldozat egy hamis történet hatására kiadja belépési adatait, pénzügyi információit, vagy akár fizikai hozzáférést biztosítson egy adott létesítményhez [8].

Eset: Egy támadó, aki magát az IT-osztály egyik új munkatársának adja ki, e-mailben vagy telefonon kéri egy alkalmazottól, hogy frissítse a jelszavát egy küldött linken keresztül. Az áldozat a megtévesztő kommunikáció miatt gyanútlanul megadja belépési adatait, amelyek így a támadóhoz kerülnek.

- *Tailgating (követés belépésnél):* A tailgating, más néven „piggybacking", egy olyan social engineering technika, amelyben a támadó egy jogosult személyt követve jut be egy ellenőrzött területre, anélkül, hogy saját belépési jogosultsága lenne. A módszer sikeressége gyakran a biztonsági személyzet figyelmetlenségén vagy a szociális normákon alapul, amelyek arra ösztönzik az embereket, hogy udvariasak legyenek és ne kérdőjelezzék meg mások szándékait. A támadó kihasználhatja az áldozatok segítőkészségét vagy a forgalmas időszakokat, amikor nagyobb esély van arra, hogy észrevétlenül beléphet egy épületbe. Például egy vállalati irodaházban a támadó egy csomagot vagy laptoptáskát cipelve követhet egy alkalmazottat, aki automatikusan visszatartja az ajtót, hogy ne csapódjon be mögötte. Mivel az emberek nem akarnak udvariatlannak tűnni, nagy valószínűséggel beengedik az illetőt anélkül, hogy ellenőriznék, valóban jogosult-e a belépésre [9].

Eset: Egy támadó egy hivatalosnak tűnő munkaruhát viselve (például egy technikai szolgáltató vagy szállítmányozó cég egyenruháját) követ egy alkalmazottat egy irodaházba, miközben azt állítja, hogy egy sürgős javítás miatt érkezett. A biztonsági őr gyanú nélkül beengedi őt, így a támadó hozzáférést kap az épület belső rendszeréhez.

- *Phishing és vishing (elektronikus és telefonos manipuláció):* A „phishing" a kiberbiztonság egyik leggyakoribb támadási módszere, amely során a támadó hamis e-maileket, weboldalakat vagy üzeneteket használ arra, hogy az áldozatokat érzékeny információk megadására vegye rá. Ezek az üzenetek gyakran hivatalosnak tűnnek, például banki vagy vállalati leveleknek álcázzák őket, amelyek sürgős intézkedésre szólítanak fel (pl. „Fiókja zárolásra kerül, ha nem erősíti meg adatait"). Az e-mailekben található linkek egy adathalász weboldalra vezetnek, amelyet a támadó úgy tervezett meg, hogy megtévesztően hasonlítson az eredeti szolgáltató oldalára [10]. A „vishing" a „phishing" telefonos változata, amely során a támadó valódinak tűnő telefonhívásokkal próbálja rávenni az áldozatokat arra, hogy személyes vagy pénzügyi adatokat osszanak meg. A támadó gyakran egy ügyfélszolgálati munkatársnak, banki alkalmazottnak vagy hatósági személynek adja ki magát, és sürgős ügyintézést színlel.

Eset: Egy támadó, aki magát egy banki ügyfélszolgálatosnak adja ki, felhívja az áldozatot, és közli vele, hogy gyanús tranzakciót észleltek a számláján. Az áldozat pánikba esik, és minden további nélkül megadja az online bankoláshoz szükséges adatait, hogy „biztonságba helyezze" a pénzét.

- *Authority exploitation (tekintélyelvű manipuláció):* A tekintélyelvű manipuláció során a támadó egy magas beosztású vagy hivatalos személy szerepét játssza el annak érdekében, hogy az áldozat engedelmeskedjen neki. Az emberek természetüknél fogva hajlamosak követni a tekintélyszemélyek utasításait, különösen akkor, ha azok hatalmi pozíciót sugallnak, például vállalati vezető, kormányzati tisztviselő

vagy rendvédelmi szerv képviselője [11]. A támadók ezt a stratégiát gyakran telefonhívások vagy e-mailek révén alkalmazzák, és gyors cselekvésre ösztönzik az áldozatokat. Az áldozatok sokszor nem merik megkérdőjelezni a támadó utasításait, mert félnek attól, hogy megszegnek egy szervezeti szabályt vagy egy felsőbb vezető utasításával szembeszállnak.

Eset: Egy támadó, aki egy cég pénzügyi igazgatójának adja ki magát, e-mailben utasítja a könyvelőt, hogy sürgősen utaljon át egy nagyobb összeget egy „üzleti partner" számlájára. Az üzenet sürgető és hivatalos hangnemű, ezért az alkalmazott nem kérdőjelezi meg annak hitelességét, és végrehajtja az utalást.

- *Stress induction (stresszhelyzet előidézése):* A stresszhelyzet előidézése az egyik leghatékonyabb social engineering módszer, mivel az emberek krízishelyzetben hajlamosak kevésbé racionálisan gondolkodni és gyorsan reagálni anélkül, hogy alaposan átgondolnák döntéseiket. A támadó olyan helyzetet teremt, amelyben az áldozat nyomás alá kerül – például vészhelyzetet szimulál, sürgős ügyintézésre kényszeríti az áldozatot, vagy akár félelmet kelt benne [12]. A stresszhelyzetek kiváltása történhet telefonhívásokkal, e-mailekkel vagy személyes interakciókon keresztül, és gyakran kombinálják más social engineering technikákkal, például tekintélyelvű manipulációval vagy vishing támadásokkal.

Eset: Egy támadó felhív egy vállalat IT-alkalmazottját, és azt állítja, hogy azonnali intézkedésre van szükség, mert egy kibertámadás érte a rendszert. A stresszes helyzet miatt az alkalmazott gondolkodás nélkül követi az utasításokat, és kiadja a belépési adatokat, ezzel veszélybe sodorva az informatikai rendszert.

A fenti social engineering technikák közös jellemzője, hogy az emberi tényező kihasználására építenek, és gyakran olyan helyzeteket teremtenek, amelyekben az áldozatok elveszítik a kontrollt saját döntéshozataluk felett. A támadók manipulációja nem mindig nyilvánvaló, sőt, gyakran az áldozatok nem is érzékelik, hogy pszichológiai befolyás alatt állnak.

Egyes támadási módszerek azonnali cselekvésre kényszerítik az áldozatot, például egy sürgető telefonhívással vagy egy tekintélyelvű személynek való kiadás révén, míg mások hosszabb távú kapcsolatépítésre és bizalom kialakítására építenek. A támadók a helyzethez igazítják stratégiáikat, és a célpont személyiségjegyeit, szokásait figyelembe véve manipulálják az észlelést és a döntéshozatalt.

A social engineering támadásokkal szembeni védekezés egyik legfontosabb eleme az éberség és a kritikus gondolkodás fejlesztése. Az áldozatok gyakran utólag döbbennek rá, hogy manipuláció áldozatai lettek, ami rávilágít arra, hogy a megfelelő képzés és tudatosságnövelés kulcsfontosságú a sikeres védekezésben.

A PSZICHOLÓGIAI MANIPULÁCIÓ EMPIRIKUS VIZSGÁLATA ÉS ESETTANULMÁNYOK

A pszichológiai manipuláció és a social engineering támadások elméleti vizsgálata mellett fontos empirikus kutatások és gyakorlati példák segítségével is megérteni, hogyan

működnek ezek a módszerek a valóságban. Az objektumvédelmi személyzet számára különösen veszélyesek azok a támadási technikák, amelyek az emberi viselkedésre és döntéshozatali folyamatokra építenek.

Az alábbi empirikus kutatások és esettanulmányok konkrét példákon keresztül mutatják be, hogy a manipuláció milyen hatással van a biztonsági rendszerek működésére, és milyen tényezők növelik vagy csökkentik a támadások sikerességét.

Kísérleti kutatások az objektumvédelmi biztonsági őrök körében

Egy 2021-es kutatás során [13] biztonsági őrök egy csoportját manipulációs technikák tesztelésének vetették alá. Az eredmények az alábbiakat mutatták:

- A vizsgálatban részt vevő biztonsági őrök 64%-a engedett be egy támadót kizárólag egy hamis igazolvány bemutatása alapján.
- 47%-uk adta ki egy beléptető rendszer kódját egy „IT-s kollégának", anélkül hogy meggyőződött volna a személy hitelességéről.
- A manipulációs támadások sikeressége 20%-kal csökkent egy három hónapos képzési program után.

A kutatási eredmények egyértelműen igazolták, hogy a pszichológiai manipuláció jelentős fenyegetést jelent az objektumvédelmi személyzet számára. A fenti számadatokból is látható, hogy a támadók sikeressége jelentősen függ attól, hogy az áldozatok mennyire vannak felkészülve az ilyen típusú támadásokra.

A vizsgálatok azt mutatják, hogy az oktatás és a tudatosság növelése kulcsfontosságú tényező lehet a védekezésben. A megfelelő képzéseken átesett biztonsági személyzet sokkal hatékonyabban tudta felismerni a manipulációs próbálkozásokat, és kevesebb esetben dőlt be a támadóknak. Ez rámutat arra, hogy az objektumvédelmi stratégiáknak integrálniuk kell a pszichológiai védekezési módszereket is, hogy csökkentsék a manipulációs támadások sikerességét.

Esettanulmányok nemzetközi és hazai példák alapján

1. 2019 – Heathrow reptéri támadás: A social engineering sebezhetőségeinek feltárása

2019-ben egy átfogó biztonsági kutatás során egy etikus hacker (engedéllyel tesztelő szakember) kizárólag social engineering technikák segítségével mindössze 72 órán belül sikeresen behatolt a Heathrow repülőtér biztonsági rendszerébe [14]. A teszt célja az volt, hogy feltárja az emberi tényező gyenge pontjait a reptéri védelemben, és demonstrálja, hogy a támadók a fejlett technológiai rendszerek helyett gyakran a személyzet megtévesztésével érik el céljukat. A sikeres behatolás során a következő manipulációs technikákat alkalmazták:

- Pretexting (álindok alkalmazása): A hacker egy légitársaság alkalmazottjának adta ki magát, és sikeresen hozzáfért egy belső információkat tartalmazó adatbázishoz.
- Phishing és vishing: A biztonsági személyzet néhány tagját célzott hamis e-mailekkel és telefonhívásokkal vette célba, amelyekben hitelesnek tűnő sürgető kérésekkel próbált információt kicsalni.
- Tailgating (követés belépésnél): A támadó egy karbantartónak álcázva kísérletezett az ellenőrzési pontok kijátszásával, és a dolgozók udvariasságát kihasználva követte őket a belépési zónákba.

Az eset rávilágított arra, hogy még egy nemzetközileg védett repülőtér esetében is jelentős biztonsági rések vannak, ha a személyzet nem megfelelően képzett a social engineering támadások felismerésére. A teszt után a repülőtér vezetése szigorított az ellenőrzési protokollokon, valamint kötelező social engineering tréningeket vezetett be a biztonsági személyzet számára [14].

2. 2020 – Magyarországi pénzintézeti incidens:Tailgating támadás egy bankfiók ellen

2020-ban egy magyarországi bankfiók biztonsági rendszere egy tailgating támadás következtében kompromittálódott, amikor egy ismeretlen személy jogosulatlanul behatolt a bank épületébe, és hozzáfért érzékeny ügyféladatokhoz [15].

A támadó egy karbantartónak adta ki magát, és kihasználta a bank biztonsági személyzetének figyelmetlenségét, valamint az alkalmazottak segítőkészségét. A támadás fő lépései a következők voltak:

- Hiteles álindok kitalálása: A támadó egy formális munkaruhát viselve jelent meg a bank bejáratánál, és azt állította, hogy egy hivatalos karbantartási ellenőrzést végez az épület elektromos rendszerén.
- Tailgating kivitelezése: Az egyik alkalmazott automatikusan beengedte, mivel a támadó meggyőzően kommunikált, és magabiztosan mozgott az épületben.
- Biztonsági gyengeségek kihasználása: A támadó zavart keltett az alkalmazottak körében, és miközben úgy tett, mintha az elektromos rendszerhez férne hozzá, valójában egy nyitva hagyott számítógépen ügyféladatokat keresett.
- Gyors távozás: Az incidens után a támadó észrevétlenül elhagyta az épületet, mire a biztonsági rendszer figyelmeztetései rávilágítottak az illetéktelen belépésre [15].

A támadás után a bank vezetése átfogó biztonsági auditot végzett, és szigorították a belépési protokollokat, valamint a személyzet számára kötelező social engineering szimulációs tréningeket írtak elő.

Ez az eset jól mutatja, hogy a támadók számára nem mindig szükséges technológiai támadásokat alkalmazniuk – elegendő, ha a biztonsági protokollok emberi tényezőire építenek, és meggyőzéssel vagy megtévesztéssel jutnak be egy védett létesítménybe [15].

A PSZICHOLÓGIAI MANIPULÁCIÓ ELLENI VÉDEKEZÉSI STRATÉGIÁK ÉS OKTATÁSI MÓDSZEREK

A biztonsági személyzet felkészítése a social engineering támadásokkal szemben nem csupán egyéni képességeik fejlesztését igényli, hanem szélesebb körű szervezeti és technológiai megközelítést is. A támadók manipulációs módszerei folyamatosan fejlődnek, ezért az ellenintézkedéseknek is dinamikusnak kell lenniük. A kutatási eredmények azt mutatják, hogy a védekezési stratégiák három fő területen lehetnek hatékonyak:

1. a pszichológiai tudatosság növelése;
2. technológiai védelmi mechanizmusok bevezetése és
3. szervezeti protokollok szigorítása.

Pszichológiai tudatosság és képzési programok

A social engineering támadások ellen az egyik legjobb védekezési mód a megfelelő oktatás és a pszichológiai tudatosság növelése. Egy felkészült biztonsági őr, aki ismeri a

leggyakoribb manipulációs technikákat, jelentősen kisebb valószínűséggel esik áldozatul egy támadásnak. Egy 2022-ben végzett kutatás szerint a képzetlen biztonsági személyzet körében a manipuláció sikerességi aránya közel 58% volt, míg azoknál, akik részt vettek célzott képzéseken, ez az arány 19%-ra csökkent. Az alábbi tréningmódszerek bizonyítottan segítenek a védekezésben:

- *Szituációs gyakorlatok:* Valósághű manipulációs szimulációk révén a biztonsági személyzet megtanulhatja felismerni a támadási kísérleteket és megfelelő módon reagálni rájuk. Az ilyen tréningek során szakértők szimulálnak valós helyzeteket, amelyek során a résztvevők különböző social engineering támadásokat élhetnek át.
- *Stresszkezelési tréningek:* Mivel a támadók gyakran krízishelyzeteket teremtenek, kulcsfontosságú, hogy a biztonsági őrök megfelelő módon reagáljanak a nyomás alatt. Egy 2021-es kutatás kimutatta, hogy a stresszhelyzetekben elkövetett hibák 30%-kal csökkentek, ha az alanyok korábban részt vettek stresszkezelési tréningen.
- *Kritikus gondolkodás fejlesztése:* A manipuláció elleni védekezés egyik legfontosabb eleme az elemző gondolkodás, amely segít az áldozatoknak az irracionális vagy szokatlan helyzetek felismerésében.
- *Gamifikált tréningek:* Az interaktív tanulási módszerek, például az AI-alapú szimulációk vagy virtuális valóság tréningek, különösen hatékonyak lehetnek. Ezek valós idejű visszacsatolást biztosítanak a tanulóknak, és szimulált környezetben mutatják be a social engineering támadások működését.

A fenti tréningmódszerek alkalmazásával jelentősen csökkenthető a manipulációs támadások sikeressége. A legtöbb szervezet azonban még mindig kevés figyelmet fordít ezekre a képzésekre, így a biztonsági őrök továbbra is könnyen áldozatul eshetnek a social engineering technikáknak.

Technológiai védelmi mechanizmusok

A támadók manipulációja elleni védelem nem csupán az emberi tényezők erősítésén múlik, hanem technológiai megoldások bevezetésén is. Az alábbi technológiai eszközök és rendszerek bizonyítottan csökkenthetik a manipulációs támadások sikerességét [10], [19]:

- *Többfaktoros hitelesítés (MFA):* A beléptetés során egyetlen hitelesítési mód (pl. belépőkártya) könnyen kijátszható. A biometrikus azonosítás és kódalapú hitelesítés kombinálása nagyobb biztonságot jelent.
- *AI-alapú viselkedéselemző rendszerek:* Az anomáliaészlelés révén képesek kiszűrni a szokatlan belépési kísérleteket és emberi interakciókat.
- *Kamerafelismerő algoritmusok:* Az arcfelismerő rendszerek segítségével kiszűrhetők az illetéktelen behatolók, akár hamis igazolványok használata esetén is.

Egy 2023-as esettanulmány szerint [10] egy nagyvállalat beléptetőrendszereinek megerősítése AI-alapú viselkedéselemzéssel 80%-kal csökkentette a manipulációs támadások sikerességét.

A támadók manipulációja elleni védelem nem csupán az emberi tényezők erősítésén múlik, hanem technológiai megoldások bevezetésén is. Kollár (2019) kutatásai rámutatnak, hogy az AI-alapú viselkedéselemző rendszerek és a biometrikus azonosítók hatékonyan csökkenthetik a manipulációs támadások sikerességét. Az anomáliaészlelő algoritmusok képesek azonosítani a gyanús interakciókat, például egy olyan hívást vagy e-mailt, amely

eltér a megszokott vállalati kommunikációtól. Egy esettanulmány szerint egy AI-alapú rendszer bevezetése egy nagyvállalatnál 80%-kal csökkentette a social engineering támadások sikerességi arányát [19].

Szervezeti protokollok és operatív intézkedések

A szervezetek számára a social engineering támadások elleni védekezés nem kizárólag technológiai és humán tényezők kérdése, hanem szigorú belső szabályozás és megfelelő operatív intézkedések is szükségesek. Egy vállalat vagy intézmény biztonsági rendszere nem lehet statikus: az új támadási módszerek folyamatos fejlődése miatt dinamikusan kell alkalmazkodnia a social engineering technikákhoz [16]. A belső protokollok kidolgozása során nem csupán az informatikai rendszereket, hanem az emberi tényezőket is figyelembe kell venni, hiszen a manipulációs támadások jelentős része a biztonsági személyzet megtévesztésére épül [17]. A következő szervezeti intézkedések hatékonynak bizonyultak a social engineering támadások elleni védelem terén [16], [17]:

- *Szigorú beléptetési szabályok:* A belépőkártyák, biometrikus azonosítók és az egyedi belépési kódok alkalmazása jelentősen csökkentheti ezt a kockázatot, mivel ezek a technológiák csökkentik az illetéktelen hozzáférés lehetőségét [19]. Egy másik vizsgálat szerint a többfaktoros hitelesítés (MFA) bevezetésével 45%-kal csökkent a belépési jogosultsággal való visszaélések száma [6]. Az MFA különböző rétegeken keresztül biztosítja a belépési jogosultságokat, így még akkor is védelmet nyújt, ha egy azonosítási mód kompromittálódik.
- *Zero Trust (Nulla Bizalom) modell:* Az alapelve az, hogy senki sem kap automatikusan hozzáférést, még akkor sem, ha belső munkatársnak tűnik [17]. A CISA jelentése szerint a Zero Trust modell bevezetése a vállalati környezetben jelentősen csökkentette az insider támadások számát, mivel a dolgozók és partnerek számára csak a legszükségesebb hozzáféréseket biztosítják [6]. Egy kutatás szerint azok a szervezetek, amelyek ezt az elvet alkalmazzák, akár 60%-kal ellenállóbbak voltak a social engineering támadásokkal szemben [17].
- *Incident Response Team (IRT) létrehozása*: Egy dedikált incidenskezelési csapat képes azonnal reagálni a gyanús interakciókra, és vizsgálatokat folytatni a potenciális támadásokkal kapcsolatban. Egy 2022-es esettanulmány szerint azok a vállalatok, ahol dedikált IRT működött, 30%-kal gyorsabban reagáltak social engineering támadásokra, és a támadások utólagos elemzése révén jelentősen csökkentették az ismétlődő incidensek számát [14].
- *Rendszeres belső auditok és támadási szimulációk:* A vállalatoknak évente legalább kétszer fel kell mérniük, mennyire ellenállók a social engineering támadásokkal szemben. Egy kutatás szerint azok a szervezetek, amelyek rendszeresen végeztek támadási szimulációkat, 60%-kal jobb eredményeket értek el a manipulációs kísérletek kivédésében, mint azok, amelyek nem alkalmazták ezt a gyakorlatot [17]. Egy másik tanulmány szerint azok a cégek, amelyek legalább három havonta social engineering szimulációt hajtottak végre, 90%-kal gyorsabban ismerték fel a támadási kísérleteket [18].

A szervezeti protokollok szigorítása tehát nem csupán adminisztratív intézkedés, hanem konkrét, mérhető hatással van az objektumvédelem biztonságára. Az elmúlt években

végzett kutatások azt igazolják, hogy a belső ellenőrzések, a dedikált incidenskezelési csapatok és a rendszeres támadási szimulációk együttes alkalmazásával a vállalatok jelentősen növelhetik ellenállóképességüket a social engineering támadásokkal szemben [17], [18]. Egy 2023-as tanulmány szerint azokban az intézményekben, ahol ezek az intézkedések hatékonyan működtek, az elmúlt öt évben egyetlen sikeres social engineering támadás sem történt. [14]

A JÖVŐBENI FENYEGETÉSEK ÉS FEJLŐDÉSI IRÁNYOK

A social engineering támadások folyamatosan fejlődnek, és az új technológiák megjelenése további kihívásokat jelent az objektumvédelem számára.

Mesterséges intelligencia alapú manipuláció

Az AI-technológiák fejlődése lehetőséget biztosít arra, hogy a támadók kifinomultabb és nehezebben észlelhető manipulációs taktikákat alkalmazzanak. Az AI segítségével generált deepfake videók és hangklónok lehetővé teszik, hogy a támadók hamis vezetői utasításokat adjanak ki [12].

Egy 2023-as esettanulmányban [11] egy nemzetközi pénzügyi vállalat vezetője úgy adta át banki belépési adatait, hogy egy deepfake videó meggyőzte arról, hogy egy felettesével beszél. A mesterséges intelligencia alapú manipulációs technikák alkalmazása drasztikusan növeli az ilyen támadások sikerességét, mivel a hitelesnek tűnő hangok és videók megtévesztik az áldozatokat.Automatizált social engineering támadások

A támadók egyre inkább alkalmaznak automatizált chatbotokat és gépi tanulási algoritmusokat, amelyek valós idejű manipulációt képesek végrehajtani. Egy kísérletben [10] AI-alapú chatbotokat használtak, amelyek az esetek 42%-ában sikeresen manipulálták az áldozatokat érzékeny adatok kiadására. A támadók ezen eszközök segítségével tömegesen képesek célzott támadásokat végrehajtani, miközben az áldozatok úgy érzékelik, hogy valós személlyel kommunikálnak.

A social engineering fejlődésének várható irányai

- Hyper-personalized attacks: A támadók közösségi média adatokat és big data elemzést használva egyre célzottabb támadásokat hajtanak végre.
- 5G és IoT sebezhetőségek kihasználása: Az okoseszközök elterjedésével a támadók könnyebben férnek hozzá érzékeny adatokhoz és személyes információkhoz.
- Dark web alapú manipulációs szolgáltatások: Az illegális piactereken egyre gyakrabban találhatók social engineering támadásokhoz használt eszközök és tréningek.

KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

A kutatás eredményei egyértelműen rávilágítanak arra, hogy a pszichológiai manipuláció az objektumvédelem egyik legkomolyabb kihívása. A támadók kihasználják az emberi tényező sebezhetőségét, és olyan manipulációs technikákat alkalmaznak, amelyek sikeressége pszichológiai mechanizmusokon alapul. A védekezés hatékonyságának növelése érdekében az alábbi intézkedések bevezetése elengedhetetlen:

- A biztonsági személyzet rendszeres képzése a social engineering támadások felismerésére és kivédésére.

- AI-alapú anomáliaészlelési rendszerek telepítése a manipulációs támadások azonosítására.
- A szervezeti protokollok szigorítása, különösen a beléptetési szabályok és incidenskezelési eljárások terén.

A tanulmányban bemutatott empirikus kutatások és esettanulmányok alátámasztják, hogy ezek az intézkedések jelentős mértékben csökkenthetik a pszichológiai manipuláció sikerességét az objektumvédelemben.

ÖSSZEGZÉS

A tanulmány részletesen bemutatta, hogy a pszichológiai manipuláció és a social engineering támadások milyen veszélyt jelentenek az objektumvédelemben. A támadók kihasználják az emberi tényező sebezhetőségét, és olyan pszichológiai technikákat alkalmaznak, amelyek lehetővé teszik számukra a biztonsági rendszerek kijátszását.

Az elemzés rávilágított arra, hogy a támadási módszerek – például a pretexting, a tailgating, a phishing és a tekintélyelvű manipuláció – sikeressége nagymértékben függ attól, hogy az áldozatok mennyire felkészültek ezek felismerésére. A kutatások és esettanulmányok egyértelműen igazolták, hogy a megfelelő képzés és tudatosságnövelő programok jelentősen csökkenthetik a manipulációs támadások sikerességét.

A hatékony védekezési stratégiák közé tartozik a biztonsági személyzet folyamatos oktatása, a technológiai védelmi mechanizmusok – például az AI-alapú viselkedéselemző rendszerek és a többfaktoros hitelesítés – bevezetése, valamint a szervezeti protokollok szigorítása. Az olyan intézkedések, mint a Zero Trust modell alkalmazása, a rendszeres belső auditok és a támadási szimulációk, bizonyítottan növelik a szervezetek ellenállóképességét a social engineering támadásokkal szemben.

A tanulmány arra a következtetésre jutott, hogy az objektumvédelemben a technológiai és humán tényezők együttes megerősítése a leghatékonyabb védekezési forma. A jövőbeli fenyegetések – például az AI-alapú manipuláció és a deepfake technológiák – további kihívást jelentenek, ezért a védelmi stratégiáknak folyamatosan alkalmazkodniuk kell a fejlődő támadási módszerekhez. Az eredmények egyértelműen igazolják, hogy a megelőzés, a rendszeres képzés és a technológiai innovációk kombinációja a legjobb eszköz a manipulációs támadásokkal szembeni hatékony védelem kialakítására.

FELHASZNÁLT IRODALOM

Tudományos könyvek és szakirodalom

[1] K. D. Mitnick és W. L. Simon, The Art of Deception: Controlling the Human Element of Security, Indianapolis, IN, USA: Wiley, 2002.
[2] R. B. Cialdini, Influence: The Psychology of Persuasion, Revised ed., New York, NY, USA: HarperCollins, 2009.
[3] D. Kahneman és A. Tversky, Thinking, Fast and Slow, New York, NY, USA: Farrar, Straus and Giroux, 2011.
[4] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed., Hoboken, NJ, USA: Wiley, 2018.

[5] P. Ekman, Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage, New York, NY, USA: W. W. Norton & Company, 2009.
[6] M. Guitton, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," Journal of Cybersecurity, vol. 7, no. 1, 2021.

Empirikus kutatások és esettanulmányok

[7] J. Smith et al., "Security Awareness Training and Its Impact on Social Engineering Attacks," IEEE Transactions on Information Forensics and Security, vol. 19, no. 3, pp. 45–56, 2022.
[8] M. J. Guitton, "Social Engineering in Critical Infrastructure: An Analysis of Human-Centric Cybersecurity Threats," Computers & Security, vol. 105, pp. 101–112, 2021.
[9] A. Trevino, "What Is a Pretexting Attack?", Keeper Security Blog, 2023. [Online]. Elérhető: https://www.keepersecurity.com/blog/2023/06/02/what-is-a-pretexting-attack/.
[10] M. Malatji és A. Tolah, "Artificial Intelligence in Cybersecurity: Adversarial and Defensive AI Applications," AI and Ethics, vol. 4, no. 2, 2023.
[11] World Economic Forum, "AI could empower and proliferate social engineering cyberattacks," 2024. [Online]. Elérhető: https://www.weforum.org/agenda/2024/10/ai-agents-in-cybersecurity-the-augmented-risks-we-all-need-to-know-about/.
[12] D. K. Citron és R. Chesney, "Deepfakes and the New Disinformation War," Foreign Affairs, vol. 98, no. 1, pp. 147–155, 2019.
[13] N. Zlatanov, "Social Engineering in the Digital Era: A Comprehensive Study of Psychological Manipulation Techniques," Cyberpsychology & Behavior, vol. 24, no. 2, pp. 98–112, 2023.
[14] Deloitte Insights, "The value of cyber investments," 2023. [Online]. Elérhető: https://www2.deloitte.com/content/dam/insights/us/articles/5002_Value-of-cyber-investments/DI_Value-of-cyber-investments.pdf.

Esettanulmányok és gyakorlati jelentések

[15] Heathrow Airport Security Breach Report, "How Social Engineering Was Used to Gain Unauthorized Access," UK Government, 2019.
[16] J. M. Kowalski, "A Study on Tailgating Attacks in High-Security Environments," Journal of Physical Security, vol. 15, no. 3, pp. 215–228, 2022.
[17] Cyber Security & Infrastructure Security Agency (CISA), "2023 Social Engineering Attack Trends," USA Department of Homeland Security, 2023.
[18] Kollár, Csaba ; Zakar, Ákos: A social engineering és a manipulációs technikák és módszerek - kutatási jelentés. BIZTONSÁGTUDOMÁNYI SZEMLE 2 : 3 pp. 31-46. , 16 p. (2020)
[19] Kollár, Csaba: A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában. In: Rajnai, Zoltán (szerk.): Kiberbiztonság – Cybersecurity 2. Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 47-61. , 15 p.

DOI: https://doi.org/10.12700/btsz.2025.7.1.107

CYBER SECURITY CHALLENGES AND SOLUTIONS IN THE HUNGARIAN BANKING INDUSTRY DURING THE PANDEMIC BASED ON THE CHANGED REGULATIONS

KIBERBIZTONSÁGI KIHÍVÁSOK ÉS MEGOLDÁSOK A HAZAI PÉNZÜGYÁGAZAT JÁRVÁNYHELYZET ALATTI SZABÁLYOZÁSI KÖRNYEZETÉNEK VÁLTOZÁSA ALAPJÁN

SOMOGYI Tamás[1] – NAGY Rudolf[2]

Abstract

In the early 2020's crises occurred that we never saw before. The COVID-19 pandemic has changed our life, e.g., the way we enjoy the essential services of the banking industry. However, the level of cyber threat has also increased significantly. Banks and their customers experienced more cyber attacks than before. The aim of this paper is to explore the solution to this problem that was provided in 2020 or in 2021 by the new regulations of the banking industry. It will be demonstrated in this study that the window of opportunity was opened in these years: regulations has been introduced in order to make the information security more matured by defining minimum mandatory standards. However, the new regulations are mainly focusing on the banks and the security of their digitalised services. Cyber threat to customers are not covered properly by the regulations introduced in the examined period.

Keywords

cyber security, banking industry, coronavirus pandemic, Multiple Stream Approach

Absztrakt

A 2020-as évek elején rendkívüli kihívások jelentek meg. A koronavírus-járvány megváltoztatta mindennapi életünket, többek között a pénzügyágazat alapvető szolgáltatásainak igénybe vétele is túlnyomórészt digitálisan történt. Ezzel párhuzamosan drasztikusan emelkedett a kiberfenyegetettség. Megnövekedett kibertámadást tapasztalhattak meg a pénzintézetek és az ügyfelek. Kutatásunk célja megválaszolni a kérdést, hogy erre a problémára 2020-ban és 2021-ben milyen válasz született a hazai pénzügyágazat szabályozásában? Igazoljuk, hogy ebben az időszakban megnyílt a lehetőségek ablaka: megoldási javaslatok kerültek a szabályozó napirendjére, és megszülettek a vonatkozó szabályok, melyek célja az ágazat információbiztonságának fejlesztése, minimum követelmény meghatározása. A vizsgált időszakban született szabályok, mint megoldások, a pénzintézetek nyújtotta alapvető szolgáltatások digitalizációjára és a biztonságos működésre helyezik a hangsúlyt. Az ügyfeleket érő kibertámadásokkal nem foglalkoznak részletesen a szabályok.

Kulcsszavak

kiberbiztonság, pénzügyágazat, koronavírus-járvány, közpolitikai változások modell

[1] somogyi.tamas@phd.uni-obuda.hu | ORCID: 0000-0003-1397-697X | PhD student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] nagy.rudolf@bgk.uni-obuda.hu | ORCID: 0000-0001-5108-9728 | habil. senior lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary | habil. adjunktus, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az épített környezetünket, infrastruktúránkat, az alapvető szolgáltatásokat fenyegető tényezők kettő csoportba sorolhatóak: emberi és nem emberi [1]. Az első csoportban hangsúlyos a magán és állami infrastruktúrát egyaránt veszélyeztető terrorizmus elleni védekezés [2] és a kiberbűnözés [3]. A nem emberi tényezők között a szakirodalom leggyakrabban a természeti események fenyegetését említi [4], és ide tartoznak a járványok is. Környezetünkkel, földünk rendszereivel együtt élünk, ebben létezünk [5]. A természeti erők hatása alól nem vonhatjuk ki magunkat, azokkal számolni kell [6], különösen a létfontosságú rendszerelemek esetében, hiszen nemzetbiztonsági kérdés ezek zavartalan működtetése és a szolgáltatásaikhoz való hozzáférés [7]. Az ókori római költő, Ovidius korszakfelosztását felidézve Lentner mai világunkat az ezüstkorhoz hasonlítja: az aranykorral szemben itt van hőség és fagy, ugyanakkor az ember képes felülkerekedni a nehézségeken [8]. A kétségtelen, hogy a 2020-as évek elején olyan események és változások történtek, melyek hatására még több nehézséggel kellett megküzdeni. Különösen igaz volt ez az alapvető szolgáltatást biztosító létfontosságú rendszerelemek és ezek felhasználói esetében.

A 2020-as évek elején növekedtek a kiberbiztonsági kihívások. Ennek oka lehet egyfelől az internetes szolgáltatások és az okoseszközök terjedése [9], másfelől külső okként a támadások is szaporodnak. A külső támadások növekedéséhez a 2020-ban kitörő koronavírus-járvány is hozzájárult. Az Europol jelentése szerint Európában a kiberbűnözés megnövekedett a koronavírus-járvány idején [10]. Ezt a szektoroktól független jelenséget a pénzügyágazat is észlelte: kutatás igazolta (például [11]), valamint az Európai Központi Bank is a kiberbűnözés növekedő tendenciáját jelentette [12]. Másrészről a kibertér biztonságát a 2020-as évek első felében további események is befolyásolták: az Ukrajnában zajló háború és a közel-keleti konfliktus [13], [14], [15]. A NATO a kiberteret műveleti térnek tekinti [16], a NATO-val és szövetségeseivel szemben álló erők pedig bizonyítottan végre is hajtanak műveleteket a kibertérben [17], [18], [19], melyek a létfontosságú rendszerelemekben zavarokat okozhatnak. Sőt, ezen támadások kimondott célja lehet üzemzavar előidézése létfontosságú rendszerelemben [20]. Az információs hadviselésre és a kibertámadások elmúlt évekbeli növekvő tendenciájára több kutatás is felhívta a figyelmet [21], [22], [23], [24]. Az igaz, hogy a nemzeti kiberbiztonság fontossága már 2020 előtt is ismert volt [25], azonban a 2020-as évek elejének változásai alátámasztották ezen terület kritikusságát. A kiberbiztonság a 2020-as évek elejére stratégiai kérdésként jelent meg a vezető országokban [26], az alapszolgáltatások biztosításának kérdésköre pedig kutatási témává vált [27] és a felsőoktatási képzésben is hangsúlyos szerepet kapott [28]. Az információs infrastruktúra védelme EU szinten egységes jogszabályokban is megjelenik [29].

A digitalizáció és kiberbiztonság kérdésköre hangsúlyosan van jelen a pénzügyágazatban is. A pénzügyágazat alapvető szolgáltatásokat is nyújt, létfontosságú rendszerelemként azonosított [30], ráadásul esszenciális a nemzetgazdaság működése és fejlődése szempontjából [31]. Ennek a támadásoknak mindig is kitett ágazatnak a védelme kiemelten fontos, különösen, amikor a kibertámadások is sújtják [32], [33].

Az alapvető szolgáltatások biztosítása, a létfontosságú rendszerelemek üzemelése kiemelt fontosságú, ezért a kapcsolódó kiberbiztonsági kérdések kutatása rendkívüli jelentőségű. Ehhez a témához járulunk hozzá jelen cikkünkkel. Célunk egy létfontosságú rendszerelem, a pénzügyágazat példáján keresztül szemléltetni a koronavírus-járvány hatását a

kiberbiztonság területére, valamint feltárni, hogy a szabályozói környezet hogyan reagált ezen kihívásokra.

KUTATÁSI MÓDSZERTAN

Kutatási kérdésként tettük fel, hogy a hazánkban is megjelenő koronavírus-járvány milyen kihívásokkal szembesítette a pénzügyágazat alapvető szolgáltatásainak folyamatos biztosítását és azok igénybe vételét a kibertérben?, és ezen kihívásokra milyen válaszokat adott a szabályozói környezet? Kutatásunk során a szakirodalom mellett a járványhoz kapcsolódó ágazat-specifikus szabályozást tekintettük át, melyek érintik az elektronikus alapszolgáltatásokat és a kiberbiztonságot. A pénzügyágazat stabil működését felügyelő Magyar Nemzeti Bank (MNB) 2020-ban és 2021-ben kiadott különböző szintű vonatkozó témájú dokumentumait a www.mnb.hu honlapon kerestük. Az MNB szorosan együttműködik az európai uniós társszerveivel és az Európai Bankhatósággal (EBA) [34]. Igaz ez az alapszolgáltatásnak tartott pénzforgalom esetében is. Az EBA pénzforgalmi területtel foglalkozó bizottságának az MNB is tagja, az ott megfogalmazott európai uniós szintű iránymutatások a hazai ágazat szabályozásának részévé válnak. A szabályozás mellett a pénzforgalmi csalásokhoz kapcsolódó EU szintű tudásmegosztás is biztosított az EBA-n keresztül. Ezért kutatásunkhoz az MNB kibocsátotta dokumentumokat használtuk fel.

Kutatásunkhoz Kingdon közpolitikai változásokról szóló modelljét (angol eredetiben: Multiple Stream Approach, a továbbiakban: MSA) választottuk, mely a folyamati szabályozásokhoz kapcsolódó kutatások során alkalmazható. Ezen modell szerint a közpolitikai változás úgy írható le, mint három folyamat vagy áramlat találkozása [35]. Az első áramlat a *probléma* (problem) melyben megfogalmazódik egy megoldandó probléma. A *közpolitika* (policy) áramlat azon megoldást, szabályozást jelképezi, mely a szakértők válasza, megoldási javaslata a felmerült problémára. A *politika* (politics) áramlat foglalja magába a jogszabályalkotót, felügyeleti szervet, vonatkozó hatóságot. Ahogyan Demszky megfogalmazza [36], egy kritikus ponton jelenik meg a *lehetőségek ablaka*, mely során a három áramlat találkozik. Ekkor a probléma és a megoldási lehetőség a politikai szereplők napirendjére kerül, és elindul a cselekvés, megtörténik a szükséges - szabályozási - változás.

Feltételezésünk szerint a koronavírus-járvány olyan kritikus pont volt, mely során megjelent a lehetőségek ablaka. Következésképpen, ebben az időszakban olyan szabályoknak (megoldásoknak) kellett születniük, melyek választ adtak a járvány előidézte vagy felerősítette kihívásokra (problémára).

A 2020-BAN KITÖRŐ KORONAVÍRUS-JÁRVÁNY HATÁSA A PÉNZÜGYÁGAZAT ALAPVETŐ ELEKTRONIKUS SZOLGÁLTATÁSAINAK KIBERBIZTONSÁGÁRA

Járványok időről időre megjelennek és befolyásolják mindennapi életünket [37]. Járványok idején speciális folyamatok, eljárásrendek lépnek életbe (például karantén és távmunka [38]), mely hatására megváltoznak a szolgáltatások igénybe vételével kapcsolatos szokások (például megugrik a távoli üzletkötések száma). Ráadásul a járványos megbetegedések veszélyt jelentenek a munkavállalók rendelkezésre állására [39]. A járványok terjedésének megelőzése érdekében bevezetett eljárások pedig kihívás elé állítják a gazdaságot és kormányzati szerveket [40]. Egy ilyen helyzetben a gazdasági fejlődés megtorpan vagy

csökken, ráadásul a gazdaság visszafejlődése évekig elhúzódó folyamat is lehet [41]. Ahogyan Vida rámutatott, egy járvány a nemzetek gazdasági-, társadalmi- és politikai biztonságát fenyegeti [42]. Ráadásul, egy kutatás szerint a komoly hatású járványok előfordulási valószínűsége nagyobb, mint azt sokan gondolnák [43]. Mindezek megerősítik, hogy hazánk Nemzeti Biztonsági Stratégiája kockázatként azonosította a járványos megbetegedéseket [44], hiszen azok az előbbi módokon hatással bírnak a szolgáltatásokat nyújtó infrastruktúra üzemeltetésére. Erre példával szolgált a 2020-as évek legelején tomboló koronavírus-járvány.

A koronavírus-járvány következményeit az életünk szinte minden területén érezhettük. Természetszerűleg hatott az egészségügy és munkabiztonság területére [45], de például átalakította a közlekedési szokásokat és szabályokat [46] és újszerű megoldásokat kényszerített a közigazgatásra [47]. Az oktatásban ösztönözte a távoktatáshoz kapcsolódó megoldások széles körű elterjedését [48], [49]. Mindezek mellett a koronavírus-járvány kétség kívül hatással volt a pénzügyágazat szolgáltatásaira is, különösen az alapvető szolgáltatásnak tekinthető elektronikus fizetési megoldásokra.

A Magyar Nemzeti Bank (MNB) az ágazatra vonatkozó adatok alapján úgy látja, hogy a digitális banki csatornák meghatározóvá váltak a koronavírus-járvány alatt [50]. Egyértelmű, hogy a korábban a bankfiókokat preferáló ügyfelek nagy számban tértek át az elektronikus bankolásra. Az pénzintézetek IT területeit is felügyelő MNB meglátása szerint a hirtelen megugró elektronikus bankolási igényeket a pénzintézetek infrastruktúrája zökkenőmentesen tudta kielégíteni. A stabil működés pozitív élménye is hozzájárulhatott a digitális megoldások szélesebb körű elterjedéséhez. Mindez pedig további digitalizációra ösztönözte a pénzintézeteket. A hazai pénzügyágazat szereplői 60 százalékánál erősítette meg és gyorsította fel a digitalizációt a járványhelyzet, vagyis a szektorban a többség hosszabb távon is középpontba helyezi a digitális átállást és az elektronikus megoldásokat. A járvány utáni számadatok tükrében az MNB úgy látja, hogy hazánkban az ügyfeleknek már csak kisebb része intézi ügyeit bankfiókban. Meg kell említeni, hogy a járványtól független, de időben azzal egybe eső lényeges változás történt az átutalási rendszerben 2020. márciusában. Ekkor került bevezetésre hazánkban az Azonnali Fizetési Rendszer, melyre a bevezetésétől kezdve a hazai Forintalapú fizetési forgalom 40%-a terelődött át [50]. Ráadásul az ügyfeleknek a hazai pénzügyágazatba vetett bizalma a koronavírus-járvány alatt is megmaradt, beleértve a bankok innovációs, környezetvédelmi és digitális újításait is [51]. Bizonyosnak tekinthető, hogy mindez hozzájárult az ügyfelek oldalán az elektronikus bankolás nagyobb mértékű használatához.

A járvány időszakában a szektor munkavállalói oldalán is teret hódított a digitalizáció: a távmunka a pénzügyágazatban is elterjedt, a pénzintézetek pedig ehhez igazítják eszközbeszerzési terveiket. A folyamatokban is változások történtek: a belső információáramlás, a jóváhagyás és aláírás is elektronikus módon valósult meg, és ez a pénzintézetek többségnek tervei szerint hosszabb távon is így marad [50].

A digitalizáció terjedésének az árnyoldalának tekinthető, hogy a digitális térben megnövekedett jelenléttel párhuzamosan a kiberbűnözés növekedése is látható volt [52]. Az MNB Kiberfenyegetettségi térképe szerint a 2020-ban pénzügyágazatban felgyorsuló digitalizációs folyamatok általánossá tették a kiberbiztonsági fenyegetést is [53]. Az MNB összegzése szerint 2020. áprilisa és 2021. júliusa között megnövekedett a hazai pénzügyágazatot érintő kiberbiztonsági fenyegetések és támadások száma. A nemzeti bank ebbe a körbe

sorolja a megtévesztésen alapuló támadást, az ügyfelek adataival szembeni fenyegetéseket, valamint az alapvető szolgáltatások rendelkezésre állása elleni fenyegetéseket, mint például a DDoS támadást [53]. Ahogyan az MNB hangsúlyozza, a támadók egyre szofisztikáltabb megoldásokat alkalmaznak. A sikeres támadások után anyagi erőforrás áll a támadók rendelkezésére, amit felhasználhatnak még komolyabb támadásokhoz. Ezáltal a csalási kísérletek, támadási szcenáriók bonyolultabbá és hitelesebbé válnak az ügyfelek számára, így a sikeres támadások száma tovább növekedhet.

Az MNB a pénzügyágazat szereplőinek jelzésén túl ügyfélpanaszokból is képet kap a trendekről. Az ügyfélszolgálatán megtett, kibervisszaélés témájú ügyfélbejelentések száma megugrott a koronavírus-járvány időszakában. A Kiberfenyegetettségi térképben közzétett adatok szerint 2019. negyedik negyedévében 4 ügyfélbejelentés történt, míg 2020. második negyedévétől kezdve negyedévenként 10 feletti, 2021-ben negyedévenként már 20 feletti volt az ügyfélpanasz [53]. Az MNB 2020. év adatait feldolgozó éves jelentése szerint az érzékeny fizetési adatok (jelszó, egyszer használatos kód) megszerzése támadási módszer a koronavírus-járvány időszakában továbbra is kiemelkedő volt [53]. Ugyanakkor újdonságként jelent meg 2020. tavaszán azon megtévesztéses csalástípus, mely során az ügyfeleket rábírták átutalásra olyan egészségügyi eszközök megvásárlásának ígéretével, melyek kereskedelmi forgalomban akkor hiánycikknek számítottak.

Elmondható tehát, hogy a koronavírus-járványra válaszul bevezetett intézkedések hatására elterjedtebbé váltak a digitális szolgáltatások, megnövekedett a kibertér használata. Igaz ez a pénzügyágazat nyújtotta alapvető szolgáltatásokra is. Ezzel párhuzamosan megnövekedett a kiberbiztonsági fenyegetések és támadások száma, illetve fejlődtek a támadók alkalmazta módszerek. Kingdon közpolitikai változásokról szóló modelljének kifejezéseivel élve, megjelent vagy hangsúlyosabbá vált a probléma, a pénzügyágazat alapvető szolgáltatásainak kiberbiztonsága. Felmerül a kérdés, hogy ebben az időszakban eljött-e a kritikus pont, amikor megjelenik a lehetőségek ablaka? Más szóval, a szakértők megoldási javaslata (közpolitika) a politika napirendjére kerül-e, és elindul-e a cselekvés a probléma megoldására? A hazai pénzügyágazat szabályozói környezetének a kiberbiztonság fokozása érdekében történő változását a következő rész vizsgálja.

ÚJ KÖVETELMÉNYEK A HAZAI PÉNZÜGYÁGAZAT SZABÁLYOZÓI KÖRNYEZETÉBEN

A 2020-ban megjelenő koronavírus-járvány a megszokott életünkben hirtelen jött változásokat idézett elő, melyek között szerepel az elektronikus fizetési megoldások szélesebb körű használata. Ahogyan arra fentebb rámutattunk, a kiberbiztonság jelentősége is megnövekedett. Felmerül a kérdés, hogy mindez a hazai pénzügyágazatban indukált-e változást, fejlődést 2020-ban és 2021-ben?

Az MNB 2020-ban és 2021-ben több, a biztonság témájával foglalkozó ajánlást tett közzé. Első helyen említendő *Az informatikai rendszer védelméről* szóló 8/2020. (VI. 22.) MNB ajánlás és *A pénzügyi szervezetek működésének fizikai biztonsági és humánkockázatkezelési feltételeiről* szóló 11/2020. (X.20.) MNB ajánlás. Ahogyan a 11/2020 sz. ajánlás *I. Az ajánlás célja és hatálya* c. részben írja, az MNB ebben a kettő ajánlásában „*összefoglalja azokat az eljárásokat, amelyeket a pénzügyi szervezeteknek a biztonságos működésük érdekében alkalmazni célszerű*“. Ez a kettő ajánlás együtt fedi le a fizikai és a logikai biztonsági követelményeket, beleértve a kiberbiztonság területét is. Az informatikai védelemről szóló

ajánlás részletesen leírja az informatikai biztonsági elvárásokat a tervezéstől és szabályozástól a kockázatelemzésen, fejlesztésen, beszerzésen, tesztelésen át az üzemeltetésig, külön kitérve a szolgáltatás-folytonosságra és a független ellenőrzésre. Érdemes itt megemlíteni, hogy a 16.3.4. pontban elvárja az MNB az ügyfél adatainak és vagyonának védelme érdekében, hogy a pénzintézet a visszaélések észlelésére és megelőzésére csalásfelderítő rendszert működtessen.

Fentiek mellett az MNB kiadta *A távmunka és távoli hozzáférés informatikai biztonsági követelményeiről* szóló 12/2020. (XI.6.) számú ajánlását is, melynek *I. Az ajánlás célja és hatálya* című része szerint a pénzügyágazatban a távmunkát „*a kényelmen túl más gazdasági és társadalmi szempontok is kikényszerítették, a pandémiás helyzet okozta kijárási korlátozások miatt olyan intézményeknél is megjelent a távmunka tömeges igénye, ahol korábban nem, vagy csak korlátozott keretek közt éltek a munkavégzés ilyen formájával.*“ A távmunka széles körű megjelenését tapasztalva, az ajánlás célja, hogy a pénzügyágazat intézményei kezeljék a távmunkához köthető kiberbiztonsági kockázatokat, beleértve az adatvédelmi kérdéseket is. Ez utóbbi érdekében a 8. a) pont előírja, hogy „*a távoli hozzáférés minden esetben titkosított csatornán keresztül történjen*“. Lényeges továbbá a 8. i) pontja, mely elvárja a távoli felhasználó és eszköze (mely kizárólag az intézmény által menedzselt eszköz lehet) hitelesítéséhez a többfaktoros autentikációt. A kiberbiztonsági kockázatok kötelező elemzése után azokat megfelelően kezelni kell adminisztratív szabályozással; az intézmény kezelte eszközök konfigurálhatóságának korlátozásával; a nem az intézmény felügyelte eszközök kitiltásával; hálózatvédelmi megoldásokkal; a napi üzemeltetési feladatok folyamatos ellátásával; a távoli hozzáférés és tevékenység folyamatos figyelésével.

A koronavírus-járvány alatti átmeneti védekezési intézkedések korlátai is hozzájárultak a digitális szolgáltatások szélesebb körben történő igénybe vételéhez. Ahogyan fentebb rámutattunk, ez is ösztönözte a digitális átalakulást. Az MNB ebben a témakörben is kibocsátott ajánlást. *A hitelintézetek digitális transzformációjáról* szóló 4/2021 (III.30.) MNB ajánlás célja a pénzügyágazat digitális átalakulásának biztonságos keretek között történő elősegítése. Ezen ajánlás 2. pontjában megfogalmazottak szerint az MNB elvárja egy digitális transzformációs stratégia kialakítását célkitűzésekkel és azok megvalósulásának nyomon követésével. A 3. a) és b) pontok szerint ezen stratégia célkitűzései között szerepelnie kell a digitálisan elérhető termékek és szolgáltatások körének bővítésének, valamint a különböző digitális csatornák használatának ösztönzésének. Az MNB ajánlása ugyanakkor a biztonságra is kitér, amikor a 3. j) pontban elvárja az informatikai biztonság fejlesztését is. Az 5. pont pedig megfogalmazza azt az elvárást, hogy a digitális transzformációs stratégia és az IT stratégia legyen egymással összhangban. Ezen felül lényeges az ajánlás 13.3. pontja: „*az MNB a csalás elleni kockázatok feltérképezése, kiértékelése és kezelése kapcsán – a vonatkozó jogszabályi megfelelés mellett – elvárja, hogy a hitelintézet a digitalizáció növekedése kapcsán esetlegesen újonnan megjelenő csalási eseteket is beépíti a kockázatkezelési módszereibe*“. A 15. pont külön kiemeli az informatikai biztonsági fejlesztések esetében a fentebb említett 8/2020. (VI. 22.) MNB ajánlást. A digitalizáció részeként a távoli ügyintézés ösztönzése és terjedése kapcsán érdemes még megemlíteni, hogy 2020. októberében az MNB közzétett egy állásfoglalást is az elektronikus csatornákon keresztül előterjesztett panaszok kezelésének módjára vonatkozóan [54].

2020-ban és 2021-ben a hazai pénzügyágazatban megjelenő, IT biztonsági témájú új elvárások és ajánlások bemutatása után a következőkben kerül sor következtetések levonására.

KÖVETKEZTETÉSEK

Fentiekben bemutattuk, hogy a hazánkban 2020-ban kitört koronavírus-járvány felgyorsította a pénzügyágazat digitalizációját és növelte az elektronikus banki szolgáltatások igénybe vételét. A járvány időszakában, illetve a digitalizációval összhangban az ügyfelek bankfiók felkeresése nélkül, távolról intéztek banki ügyeket a korábbinál nagyobb mértékben. Ugyanakkor, ezzel párhuzamosan a kibertámadások és visszaélések száma is megnőtt. A pénzügyágazat tapasztalata szerint az alapvető szolgáltatások rendelkezésre állása elleni támadások gyakoribbá váltak. Továbbá az ügyfelek elleni támadások is megnövekedtek, melyek célja adatok vagy pénz megszerzése. Ebben a körben új csalástípus is megjelent a járvány időszakában.

Az alkalmazott MSA modell terminológiáját használva, megjelent egy probléma: az elektronikus banki szolgáltatások biztonságát veszélyeztető tényezők jelentőssé váltak. Talán legfontosabb következtetésünk, hogy a problémára válaszul az információbiztonság szintjének emelését célzó előírások és a szektorban alkalmazandó megoldások megjelentek az ágazat-specifikus szabályzatokban. Igazoltuk tehát, hogy a koronavírus-járvány alatt tapasztalt kiberbiztonsági kihívások megjelenése kritikus pont volt, 2020-ban és 2021-ben megnyílt a lehetőségek ablaka, a szabályozó cselekedett. Az MNB ajánlásokat bocsátott ki az informatikai és a fizikai biztonság területén, az ágazatban a távmunka terén, valamint a digitalizáció kérdéskörében, továbbá, vonatkozó állásfoglalást is közzé tett.

Látható, hogy a vizsgált időszakban megnyílt a lehetőségek ablaka, de ebből nem következik az, hogy előtte ne cselekedett volna a szabályozó. Az informatikai rendszerek védelme terén korábban is létezett ágazatspecifikus ajánlás, mivel a fentebb említett 8/2020-as MNB rendelet lecserélte a korábbi 7/2017. (VII. 5.) számú ajánlást. Ugyanakkor a távmunka tárgykörében nem létezett korábban ajánlás, tehát ebben az esetben a vizsgált időszakban nyílt meg először a lehetőségek ablaka. A WHO vissza-visszatérően aktualizált, 2009-es kiadású járványügyi ajánlása felhívta a nem egészségügyi szektor szereplőinek figyelmét járványhelyzeti terv készítésére, benne az erőforrások átcsoportosítására az alapvető szolgáltatások biztosítása érdekében [55]. Ebben a témában mégsem nyert teret a kérdés ezen aspektusa a kockázatkezelésben korábban.

Részleteiben megnézve a szabályozói választ (politika), látható, hogy az MNB ajánlásai hangsúlyt fektetnek a pénzintézetek fizikai- és informatikai biztonságára. A kiberbiztonság terén megfogalmazott elvárások, mint minimum követelményszint, komplex választ adnak a külső támadásokra vonatkozóan. Lefedik az informatikai biztonság minden területét a bankok oldalán. Ehhez kapcsolódik a járvány hatására a pénzügyágazatban széles körben elterjedt távmunka informatikai biztonságának követelményeiről szóló ajánlás is, mely az alkalmazottak biztonságos munkavégzésének követelményeit adja meg. Az ágazatban tapasztalható, a járvány is ösztönözte digitális transzformációra válaszul megjelent ajánlás pedig a digitalizáció további terjedését célozza, előírva a biztonsági követelményeket, az IT stratégiához és információbiztonsági ajánláshoz kapcsolódva. Mindezzel az MNB, mint szabályozó, komplex választ ad az ágazat alapvető szolgáltatásait fenyegető kiberbiztonsági problémára.

Ugyanakkor a kutatásunk során fellelt MNB ajánlásokban kevés szó esik a kiberbiztonsági probléma másik részéről, az ügyfeleket fenyegető támadásokról. A koronavírus-járvány időszakában megnövekedett csalásra az MNB külön ajánlást nem fogalmazott meg, a csalásmegelőzés banki oldali részével csak kismértékben foglalkozott ajánlásaiban. Erre magyarázatot nem találtunk. Lehetséges, hogy ennek oka a közpolitikai áramlatban keresendő, vagyis az ügyfeleket érő támadásokra megfelelő megoldási javaslat nem született a vizsgált időszakban, hiszen új csalástípus is megjelent. Esetleg a politikai áramlat nem volt megfelelő, vagyis a szabályozói oldalon nem kezelték kellő hangsúllyal a problémát, és nem fogalmaztak meg megfelelő szabályozói elvárást. Mindenesetre látható, hogy a vizsgált időszakban erre a részproblémára vonatkozóan nem nyílt meg a lehetőségek ablaka, vagy csak részlegesen, elsősorban más témájú ajánlásokban. Ez a jelenség további kutatások témája lehet.

ÖSSZEFOGLALÁS

A 2020-as évek első éveiben rendkívüli kihívásokkal szembesültünk, köztük a koronavírus-járvánnyal. Ahogyan bemutattuk, a járvány időszakában a pénzügyágazat alapvető szolgáltatásai közül az elektronikus szolgáltatások igénybe vétele hirtelen megnövekedett. Ezzel párhuzamosan azonban drasztikusan emelkedett a kiberfenyegetettség is, mind a pénzintézetekkel szemben, mind pedig az ügyfelekkel szemben. Kutatási kérdésként tettük fel, hogy a hazánkban is megjelenő koronavírus-járvány milyen kihívásokkal szembesítette a pénzügyágazat alapvető szolgáltatásainak folyamatos biztosítását és azok igénybe vételét a kibertérben?, és ezen kihívásokra milyen válaszokat adott a szabályozói környezet?

Kutatásunkhoz a közpolitikai változások modellt (Multiple Stream Approach) választottuk. A hazai pénzügyágazatban 2020-ban és 2021-ben megjelenő szabályozást áttekintve igazoltuk, hogy ebben az időszakban megnyílt a lehetőségek ablaka. A kiberfenyegetettség problémájára megoldási javaslatok kerültek a szabályozó napirendjére, és megszülettek a vonatkozó szabályok, melyek célja az ágazat információbiztonságának fejlesztése, minimum követelmény meghatározása. Az igaz, hogy az informatikai rendszerek védelmének területén korábban is jelent meg MNB ajánlás (korábban is megnyílt a lehetőségek ablaka). Ugyanakkor a távmunka terén a vizsgált időszakban nyílt meg először a lehetőségek ablaka, a WHO korábbi ajánlása ellenére ez a terület kevés figyelmet kapott.

Rámutattunk továbbá, hogy a vizsgált időszakban megszületett szabályok, mint megoldások a pénzintézetek nyújtotta alapvető szolgáltatások digitalizációjának jelenségére és a biztonságos működésre helyezik a hangsúlyt. Az ügyfeleket érő kibertámadásokra válaszul külön szabályozás nem jelent meg a vizsgált időszakban, ezt a kérdést részletesen nem tárgyalják a megjelent szabályok.

FELHASZNÁLT IRODALOM

[1] Faramondi, L., Oliva, G. and Setola, R. "Multi-criteria node criticality assessment framework for critical infrastructure networks." *International Journal of Critical Infrastructure Protection*, 28, 2020, https://doi.org/10.1016/j.ijcip.2020.100338

[2] Besenyő J., Sinkó G. „Terrorist Organizations' Activities Against Crucial Installations: Al-Shabaab's Attacks on Critical Infrastructure in Kenya", In: Besenyő, János;

Khanyile, Moses B.; Vogel, David (szerk.) *Terrorism and Counter-Terrorism in Modern Sub-Saharan Africa*, Cham, Svájc : Springer Nature Switzerland (2024) pp. 169-193. https://doi.org/10.1007/978-3-031-56673-8_8

[3] Márton Z., Rajnai Z. „A social engineering fejlődése és jövője: a pszichológiai sebezhetőségek kihasználása a digitális korban”, *Biztonságtudományi Szemle*, 6(4), 2024. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/525

[4] Teknős L. „Természeti katasztrófák tendenciális változásainak elemzése, értékelése”, *Belügyi Szemle*, 72(2), 2024. https://doi.org/10.38146/BSZ.2024.2.5

[5] Bándi Gy. „A teremtésvédelem egyetemessége“ In: Komáromi L., Szabó P., Birher N., Cserey Gy., Puskás A. (szerk.) *Munus et dilectio*. Pázmány Press, Budapest, pp. 75-83. (2024) ISBN 9789633085028

[6] Földi L., Halász L. „Investigation of Climate Vulnerability of Domestic Natural and Artificial Ecosystems”, *Hadmérnök*, 14(2), 2019. https://doi.org/10.32567/hm.2019.2.14

[7] Demény, Á., Tollár, T., Endrődi, I. „Biztonsági, nemzetbiztonsági kihívások hatásai a Magyarországi nemzetgazdaságra”, *Polgári Védelmi Szemle*, XVI, 2024. https://mpvsz.hu/pvszemle/

[8] Lentner Cs. „Ezüstkor”, *Polgári Szemle*, 19(1–3), 2023. https://doi.org/10.24307/psz.2023.0901

[9] Mandic, D., Kiss, G., Rajnai, Z. „Password Usage among Users of Smart Devices in Hungary and Serbia”, *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania, 2024. https://doi.org/10.1109/SACI60582.2024.10619863

[10] Europol. „COVID-19 sparks upward trend in cybercrime” Press release 5 October 2020. https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

[11] Gulyás O., Kiss G. „Kiberbiztonság 2021-ben a bankszektorban és a pénzügyi szervezeteknél”, *Biztonságtudományi Szemle*, 4(1), 2022. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/205/181

[12] European Central Bank. „Supervision newsletter, IT and cyber risk: a constant challenge”, 18 August 2021, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2021/html/ssm.nl210818_3.en.html

[13] Brožič L. „Modern Warfare”, *Contemporary Military Challenges*, 26(3), 2024. https://doi.org/10.2478/cmc-2024-0017

[14] Pavel Tal „Avoiding a ‘Digital 7 October’: a study on cyberwarfare against Israel during the October 2023 war”, *Contemporary Military Challenges*, 26(3), 2024. https://doi.org/10.2478/cmc-2024-0022

[15] Horváth D. „The background of the Russian-Ukrainian war in terms of new methods and warfare”, *National Security Review*, 2024/1, https://www.knbsz.gov.hu/hu/letoltes/szsz/2024_1_NSR.pdf

[16] Reveron, D.S., Savage, J.E. „Cybersecurity Convergence: Digital Human and National Security”, *Orbis*, 64(4), 2020. https://doi.org/10.1016/j.orbis.2020.08.005

[17] Lendvai T. „A Kínai Népköztársaság feltételezett kiberhírszerzési műveleteinek értékelése: eljárások és a nemzetközi hatások áttekintése”, *Nemzetbiztonsági Szemle*, 12(2), 2024. https://doi.org/10.32561/nsz.2024.2.4

[18] Strucl, D. „Russian aggression on Ukraine: cyber operations and the influence of cyber space on modern warfare”, *Contemporary Military Challenges*, 24(2), 2022. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6
[19] Besenyő J. „Újfajta háború? Internetes hadviselés Grúziában”, *Sereg Szemle*, 6(3), 2008.
[20] Kovács L. „Nyomásgyakorlás a kritikus információs infrastruktúrák támadásán keresztül: A Digital Pearl Harbortól a digitális ökoszisztéma teljes támadásáig”, In: Krasznay Csaba (szerk.) *Taktikák és stratégiák a kiberhadviselésben*, Budapest, Magyarország : Ludovika Egyetemi Kiadó (2023) 304 p. pp. 151-168.
[21] Dér A., Busa A. „Kritikus információs infrastruktúra rendszerei ellen intézett támadási trendek”, *Biztonságtudományi Szemle*, 6(1), 2024. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/434
[22] Pál A.B. „Információs műveletek és információs hadviselés”, *Biztonságtudományi Szemle*, 5(1), 2023. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/308
[23] Jagodics I., Kollár Cs. „21. századi social engineering támadások, védekezés és szervezeti hatások Európában”, *Belügyi Szemle*, 71(1), 2023. https://doi.org/10.38146/BSZ.2023.1.6
[24] Beregi A.L., Babos T. „Security and Military Relevancies of Digitisation, Globalisation and Cyberspace”, *Academic and Applied Research in Military and public management Science*, 20(1), 2021. https://doi.org/10.32565/aarms.2021.1.6
[25] Kovács L. „National cyber security as the cornerstone of national security”, *Revista Academiei Fortelor Terestre*, 23(2), 2018. https://doi.org/10.2478/raft-2018-0013
[26] Csiki Varga T., Tálas P. „Erő és diplomácia – Az Egyesült Államok stratégiai érdekei és lehetőségei a Biden-kormányzat időszakában”, *Nemzet és Biztonság*, 2022/1, 2022. https://doi.org/10.32576/nb.2022.1.2
[27] Vass Gy., Ambrusz J., Restás Á., Varga F., Kátai-Urbán L. „A katasztrófavédelmi kutatások eredményei és fejlesztése a rendészettudomány rendszerében”, *Belügyi Szemle*, 72(5), 2024. https://doi.org/10.38146/BSZ-AJIA.2024.v72.i5.pp815-833
[28] Bakos T., Pető R. „A biztonságtechnikai mérnöki képzés múltja és jövője”, *Műszaki Katonai Közlöny*, 34. évf. különszám, 2024. https://doi.org/10.32562/mkk.2024.ksz.15
[29] Bederna Zs., Rajnai Z. „Review of the advacement of critical information infrastructures and their structural analysis”, *National Security Review*, 2020/2, 2020. https://www.knbsz.gov.hu/hu/letoltes/szsz/2020_2_NSR.pdf
[30] Bakos T. „A létfontosságú rendszerek azonosításáról, kijelöléséről és védelméről szóló hatályos magyar jogi dokumentumok”, *Műszaki Katonai Közlöny*, 34. évf., különszám, 2024. https://doi.org/10.32562/mkk.2024.ksz.17
[31] Kenesey Zs., Pataki L., Tóth R. „A banki szabályozói követelmények szigorításának hatása az Európai Unió bankszektorának jövedelmezőségére és a nemteljesítő hitelek arányára”, *Polgári Szemle*, 17(1–3), 2021. https://doi.org/10.24307/psz.2021.0710
[32] Gulyás O., Kiss G. „Cybersecurity threats in the banking sector”, *2022 8th International Conference on Control, Decision and Information Technologies (CoDIT)*, Istanbul, Turkey, 2022. https://doi.org/10.1109/CoDIT55151.2022.9804140
[33] Ubaldo, A.L.V., Barreto, V.Y.G., Albines, J.A.B., Andrade-Arenas, L., Bellido-García, R.S. „Information Security in the Banking Sector: A Systematic Literature Review

on Current Trends, Issues, and Challenges", *International Journal of Safety and Security Engineering*, 13(1), 2023. https://doi.org/10.18280/ijsse.130111
[34] MNB. „Fizetési Rendszer Jelentés 2021". 2021. ISSN 2498-7077 https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2021.pdf
[35] Kern, F., Rogge, K.S. „Harnessing theories of the policy provess for analysing the politics of sustainability transactions: a critical survey", *Environmental Innovation and Societal Transitions*, 27, 2018. https://doi.org/10.1016/j.eist.2017.11.001
[36] Demszky A. „A tapasztalat alapú tudás szerepe a politikai döntéshozatalban" In: Erőss, Gábor és Berényi, Eszter és Neumann, Eszter, (szerk.) *Tudás és politika: A közpolitikaalkotás gyakorlatának nyomában*, L'Harmattan, Budapest, 2013, ISBN 978 963 963 236 651 7
[37] Nagy R., Boda P. „Security policy and social challenges of epidemics in our days", *Polgári Védelmi Szemle*, XIV., 2022. https://mpvsz.hu/pvszemle/
[38] Petri B. „Az Európai Parlament működése a koronavírus-járvány idején: valódi megoldás-e a távmegoldás?", *Európai Tükör*, 23(3), 2020. https://doi.org/10.32559/et.2020.3.4
[39] Zellei G. „Veszélyes üzemek humán kockázatai: összefüggések, hazai helyzet, és a közeljövő feladatai", *Polgári Védelmi Szemle*, XIII., 2020. https://mpvsz.hu/pvszemle/
[40] Domokos L. „A koronavírus-járvány közpénzügyi kihívásai és a számvevőszéki válaszok", *Polgári Szemle,* 17(4-6), 2021. https://doi.org/10.24307/psz.2021.1204
[41] Posgay I., Regős G., Horváth D., Molnár D. „A koronavírus-járvány gazdasági hatásairól", *Polgári Szemle*, 16(4–6), 2020. https://doi.org/10.24307/psz.2020.1004
[42] Vida Cs. „A koronavírus-járvány hatása a biztonságra - paradigmaváltás a biztonsági rendszerben", *Felderítő Szemle*, 19(1), 2020. https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-1.pdf
[43] Sabelli, C. „Le epidemie estreme sono più probabili di quanto si pensasse", *Nature Italy*, 2021, https://doi.org/10.1038/d43978-021-00106-6
[44] Horváth Z., Tóth R. „A stratégiai szabályozás elméleti és gyakorlati kérdései a hivatásos katasztrófavédelemnél", *Katonai Logisztika*, 31(3-4), 2023. https://doi.org/10.30583/2023-3-4-185
[45] Simon M. „A COVID-19 munkabiztonsága", *Biztonságtudományi Szemle*, 4(2), 2022. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/227/197
[46] Shatnawi, M., Rajnai, Z. "Assessment of the impact of the covid-19 crisis on transportation and mobility – analysis of applied restrictions", *Interdisciplinary Description of Complex Systems*, 21(4), 2023. https://doi.org/10.7906/indecs.21.4.6
[47] Jónás K. „A koronavírus-járvány hatása a magyar közigazgatásra, különös tekintettel a pártfogó felügyelői eljárásokra", *Belügyi Szemle*, 72(4), 2024. https://doi.org/10.38146/bsz-ajia.2024.v72.i4.pp611-628
[48] Altaleb, H., Shatnawi, M., Rajnai, Z. „Digital Education: Governments' Strategies, Teaching Tools in the European Union and a Case Study of Digital Transformation in Budapest", *Interdisciplinary Description of Complex Systems*, 21(2), 2023. https://doi.org/10.7906/indecs.21.2.3
[49] Kádár Z., Rácz A. „A Covid19-járvány hatásai a társadalmi jóllét tekintetében - avagy miként adaptálódtak a járvány szülte új kívánalmakhoz a szegedi egyetemisták 2020

tavaszán", In: Szécsi Gábor, Tóth I. János (szerk.) *Társadalom a világjárvány hálójában : Alkalmazott filozófiai tanulmányok a pandémia társadalmi és kulturális hatásairól*. Budapest, Magyarország: Gondolat Kiadó (2023) 227 p. pp. 189-202.

[50] MNB. „Fintech és digitalizációs jelentés", 2021. ISSN 2732-3137 https://www.mnb.hu/letoltes/fintech-e-s-digitaliza-cio-s-jelente-s-2021.pdf

[51] Boros A., Lentner Cs., Nagy V., Tőzsér D. „Perspectives by green financial instruments – a case study in the Hungarian banking sector during COVID-19", *Banks and Bank systems*, 18(1), 2023. https://doi.org/10.21511/bbs.18%281%29.2023.10

[52] Katona G. „A Covid-19 kiberbiztonsági kihívásai az első hullám idején", *Hadmérnök*, 16(3), 2021. https://doi.org/10.32567/hm.2021.3.12

[53] MNB. „A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022", 2022. ISSN 2939-7383 https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf

[54] MNB. „Állásfoglalás az elektronikus csatornákon keresztül előterjesztett panaszok minősítéséről", 2020. https://alk.mnb.hu/data/cms2483747/tmpCB06.tmp(25189558).pdf

[55] WHO. „Pandemic Influenza Preparedness And Response", 2009. ISBN 9789241547680, https://www.who.int/publications/i/item/9789241547680

DOI: https://doi.org/10.12700/btsz.2025.7.1.119

STUDY OF SOME FIRE SAFETY ISSUES OF NUCLEAR POWER PLANS

ATOMERŐMŰVEK EGYES TŰZBIZTONSÁGI KÉRDÉSEINEK VIZSGÁLATA

KURMAY Sándor[1] – NAGY Rudolf[2]

Abstract

The use of nuclear energy for civilian purposes has developed over the past nearly 70 years as a result of the increased consuming of electricity used by industry and the population. The first reactors grew out of their initial imperfections and went through a generational change, there are several types that developed from the previous ones and still in use today. Malfunctions and accidents that had occurred during their operation taught the decision-makers to carefully plan the design, construction, operation, and decommissioning phases. Based on these experiences, the legal background governing the use of nuclear energy has also changed from country to country. In present article, we do our research on examination of the fire safety requirements of nuclear power plants, taking into consideration its evolutional process.

Keywords

nuclear power plant, nuclear energy, fire safety, nuclear safety

Absztrakt

Az atomenergia polgári célú felhasználása az elmúlt mintegy 70 évben az ipar és a lakosság által felhasznált villamosenergia szükségleteinek növekedése következtében fejlődött. Az első reaktorok gyermekbetegségükből kinőve generációváltáson mentek keresztül és több, napjainkban is működő típusuk fejlődött ki belőlük. A működésük során fellépő üzemzavarok és balesetek megtanították a döntéshozókat a tervezési, kivitelezési, üzemeltetési és leszerelési fázisok alapos megtervezésére. Ezen tapasztalatok mentén az atomenergia felhasználását szabályzó törvényi háttér is változott országonként. Ezen cikkünkben az atomerőművek tűzbiztonsági követelményeinek a vizsgálatával foglalkozunk betekintve annak evolúciójába.

Kulcsszavak

atomerőmű, atomenergia, tűzbiztonság, nukleáris biztonság,

[1] kurmay.sandor@uni-obuda.hu | ORCID: 0009-0004-9939-9353 | PhD student, Óbuda University Doctoral School of Safety and Security Sciences, Budapest, Hungary | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] nagy.rudolf@uni-obuda.hu | ORCID: 0000-0001-5108-9728| habil. senior lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary| habil. adjunktus, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

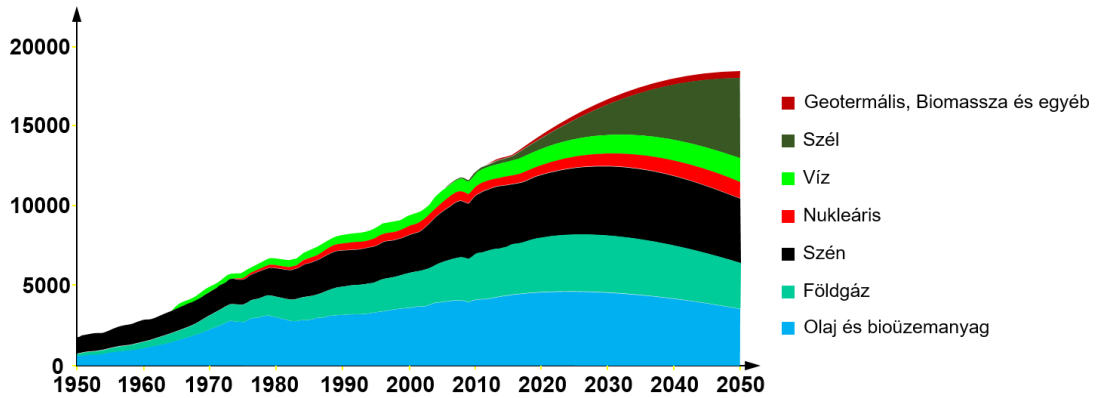
Az izzólámpa feltalálása óta a villamosenergia felhasználása az elmúlt 140 évben szédületes gyorsasággal terjedt el, napjainkra szerves részévé vált életünknek. Ezzel együtt járva a világ energiatermelése globálisan a megnövekedett fogyasztási szint miatt környezeti problémákat okoz. Ennek oka az energia mixben található magas szén-dioxid kibocsátású fosszilis tüzelőanyagok masszív alkalmazása, amelyek a teljes globális energiaellátás mintegy 80 %-át adják. A probléma enyhítésének az egyik módja az atomenergia, mint a legnagyobb karbonmentes termelő alkalmazása, hiszen a nukleáris energia felhasználásával alapvetően környezetbarát energia állítható elő. [1]

A nukleáris energia békés célú alkalmazása viszont kockázattal jár, annak üzemi biztonsági követelményeinek betartása és betartatása prioritás. Meghibásodásuk során jelentősen károsíthatják a környezetet és veszélyt jelentenek az emberi életre, ezért társadalmi megítélésük és alkalmazásuk országonként változó. Ráadásul az elmúlt évtizedek komoly atomerőművi baleseteinek hatásai nemcsak a szűk reaktori környezetben, de a megye és országhatárokat átívelően hatottak. [1]

Ezek tudatában tehát minél jobban megismerjük és feldolgozzuk a megtörtént káreseteket, azok kiváltó okait, annál jobban fel tudunk készülni technológiailag és emberi oldalról is ezek elkerülésére és elhárítására.

A NUKLEÁRIS ENERGIA SZEREPE NAPJAINKBAN

A világ energiaigénye az előrejelzések szerint tovább növekszik majd, ahogy az az 1. ábrán leolvasható. A 2025-ig szóló tendencia alapján az energia mixben minden komponens növekedést fog mutatni. A 20-as évek második felétől viszont már a fosszilis energiahordozók aránya abszolút értékben is csökkenni fog a várható előrejelzések szerint. Ennek pótlására nagy léptékben növekszik majd a megújuló energiahordozók aránya.



1. ábra: Globális primer energiaigények dinamikája (1 millió tonna olaj=41,868 PJ)
Forrás: Szerkesztette [2] nyomán a szerzők

A világ harminc országában működik mintegy négyszáznegyven atomerőművi reaktor, amelyek 2019 végére a globális villamosenergia-termelés mintegy 10 %-át adták. Elmondható tehát, hogy az atomenergia kulcsfontosságú alacsony széndioxid-kibocsátású energiatermelési mód. Ugyan az utóbbi időben a nukleáris energiatermelés arányaiban

csökken, bár abszolút értékben az atomerőművi energiatermelés növekedett. Ugyanis egyes országok, mint például Németország, ahol az atomerőművek a leállítása mellett döntöttek. Ellenpéldaként viszont más országok folyamatosan fejlesztik az atomreaktorok hatékonyságát és üzemeltetési rugalmasságát.

A nemzetközi trendek szakmai vizsgálata (WNISR) rámutat, hogy a nukleáris energetika terén a jövő vezető régiói várhatóan áttevődnek az ázsiai térségre. Köztük is kiemelten a feltörekvő két gazdasággal rendelkező két legnépesebb Kínát és Indiát sorolják az élre az elemzések. Mindkét ázsiai ország a terveik szerint „flotta üzemmódban" építi az atomerőműveit. A tanulmány szerint jelenleg Kína rendelkezik a világ legfiatalabb, mindössze 8,8 év átlagéletkorú nukleáris erőművi flottájával. [3] [6]

ATOMERŐMŰVEK GENERÁCIÓI

1. generáció

A II. világháború befejezése után a tudósok az atomenergia békés célú felhasználásának az alapjait kívánták lefektetni, de a két szuperhatalom közötti hidegháború kitörése elodázta a nukleáris energia kiaknázásának a lehetőségét. A múlt század közepén létesült atomerőművek jelentős részben katonai célt szolgáltak. Az első hálózatra kapcsolt atomerőművek viszonylag kis teljesítményűek voltak (<250 MW), kis darabszámú szériák készültek el belőlük, többnyire természetes urán üzemanyaggal működtek és a biztonságos üzemeltetés nem játszott nagy szerepet bennük. Az 1957-ben az angliai Windscale-ban és a szovjet Kistimben bekövetkezett súlyos balesetek rávilágítottak a technológiák veszélyeire. [4]

2. generáció

A jelenleg működő nukleáris reaktorok többsége ide sorolható, de tervezett élettartalmuk hamarosan lejár. Ezek már kereskedelmi forgalomban kapható nagy darabszámú szériák voltak. Az első generációs reaktorok hibáiból levont tanulságokat figyelembe véve a 70-es évektől kezdődően biztonságnövelő átalakításokat alkalmazva épültek meg a második generációs reaktorok. A műszaki fejlesztés révén alkalmazásba került a nyomásálló konténment szerkezet, amely baleseti helyzetben megakadályozta a radioaktív anyag kijutását a szabadba, valamint beépítésre került az üzemzavari hűtőrendszer, és mindkettő alkalmazásának 100 %-os biztonságot tulajdonítottak. Továbbá a 70-es években dolgozták ki a Norm Rasmussen nevével fémjelzett valószínűségi kockázat elemzés módszerét is. Ezzel a módszerrel lehet kiszámolni a bekövetkezhető reaktorbalesetek valószínűségét. Az ebből készült jelentés kimutatta, hogy a kockázatok terén élen járnak a humán faktorra visszavezethetők. Nem sokkal később, az évtized végén bekövetkezett amerikai Three Mile Island-i atomerőmű balesete megerősítette ezt a megállapítást. [4] [5] [6] A baleset után megváltozott az atomerőművi operátorok továbbképzése, alkalmazni kezdték a szimulátorokat.

3. generáció

A 90-es évektől kezdve létesült atomerőműveket soroljuk a harmadik generációhoz, vagy más néven evolúciós erőművekhez. Itt szintén az előző generáció üzemeltetési tapasztalatára támaszkodva kidolgozott korszerűsített műszaki-technikai újítások kerültek beépítésre. A fejlődésüknek köszönhetően magasabb üzemanyag hasznosítással és hatásfokkal üzemelnek, a korábbiakhoz képest jóval nagyobb, akár 60 éves üzemidővel. A sajnálatos balesetekből levont tapasztalatok, valamint a technológiai és számítástechnikai fejlődésnek

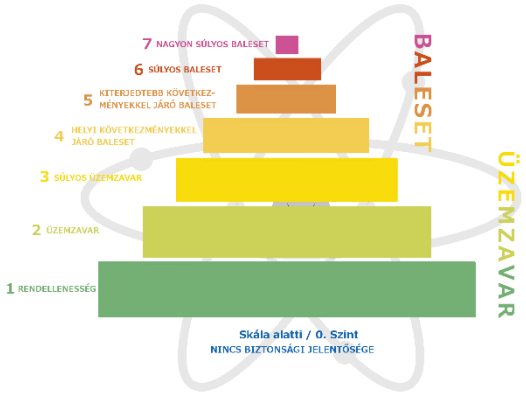
köszönhetően az aktív és passzív biztonsági rendszerek is jelentős fejlődésen mentek keresztül. [4] [5]

4. generáció

Innovációs erőműveknek is nevezhetők, fejlesztés alatt álló reaktorok. Meg kell, hogy feleljenek a megnövekedett biztonsági feltételeknek, minimális a radioaktív hulladéktermelés, valamint magas fokú profitabilitás. A most még kísérleti fázisban leledző erőművek jelentős előrelépést hozhatnak. Az elképzelések a hagyományos termikus reaktorok továbbfejlesztése mellett, a gyorsreaktorok térnyerésével is számolnak. A megemelt termikus viszonyok hatásfok növekedést eredményeznek, továbbá kapcsolt energiatermelésre is alkalmassá teszi őket. Kapcsolt műveletnek olyan üzemanyagok gyártását értjük, mint hidrogén, metanol vagy metán. [6]

AZ ATOMENERGIA KOCKÁZATAI

Az INES skálát a Nemzetközi Atomenergiai Ügynökség (IAEA) és a Nukleáris Energia Ügynökség (OECD) szakértői grémiuma a 90-es évek elején alkotta meg. A metodológiát eleinte a nukleáris energetikában vezették be, a későbbiekben viszont tovább fejlesztve kiszélesítették annak felhasználási körét az atomiparhoz kötődő létesítményi környezetben lezajlódó nem várt üzemállapotok adekvátabb megítélésére. [7] Az INES skála hét csoportra osztja a biztonságot érintő rendellenességeket, ahogy az a 2. ábrán leolvasható.



2. ábra: Az INES eseményskála [8]

A skála kialakításánál a cél az volt, hogy egy adott szintű esemény súlyosságánál közel egy nagyságrenddel legyen jelentősebb a skála eggyel magasabb szintjére sorolt esemény súlyossága (a skála tehát logaritmikus). A csernobili atomerőműben 1986-ban bekövetkezett baleset az INES skálán 7-es szintű (kiterjedt egészségügyi és környezeti hatás) besorolást kapott. Ezzel egyenértékű a 2011-ben bekövetkezett Fukusimai baleset is (kiterjedt környezeti hatás). A skála nem alkalmazható azokra az esetekben, amelyek tisztán ipari biztonsággal vannak összefüggésbe, vagy amelyeknek nincs sugárbiztonsági vagy nukleáris biztonsági vonzatuk. Nem minősíthető a skála alkalmazásával pl. azon tűzesetek besorolására sem, melyek nem járnak radiológiai kockázattal, és nem érintenek nukleáris biztonsági

jelentőségű berendezést. [7] Köszönhetően annak, hogy az INES skála egységesen alkalmazott kategóriarendszer, és jelentéstartalmában mindenki által használt egyformán értelmezett, ezért a határ-menti együttműködésben is azonnali kommunikációs eszközként használható.

JOGSZABÁLYI KÖRNYEZET

A Magyar Országgyűlés 1980. március 7-én fogadta el az első Atomtörvényt, ami a rendkívüli szigorú követelmények jogi alátámasztását tette lehetővé. Tizenhat évvel később ezt váltotta fel 1996. december 18-án kihirdetett 1996. CXVI. törvény az atomenergiáról, amelynek 4. § (2) pontja szerint „*Az atomenergia alkalmazása során a biztonságnak minden más szemponttal szemben elsőbbsége van".* [9] E szabályozási körben a jogalkotó a nukleáris balesetek elhárításával kapcsolatos hatósági felügyeleti jogköröket az Országos Atomenergia Hivatalhoz (OAH) telepítette. A hivatal feladatainak sorában markánsan megjelenített kötelezettség a tájékoztatási tevékenység. [1] Mivel a biztonságos üzemeltetés teljesülése prioritás az atomenergia békés célú alkalmazásánál, ezért már a létesítési folyamat kezdeti fázisában is központi kérdés a tűzvédelmi előírások érvényesítése. Ebben alapelvnek tekintjük a mélységi védelem kialakításának elvét. Ami azt jelenti, hogy a nukleáris erőművek tervezésének folyamán úgy kell kialakítani a szervezeti struktúrákat és konstrukciókat, hogy az összekapcsolódó és egymáshoz illeszkedő védelmi szinten garantálják a bekövetkezhető hibák kompenzálása, kijavítása mielőtt még döntően veszélyeztethetnék a biztonságot. Ezzel az egymásra épülő műszaki megoldásokkal és intézkedésekkel az üzemzavar vagy baleset bekövetkezése terén nagyfokú robusztussággal ruházható fel a rendszer. [10]

Ezáltal a létesítmény külső és belső zavarokkal szembeni ellenállása egyaránt fokozható. A humán faktor jelentette kockázatok szerepének érdemi háttérbe szorítása céljából, minél nagyobb teret kell engedni a műszaki megoldásoknak. Egyúttal a kivitelezésben minőség valamennyi szegmensében az elérhető legmagasabb követelményrendszert kell érvényesíteni, kiküszöbölendő a rendellenes üzemállapotok bármiféle létrejöttének lehetőségét. Az aktív és passzív tűzvédelmi rendszerek kompatibilitását olyan színtűre kell emelni, hogy azok funkcióvesztése ne eredményezhesse más elemek esetleges működési zavarát, kiesését. Már a tervezési fázisban meg kell határozni a veszélyes és éghető anyagok veszélytelen elhelyezését és kezelésük kockázatmentes elvégzését. Mindemellett a különös gondossággal kell eljárni a kockázati egységek és tűzszakaszok definiálásában és az ezekhez kapcsolódó menekülési és felvonulási útvonalakat érintően. [1] [10]

Az Országos Tűzvédelmi Szabályzatról szóló 54/2014. (IX.6.) BM rendelet alapján "*az atomerőmű vonatkozásában olyan tűzvédelmi biztonsági rendszerek és rendszerelemek alkalmazására továbbá manuális tűzoltási lehetőségek kombinálására van szükség, amely olyan jelző és oltó eszközökkel rendelkezik, hogy képes a tüzeket ellenőrzése alatt tartani*." [11]

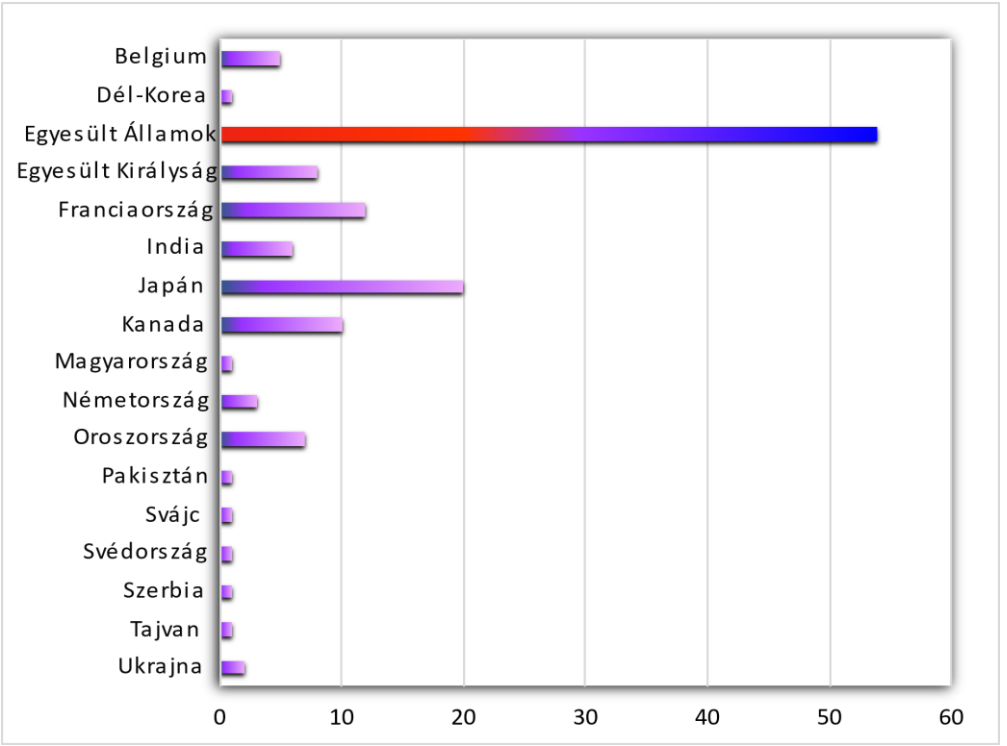
Az atomerőművek esetében a létesítési megfontolások valamennyi paraméterét érintően – az egyéb területekhez hasonlóan - tűzvédelmi tervezést meg kell, előzze a tűzkockázat-elemzés. Ennek köszönhetően szavatolható, hogy valamennyi a tűzbiztonságot hátrányosan befolyásolható tényező adekvát módon legyen megítélhető. A kockázatelemzés nukleáris energiatermelés valamennyi műszaki és üzemeltetési szempontjait egyesíti a tűzmegelőzés előírás rendszerének legmagasabb szintjén.

ÜZEMI ESEMÉNYEK VIZSGÁLATA

Az atomkorszak kezdetén atomlétesítmények vonatkozásában jelentős prioritást kaptak a nukleáris fegyverkezés szempontjai, melynek köszönhetően a fegyverminőségű hasadóanyagok előállítását szolgáló reaktorok domináltak. Ezt követően az 1950-es évek második felében jelentek meg a hálózatra termelő első atomerőművek.

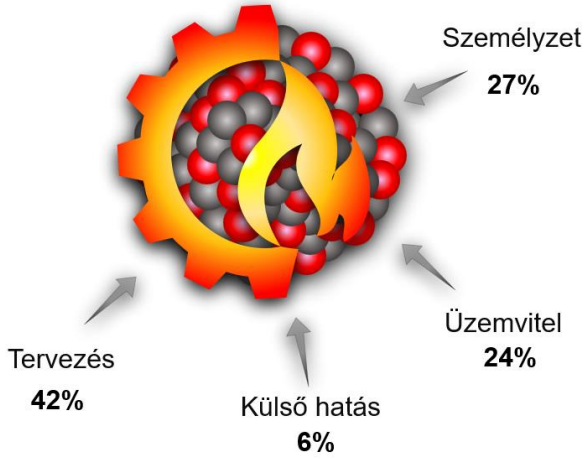
A Nemzetközi Atomenergiai Ügynökség adatai alapján az elmúlt mintegy 70 évben több mint száz üzemzavar és baleset történt a világban. Nukleáris vagy radioaktív baleset a Nemzetközi Atomenergiai Ügynökség definíciója szerint *„olyan esemény, mely jelentős következményekkel jár az ember, a környezet vagy az infrastruktúrára tekintettel. Ide tartozik többek között minden sugárbetegség, a környezetbe jutott magas ionizáló sugárzás vagy a reaktor védőburkának megolvadása”*. [12]

A 3. számú ábrán az üzemzavarok és balesetek országonkénti bontásban láthatók. Ebből jól kiolvasható, hogy az összes atomenergiával kapcsolatos üzemzavarok és balesetek 60 %-a az Egyesült Államokban történt. Az USA-ban a világon a legtöbb, mintegy száz atomerőművi blokk működik.



3. ábra: Üzemzavarok és balesetek száma országonként
Forrás: Szerkesztette [12] nyomán a szerzők

A rendelkezésre álló több mint 100 esetből az a 33 esetet vizsgáltam meg, amelyben a baleset következményeként tűz ütött ki, vagy a tűz kitörését sikerült megakadályozni. [13]



4. ábra: Tűzesetek kiváltó okai
Forrás: Szerkesztette [12] nyomán a szerzők

Megvizsgálva a tűzbalesetek kiváltó okait, alapvetően két tényező határozta meg: műszaki tervezési, valamint emberi okok. Műszaki ok lehet például az alapvetően hibás tervezési konstrukció alkalmazás, berendezések rossz minősége, fáradása, meghibásodása. Az emberi tényezők viszont összetettebbek, mint például a biztonsági előírások akaratlan megszegése, döntésképesség csökkenése stresszhelyzetben. A 4. ábrán láthatóan ez a két fő ok mellet néhány esetben a külső tényezők, természeti katasztrófák voltak az események elindítói.

A tanulmányozott 33 esetből 12 esetben az INES skála szerinti üzemzavarról, és további 12 esetben pedig balesetről beszélhetünk (1. Táblázat). A fennmaradó 9 eset eseménye nem kapott INES skála besorolást.

Ország	INES-besorolás						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Argentína				1			
Belgium		1	1				
Egyesült Államok			2	2	1		
Egyesült Királyság					1		
Franciaország	6			1			
Japán	1			1			1
Kanada		1			1		
Oroszország						1	
Svájc				1			
Ukrajna							1
Kategória	Üzemzavar			Baleset			

1. Táblázat: INES eseményskálán besorolt tüzesetek száma
Forrás: Szerkesztette [12] nyomán a szerzők

A fenti adatokból az alábbi következtetéseket lehet levonni:

- A bekövetkezett üzemzavarok és balesetek 1. és 2. generációs reaktorokban következtek be.
- A vizsgált üzemzavarok és balesetek, majd 1/3-ban történt tűzeset.
- A legismertebb négy, az INES eseményskálán legmagasabb besorolást kapott súlyos baleset mindegyike tűzesettel járt.
- A vizsgált üzemzavarok és balesetek 24 %-a az INES eseményskálán is besorolható volt.
- A vizsgált üzemzavarok és balesetek nagy többsége emberi mulasztás és műszaki okok miatt történt.
- a balesetet szenvedett reaktorok típusai vegyes képet mutatnak. Volt közöttük plutónium tenyész reaktor, forralóvizes reaktor (RBMK, melynek moderátora grafit, hűtőközege elgőzölgő könnyűvíz), valamint nyomottvizes reaktor.

TŰZESETEK KÖVETKEZMÉNYEI

Az atomerőművek üzemi biztonságával szemben magasak az elvárások, mégis az elmúlt évtizedekben az egész világ közvéleményére ható balesetek és üzemzavarok következtek be. [14]

Az első baleset Angliában történt a Windscale erőműben. A reaktort a negyvenes években nyitották meg katonai céllal. Az 1957-ben történt katasztrófa alatt az erőmű grafitmoderátora a túlmelegedés következtében kigyulladt és két napig égett, a reaktor kéményből radioaktív jód és mérges gázok távoztak. A reaktor környezetében egy 500 km2-es terület elszennyeződött, valamint a reaktor személyzetének tagjai magas sugárterhelésnek voltak kitéve. A baleset az INES skálán 5-ös fokozatot kapta. [14]

Időben a második baleset a már korábban említett Pennsylvania államban következett be. Ezt nevezik Three Mile Island (TMI) balesetnek. A nukleáris katasztrófa kiváltásához egyidejűleg járult hozzá a konstrukció, valamint az emberi tévedés. Ráadásul a balesetben érintett TMI-2 blokkot hónapokkal korábban adták át. A balesetben az aktív zóna túlmelegedett, a fűtőelemek és szerkezeti anyagok megolvadtak, a lezajló reakciókban felszabaduló hidrogén robbanása a szerkezeti károk mellett, továbbá illékony radioaktív izotópok kiszabadulását eredményezték. A baleset az INES skálán 5-ös fokozatot kapta. [14]

A harmadik baleset Szovjetunióban történt 1986-ban, 130 km-re Kijevtől a csernobili atomerőműben. A legismertebb atomkatasztrófa kiváltásához ebben az esetben is tervezési hibák és emberi mulasztás vezettek. A baleset következtében a 4-es blokk reaktorát két robbanás rázta meg, amely felszakítva a reaktorcsarnok tetejét és megrongálva a szerkezet falait, utat engedett a radioaktív szennyezésnek. Az események után a reaktorban a tűz napokon át lángolt. A környezetbe kiszabaduló radioaktív szennyeződés mértéke, több nagyságrenddel meghaladta a II. világháborúban Japánt ért atomtámadásokban szétterjedt sugárszennyezés mértékét. A létesítmény körül 30 km-es lezárt övezetet hoztak létre, a lakosságot kitelepítve onnan. [1] A baleset az INES skálán 7-es fokozatot kapta.

A negyedik baleset szintén a 7-es besorolást kapta az INES skálán. Az esemény ezúttal a távol-keleti Japánban történt 2011-ben a Fukushima Daiichi-ben. A 9-es erősségű földrengés következtében, amelyet a működő erőmű rendszerei is érzékeltek, automatiku-

san leálltak. Ez még nem okozott kritikus problémát, mert földrengésállók voltak az építmények. Viszont az ezt követő 15 m magas szökőár következtében az 1-es, 2-es és 3-as blokkokban leállt a maradék hőelvonó rendszer, mert a szökőár tönkretette a hőcserélő rendszert és a 12 tartalék generátort. A túlhevülés következtében 3 reaktor zónasérülést szenvedett, a magas hőmérsékletű olvadék átégette a reaktortartályt, továbbá legalább 4 hidrogénrobbanás történt letépve az épületek fedelét. A robbanás következtében a távozó gőz radioaktív nemesgázokat és jódot tartalmazott. Ennek következtében 20 km sugarú szennyezett zóna keletkezett, ahonnan 165.000 embert ki kellett telepíteni. A kármentés még napjainkban is zajlik. Ennél a katasztrófánál elmondható, hogy nem következett volna be, ha magasabb gátat emeltek volna a hullámok megállítására, és a dízel generátorokat magasabbra helyezik. [15]

KÖVETKEZTETÉS

Az ENSZ 2023. november 30. és december 12. éghajlatváltozási konferenciáján a fosszilis tüzelőanyagok fokozatos kivezetése és a megújuló energiakapacitás növelése érdekében az aláíró országok 2050-re a 2020-as szinthez képest meg szeretnék háromszorozni az atomerőművek hálózatra kapcsolt áramellátó kapacitását világszerte. A nyilatkozat olyan tudományos állásfoglalásra hivatkozik, amely szerint 2050-ig a klímasemlegesség nem érhető el atomenergia nélkül.

Elmondható tehát, hogy az elfogadható léptékű kockázatok mellet, a következő évtizedekben az atomenergiában további lehetőségek rejlenek. Nem szabad viszont megfeledkeznünk a veszélyekről és le kell vonnunk a következtetéseket. Az eddigi tapasztalatokat felhasználva kell építenünk a jövőnk nukleárisenergia-startégiáját. Ennek biztonságát csak hatékony monitoring rendszerekkel és a tűzvédelmi követelményeket maradéktalanul érvényesítő mérnöki megoldásokkal lehet megvalósítani.

FELHASZNÁLT IRODALOM

[1] Manga László, Kátai-Urbán Lajos, *Nukleáris balesetekből levonható tanulságok – a tudomány állása I. rész,* BOLYAI SZEMLE 2016/4, pp.: 120-136. (2016)
[2] Engineered science, https://www.researchgate.net/figure/World-primary-energy-consumption-million-tons-of-oil-equivalent-1950-2050_fig2_326809889 (letöltés dátuma: 2024.01.07.)
[3] Energiaklub, *Atomerőművek építés alatt – 2022*. Energia Klub Környezetvédelmi Egyesület, https://energiaklub.hu/files/study/Atomeromuvek_epites_alatt_2022_0.pdf (letöltés dátuma: 2024.01.07.)
[4] Antal Zoltán, Kátai-Urbán Lajos, Vass Gyula, *Atomerőmű generációk fejlődésének vonzatai*, HADMÉRNÖK XIII. évf. 3. szám (2018)
[5] Energiaklub, *Reaktorta - Nukleáris erőművek és környezetünk*. Energia Klub Környezetvédelmi Egyesület 2001. ISBN 6930093650, https://energiaklub.hu/files/brochure/reaktorta.pdf (letöltés dátuma: 2024.01.07.)
[6] Radnóti K., Király M., *Az atomenergiáról egyszerűen: az atomerőművek működése, típusaik és jövőjük.* Nukleon, VIII 177 (2015), pp.: 1-13.oldal.

[7] Országos Atomenergia Hivatal, *AKFT1.48. sz. útmutató - Az INES minősítés elvégzésének módszertana nukleáris és radiológiai események esetén*. https://www.haea.gov.hu/web/v3/oahportal.nsf/AB534110DEE39331C1257BE400746F05/$File/AKFT1.48v1.pdf (letöltés dátuma: 2024.07.04.)
[8] Országos Atomenergia Hivatal, Veszélyhelyzet-kezelés - INES skála, https://www.haea.gov.hu/web/v3/OAHPortal.nsf/web?openagent&menu=02&submenu=2_6_1, (letöltés dátuma: 2024.06.19.),
[9] 1996. évi CXVI. törvény az atomenergiáról
[10] Antal-Farkas Zoltán: Atomerőmű létesítés nukleáris veszélyhelyzet-kezelési követelményeinek kutatása és fejlesztése. Doktori értekezés, pp.: 255-258 oldal.
[11] Antal Zoltán, Vass Gyula, Kátai-Urbán Lajos: *Atomerőmű létesítés tűzvédelmi követelményeinek vizsgálata,* Védelem tudomány II. évfolyam 1. szám, pp.: 17-30. (2017)
[12] Laka fundation, *Lokation – Europe*, Documention and research centre on nuclear energy. https://www.laka.org/docu/ines/location/europe/, (letöltés dátuma: 2024.03.07.)
[13] ARIA, Online Database, French Ministry of Environment, Bureau for Analysis of Industrial Risks and Pollutions. Analysis, Research and Information on Accidents, https://www.aria.developpement-durable.gouv.fr/?lang=en&s=nuclear%20INES%20scale&fwp_recherche=nuclear%20INES%20scale (letöltés dátuma: 2024.03.07.)
[14] Dobor József, Kossa György, Pátzay György : *Atomerőművi balesetek és üzemzavarok tanulságai 1.* Hadmérnök, XII. Évfolyam 1. szám (2017. március), pp.: 58-71.
[15] Dobor József, Kossa György, Pátzay György : *Atomerőművi balesetek és üzemzavarok tanulságai 2.* Hadmérnök, XII. Évfolyam 4. szám (2017. december), pp.: 84-98.

DOI: https://doi.org/10.12700/btsz.2025.7.1.129

A REVIEW OF THE MULTIFACETED NATURE OF CORROSION: THE IMPACT OF STEEL FORMABILITY AND SURFACE ROUGHNESS ON CORROSION RESISTANCE (PART 1)

A KORRÓZIÓS MEGHIBÁSODÁSOK ÁTTEKINTÉSE: AZ ACÉL ALAKÍTOTTSÁGÁNAK ÉS FELÜLETI ÉRDESSÉGÉNEK HATÁSA A KORRÓZIÓÁLLÓSÁGRA (1. RÉSZ)

HUSZÁK Csenge[1] – KOVÁCS Tünde Anna[2] – PINKE Péter[3]

Abstract

This two-part review article explores the diverse nature of corrosion, focusing on the impact of steel formability and surface roughness on corrosion resistance. Corrosion is a significant issue in various industries, leading to economic losses and safety risks. Traditional methods often overlook the effects of steel's formability and surface roughness, which can influence stress distribution, microstructure, and areas prone to corrosion. This article reviews environmental factors contributing to corrosion, such as material composition, electrochemical potential, surface roughness, stress, deformation, and temperature. A case study by Wang et al. presented in this article, while the 2nd part of our paper focuses more on case studies.

Keywords

Safety Critical Components, Corrosion, Surface Roughness, Corrosion Resistance, Structural Safety

Absztrakt

Ez a két részes áttekintő cikk a korrózió sokrétű természetét vizsgálja, különös tekintettel az acél alakítottságának és felületi érdességének hatására. A korrózió jelentős problémát okoz különböző iparágakban, gazdasági veszteségeket és biztonsági kockázatokat eredményezve. A hagyományos módszerek gyakran figyelmen kívül hagyják az acél alakítottságának és felületi érdességének hatásait, amelyek befolyásolhatják a feszültségeloszlást és a mikroszerkezetet. E cikk áttekinti a korrózió főbb típusait, a hozzájáruló környezeti tényezőket, mint például az anyagösszetétel, az elektrokémiai potenciál, a felületi érdesség, a feszültség és a hőmérséklet. Cikkünk első része Wang esettanulmányára épül és azt mutatja be, míg cikkünk második része további esettanulmányokat mutat be.

Kulcsszavak

Biztonságkritikus komponensek, Korrózió, Felületi érdesség, Korrozióállóság, Szerkezeti integritás

[1] huszak.csenge@bgk.uni-obuda.hu | ORCID: 0000-0001-8817-5435 | PhD Student, Óbuda University - Doctoral School on Safety and Security Sciences | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] kovacs.tunde@bgk.uni-obuda.hu | ORCID: 0000-0002-5867-5882 | University Professor, Óbuda University - Bánki Donát Faculty of Mechanical and Safety Engineering | Egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[3] pinke.peter@bgk.uni-obuda.hu | ORCID: 0000-0001-8817-5435 | Associate Professor, Óbuda University - Bánki Donát Faculty of Mechanical and Safety Engineering | Egyetemi docens, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

Corrosion is a significant problem in industry, as damage to metals and other structural materials can cause serious economic losses and pose a safety risk. It can significantly reduce the lifespan of industrial equipment, pipelines, tanks, and other structures, increasing maintenance and replacement costs. Additionally, corrosion can pose safety risks, especially in industries such as oil and gas, chemical, and energy sectors.

There are several traditional methods for determining corrosion resistance, the most common of which are [1] [2]:

- Laboratory Tests: These involve exposing metals to various corrosive environments and measuring the rate and extent of corrosion.
- Electrochemical Methods: This includes the potentiodynamic polarisation test, which measures metals' corrosion potential and current.
- Field Tests: These involve testing metals under actual environmental conditions over an extended period to determine the actual effects of corrosion.

When examining steel's corrosion resistance, the formability and surface roughness are often overlooked. However, these factors can significantly impact corrosion. Steel's formability can affect stress distribution and microstructure, while surface roughness can increase the number and size of areas prone to corrosion.

THE BASICS OF CORROSION

Corrosion processes primarily occur through chemical and electrochemical reactions, during which metals lose electrons, i.e., they oxidise and turn into ions. Any reaction involving electron donation and acceptance is called a redox reaction. The particle that donates electrons oxidises, while the one that accepts electrons reduces. Thus, corrosion is a reaction between metals and other structural materials with the environment, during which the material reverts to a more stable, lower energy state through chemical or electrochemical processes. This causes changes in size and mass, as well as a decrease in the component's strength. A disadvantageous property is that it damages machine parts during operation and storage if protection is neglected.

The most common corrosion mechanisms include hydrogen evolution corrosion, where metals dissolve in acidic environments, and oxygen absorption corrosion, where metals oxidise in aqueous solutions. Several factors, including chemical affinity, concentration, pressure, temperature, and the size of the reacting surfaces influence the corrosion rate. Corrosion can occur in liquid, gas, and solid media, leading to liquid corrosion, atmospheric or gas corrosion, and soil corrosion.

Based on the mechanism of the corrosion process, we can distinguish between chemical, transitional, and electrochemical corrosion. In chemical corrosion, the reactions between the metal and the environment are chemical, while in electrochemical corrosion, the cathodic and anodic positions of the metal, as well as the location of metal ion and electron release and the conditions for electron acceptance, determine the process. Transitional corrosion is a combination of chemical and electrochemical processes [1].

The chemical reactions occurring during corrosion can be divided into two main types: hydrogen evolution and oxygen absorption reactions. Hydrogen evolution reactions

occur on the surface of metals in contact with aqueous solutions, where metal ions are formed and pass into the solution. The general reaction equation is the following, where *Me* can be any metal:

$$Me + 2H^{+} \leftrightarrow Me^{++} + H_2$$

Oxygen absorption corrosion occurs in aqueous solutions with low H^{+} concentration and follows the reaction equation:

$$2Me + 2H2O + O2 \leftrightarrow 2Me + + + 4OH -$$

In this case, the presence of oxygen is also necessary, and metals with higher potential than hydrogen only dissolve in acid after oxidation.

Types of Corrosion

Several types of corrosion affect metals and alloys in different ways. Some common types include general (uniform) corrosion, which uniformly thins the metal surface; localised corrosion, such as pitting and crevice corrosion, which attack specific areas; and stress corrosion cracking, which causes cracks due to the combined effect of mechanical stress and a corrosive environment. Additionally, intergranular corrosion attacks the grain boundaries of metals, while selective corrosion affects specific components of alloys. Other specific types of corrosion, such as boric acid corrosion, can occur in specific environments. In the following some of the previously mentioned corrosion types are presented [1] [2] [3] [4] [5] [6] [7] [8] [9].

General (Uniform) Corrosion: This type of corrosion involves the approximately uniform thinning of the metal surface due to chemical reactions in an aggressive environment. It is particularly characteristic of equipment and pipelines made from unalloyed and low-alloy steels. The rate and other characteristics of general corrosion depend significantly on the material's chemical composition, the operating medium's properties, the operating conditions, and other environmental factors such as temperature, humidity, and the presence of acidic or alkaline vapours. This type of corrosion is presented in Figure 1/a.

Pitting Corrosion: Pitting corrosion is a form of corrosion that localises in narrow areas where the corrosion rate is significantly higher than elsewhere. As a result, relatively deep cavities form, often filled with chemically active contaminants that promote further growth. Pitting corrosion can be particularly problematic for passive metals, such as austenitic stainless steel. This type of corrosion is presented in Figure 1/b.

Crevice Corrosion: Crevice corrosion is locally accelerated damage that occurs in constructional gaps, between fitting parts, cracks, and under deposits. The crevice must be wide enough to allow the medium to enter but narrow enough to prevent the medium from flowing further, resulting in a stagnant condition. Microbiological effects generally accelerate the corrosion process, especially in pitting and crevice corrosion characterized by stagnant or slow medium flow. This type of corrosion is presented in Figure 1/c.

Intergranular Corrosion (IGA): Intergranular corrosion involves the damage of grain boundaries, leading to the loss of cohesion between grains and the disintegration of the damaged parts of the material. The sensitivity of grain boundaries can be due to several factors, such as greater deformation work or the formation of chromium carbides at the grain boundaries. One way to avoid IGA is through chromium chemistry. This type of corrosion is presented in Figure 1/d.

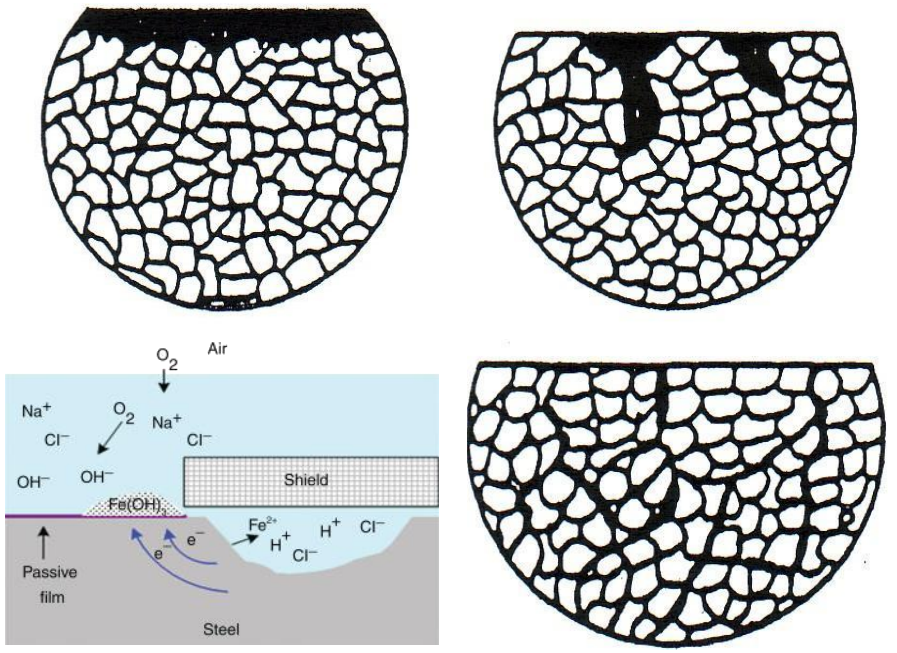


Figure 1: Different types of corrosion. a, General (Uniform) Corrosion. b, Pitting Corrosion. c, Crevice Corrosion. d, Intergranular Corrosion. [4] [10]

Layered Corrosion: A variant of intergranular corrosion observed in sheet metal parts, where the sheet separates into layers. Another variant is stress corrosion, which is caused by mechanical stress. The rate of intergranular corrosion can be characterised by the decrease in strength and elongation over time. This type of corrosion is presented in Figure 2/a.

Selective Corrosion: This type of corrosion attacks alloys, particularly those where one component has a nobler potential than the others. For example, zinc is leached out in the selective corrosion of brass (a copper-zinc alloy), leading to a spongy material. The rate of selective corrosion can also be characterised by the decrease in strength and elongation over time. This type of corrosion is presented in Figure 2/b.

Stress Corrosion Cracking (SCC): SCC can occur in materials sensitive to the combined presence of an aggressive medium and tensile stress. Several factors, such as the fragmentation of oxides, the effectiveness of passivation, or the renewal of the corrosive medium along the crack front influence the development and progression of SCC. SCC damage can be intergranular (IGSCC) or transgranular (TGSCC) and is extremely dangerous as it can cause sudden and unexpected fractures. This type of corrosion is presented in Figure 2/c.

Erosion Corrosion: Erosion corrosion occurs when the flowing corrosive medium locally accelerates the dissolution rate of the material. This damage is often referred to as flow-accelerated corrosion (FAC). The essence of erosion corrosion is that the protective oxide layer on the material surface is continuously or cyclically, locally removed by the

operating medium. The process is influenced by several factors, such as the structural material, geometric and hydrodynamic conditions, the temperature of the medium, its pH, and dissolved oxygen content. This type of corrosion is presented in Figure 2/d.

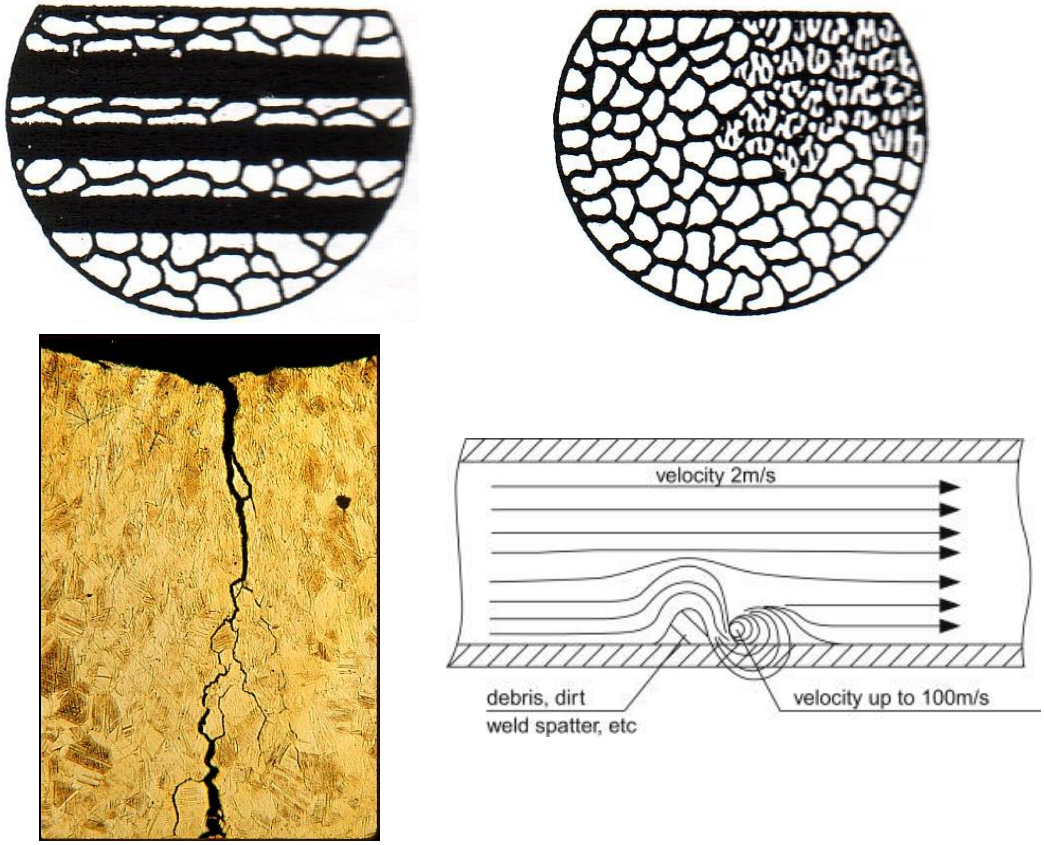


Figure 2: Different types of corrosion. a, Layered Corrosion. b, Selective Corrosion. c, Stress Corrosion Cracking. d, Erosion Corrosion. [4] [11] [12]

Stainless Steels and Their Corrosion Resistance

The chemical composition of metals significantly affects their corrosion resistance. Alloying elements such as chromium, nickel, and molybdenum can enhance corrosion resistance by forming a protective oxide layer on the surface. Unalloyed steels are generally less corrosion-resistant, while high-alloy steels, such as austenitic stainless steels, exhibit excellent corrosion resistance under various environmental conditions.

Austenitic stainless steels, such as types 304 and 316, exhibit excellent corrosion resistance due to their high chromium and nickel content. These steels are particularly resistant to uniform corrosion and pitting. Type 316 also contains molybdenum, which further enhances corrosion resistance, especially in chloride environments [6] [13] [14].

Ferritic stainless steels, such as type 430, have lower chromium and nickel content, making them less corrosion-resistant than austenitic steels. However, these steels still show

good corrosion resistance in many industrial applications, particularly due to their lower cost [15].

Duplex stainless steels, such as type 2205, combine the advantages of austenitic and ferritic steels. Their high chromium and molybdenum content provides excellent corrosion resistance, particularly against pitting and crevice corrosion. Additionally, they are favoured for their high strength and good weldability [5].

Due to their low nickel content, superferritic stainless steels, such as E-Brite and SEA-CURE, offer cost-effective solutions in chloride environments. These steels exhibit excellent corrosion resistance, particularly against pitting and crevice corrosion. They also have high strength and good thermal conductivity, making them advantageous [16].

Improving Corrosion Resistance

Several surface treatment processes, such as electropolishing, passivation, and coating, can improve corrosion resistance. These processes help remove surface contaminants and form a uniform, protective layer on the metal surface.

Adding alloying elements such as chromium, nickel, molybdenum, and nitrogen increases the corrosion resistance of metals. These elements help form a protective oxide layer on the metal surface, preventing corrosion [1] [3] [4] [5] [6].

Heat treatment processes, such as solution heat treatment and post-heat treatment passivation, help improve the corrosion resistance of metals. These processes help remove surface contaminants and form a uniform, protective layer on the metal surface [1] [2] [3].

Testing Corrosion Resistance

There are different types of testing, one of these types is laboratory tests which involve exposing metals to various corrosive environments and measuring the rate and extent of corrosion. These tests allow for comparing corrosion resistance among different materials and evaluating the effectiveness of corrosion protection measures. Laboratory tests include salt spray, potentiodynamic polarisation, and cyclic corrosion tests. Contrary to the laboratory test, the field test involves testing metals under real environmental conditions over an extended period. These tests allow for determining the actual effects of corrosion, considering changes in environmental factors such as temperature, humidity, and contaminants. Data collected from field tests help validate laboratory test results and refine corrosion protection strategies [17] [18].

Corrosion Monitoring Systems

Corrosion monitoring systems continuously monitor the corrosion status of metals and the environmental conditions. These systems provide real-time data on corrosion processes, allowing for quick intervention and minimizing corrosion damage. Corrosion monitoring systems include electrochemical sensors, corrosion potential meters, and corrosion current meters [3] [19] [7] [8].

FACTORS INFLUENCING CORROSION

Numerous environmental factors influence corrosion. Many of these factors are listed below. This list is relatively long but not exhaustive. The factors influencing the rate and spread of corrosion are listed in alphabetical order [1] [3] [6] [7] [8] [12] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36].

- Atmospheric Conditions: Weather patterns, pollution levels, and other atmospheric factors.
- Chemical Composition of the Environmental Medium: For example, the hardness and alkalinity of water or the pH, moisture content, and composition of soil can affect underground corrosion.
- Conductivity: The presence of conductive media can influence electrochemical reactions.
- Electrochemical Potential: Differences in electrochemical potential between metals can cause galvanic corrosion.
- Electromagnetic Fields: The effect of electric and magnetic fields can influence corrosion processes.
- Environmental Medium: Air, water, soil, and other environments that the metal comes into contact with.
- Exposure Time: The duration of the metal's exposure to corrosive conditions affects the extent of corrosion.
- Exposure to Chemicals: Industrial chemicals and pollutants can cause or accelerate corrosion.
- Flow Rate of Fluids: The flow rate of water or air over the metal can influence the extent of corrosion.
- Galvanic Contact: Contact between different metals can lead to galvanic corrosion.
- Human Activity: Maintenance practices, handling, and usage patterns can affect corrosion.
- Humidity: Higher humidity can increase the rate of corrosion.
- Industrial Emissions: Exposure to industrial pollutants can accelerate corrosion.
- Ion Concentration: Certain ions, such as chloride and sulphate, can accelerate corrosion.
- Material Composition: The type of metal and its alloys can significantly affect the extent of corrosion.
- Mechanical Wear: Wear and abrasion of the metal surface can expose fresh metal to a corrosive environment.
- Microbial Activity: The presence of bacteria and other microorganisms can lead to microbiologically influenced corrosion.
- Oxygen Concentration: The availability of oxygen can influence the corrosion process.
- pH Level: Acidic or alkaline environments can significantly affect the extent of corrosion.
- Presence of Contaminants: Contaminants such as salts (e.g., NaCl) can accelerate corrosion.
- Presence of Organic Materials: Interaction with organic materials can affect corrosion.
- Pressure: High or low-pressure conditions can affect the rate of corrosion.
- Protective Coatings: The presence or absence of coatings such as paint or galvanisation.
- Radiation Levels: Exposure to radioactive materials can affect corrosion.

- Salt Concentration: The salt content of the environment can significantly increase the extent of corrosion.
- Stress and Deformation: Mechanical stresses can lead to stress corrosion cracking.
- Surface Roughness: Rougher surfaces can trap moisture and contaminants, accelerating corrosion.
- Temperature: Higher temperatures generally increase the rate of corrosion.
- UV Radiation: Exposure to sunlight and UV rays can damage protective coatings and materials.

The phenomena listed in this list can initiate corrosion on metallic surfaces and influence its spread. Their combined effect, however, can accelerate this process. Three factors are highlighted: surface roughness, stress and deformation, and temperature.

Case studies related to surface roughness and stress corrosion caused by stress are presented in the following two subsections. The effect of temperature on processes is highlighted briefly, with the rule of thumb being that temperature accelerates the reaction rate of chemical processes. The empirically derived Arrhenius equation describes this observation [37], which states that the reaction rate doubles with every 10°C increase in temperature.

Effect of Surface Roughness on Corrosion (Case Studies)

In general, rough surfaces provide more sites for corrosive substances to adhere to, increasing the risk of corrosion. The passive layer forms less effectively on such surfaces, reducing corrosion resistance. In contrast, smoother surfaces provide fewer sites for corrosive substances to adhere to, thereby improving corrosion resistance. Polished and electropolished surfaces are particularly effective in forming and maintaining the passive layer.

Wang et al. [22] in their article examined the effects of temperature and pressure (T and P), velocity (V), and surface roughness (Ra) on the corrosion properties of HP-13Cr stainless steel. For their study, they varied these four parameters as follows:

Four temperature and pressure values:

- 95°C – 2.8 MPa
- 120°C – 3.2 MPa
- 150°C – 3.6 MPa
- 180°C – 3.8 MPa

At these temperature and pressure values, they examined the following four surface roughness samples:

- 0.987 ± 0.031 μm (prepared with 120-grit sandpaper)
- 0.675 ± 0.025 μm (prepared with 240-grit sandpaper)
- 0.288 ± 0.014 μm (prepared with 600-grit sandpaper)
- 0.035 ± 0.009 μm (prepared with 1000-grit sandpaper)

With two different flow rates:

- Static medium (0 m/s)
- 3 m/s medium

The following figure shows the surface roughness profiles of surfaces prepared with 120, 240, 600, and 1000-grit sandpaper.

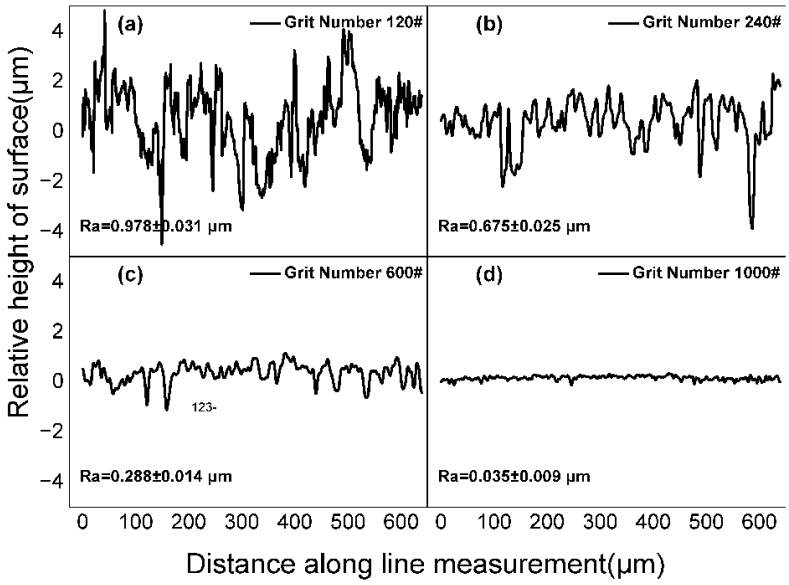


Figure 3. Surface roughness profiles [22]

They also examined their samples using SEM and 3D surface topological analysis, which they modelled with a 2D fluid dynamics simulation. The result of this simulation is shown in the following figure.

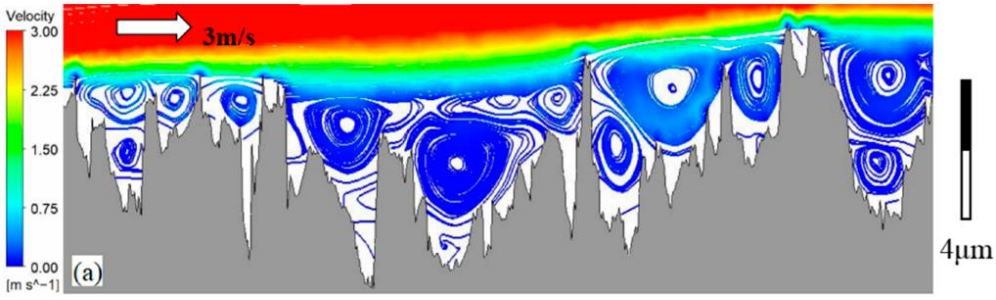


Figure 4. Effect of surface roughness on flow velocity along the surface [22]

The previous figure shows that the flowing medium slows down next to the wall and vortices form in the "trenches" of the surface roughness. The further down towards the bottom line, the more the vortices get trapped in the surface irregularities until their speed becomes zero. This phenomenon is known as the adhesion law in fluid dynamics. Wang et al. highlighted in their study that the moving medium at 3 m/s causes more corrosion than static air.

This phenomenon is also visible in the following two figures. In both figures, the test specimens were cut, and the upper layer of their cross-section is visible. The following figure (Fig. 5.) shows the corrosion test results with the static medium, while Figure 6 shows the results with the flowing medium.

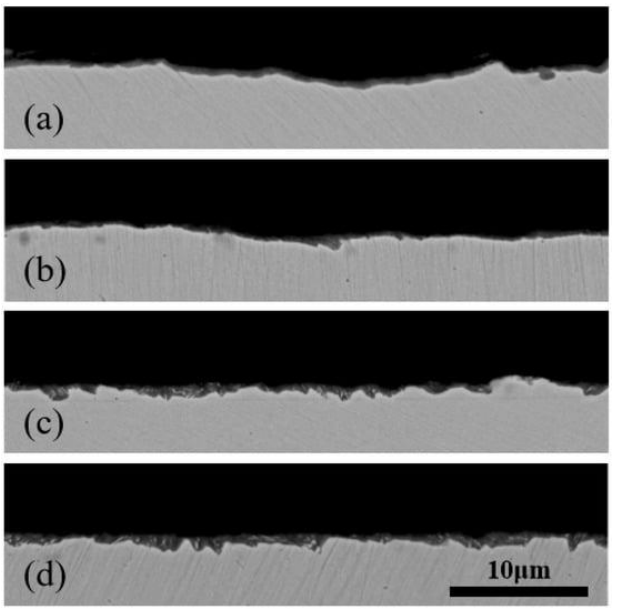


Figure 5. Cross-section upper layer of samples roughened with 120 (a), 240 (b), 600 (c), and 1000 (d) grit sandpaper after immersion test, with 0 m/s flow rate at 150°C and 3.6 MPa. [22]

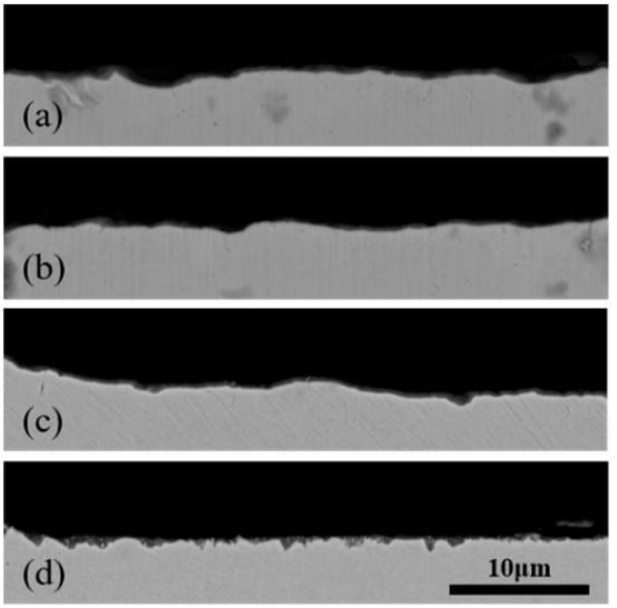


Figure 6. Cross-section upper layer of samples roughened with 120 (a), 240 (b), 600 (c), and 1000 (d) grit sandpaper after immersion test, with 3 m/s flow rate at 150°C and 3.6 MPa. [22]

The following three figures use SEM imaging to show the surfaces of the same test specimens. The first figure shows the state before the immersion corrosion test, the second shows the samples tested with the static medium, and the third shows the samples tested with the flowing corrosive medium.

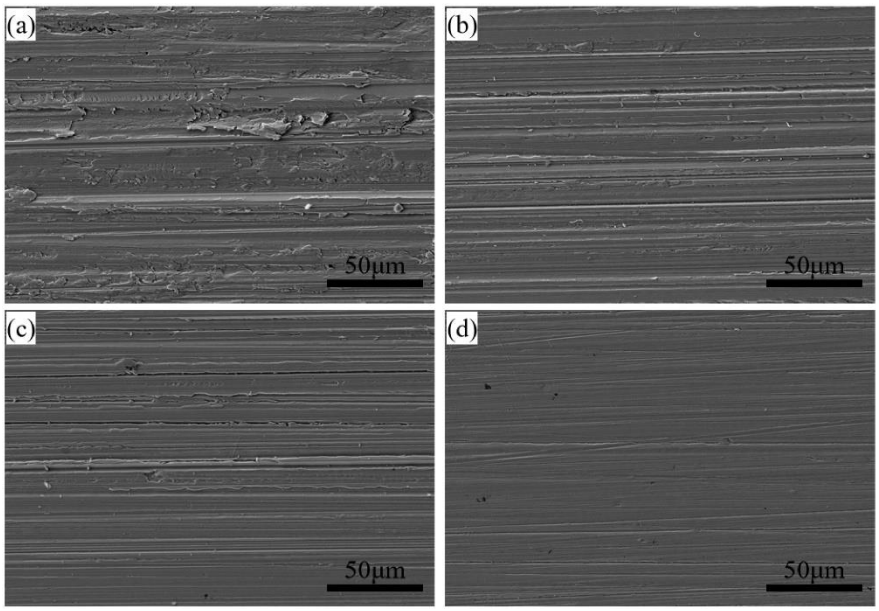


Figure 7. The surfaces of the samples were roughened with 120 (a), 240 (b), 600 (c), and 1000 (d) grit sandpaper before the immersion test. [22]

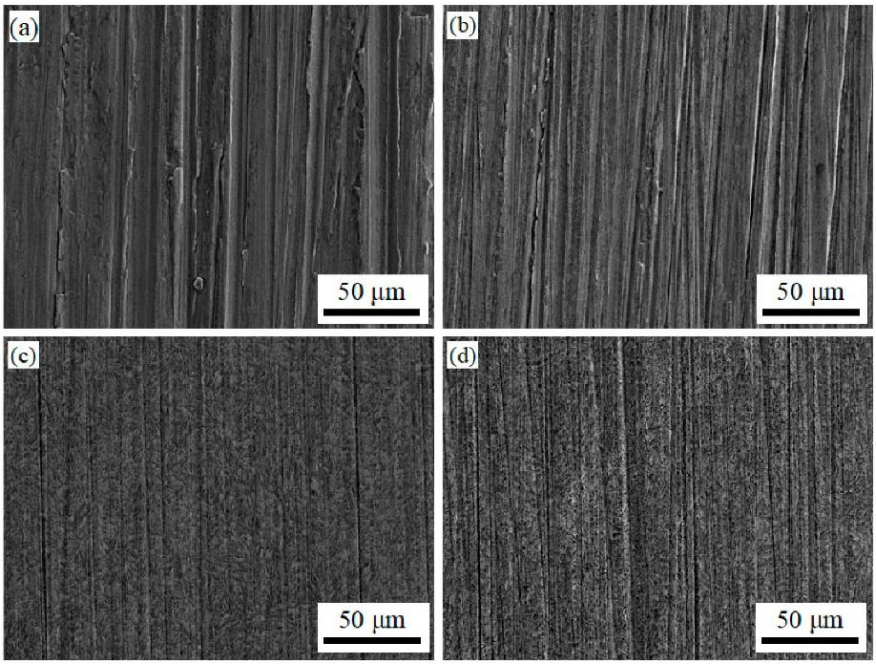


Figure 8. Surfaces of samples roughened with 120 (a), 240 (b), 600 (c), and 1000 (d) grit sandpaper after the immersion test, with 0 m/s flow rate at 150°C and 3.6 MPa. [22]

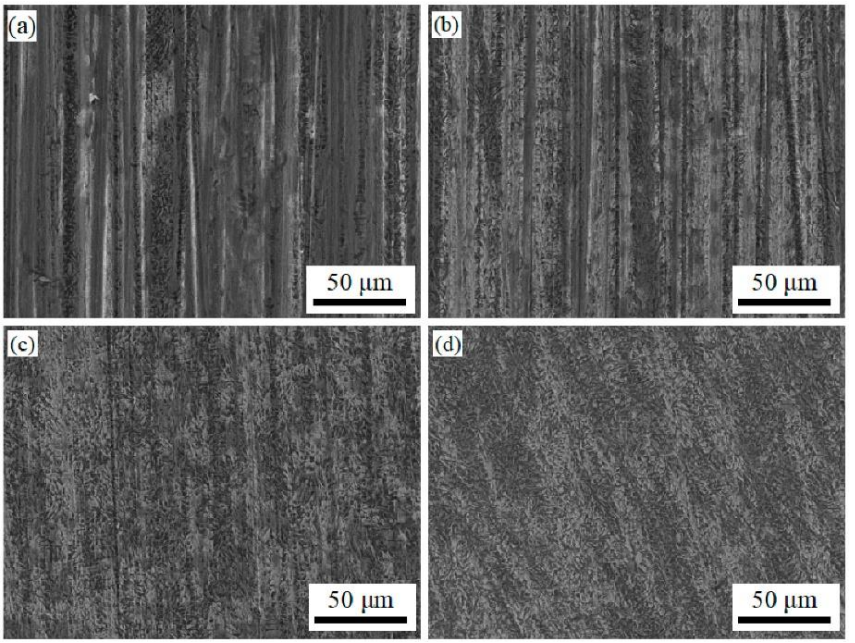


Figure 9. Surfaces of samples roughened with 120 (a), 240 (b), 600 (c), and 1000 (d) grit sandpaper after the immersion test, with 3 m/s flow rate at 150°C and 3.6 MPa. [22]

The surface roughness profile was also measured after the corrosion test. The roughness profile of the sample roughened with 120-grit sandpaper is shown in the following figure.

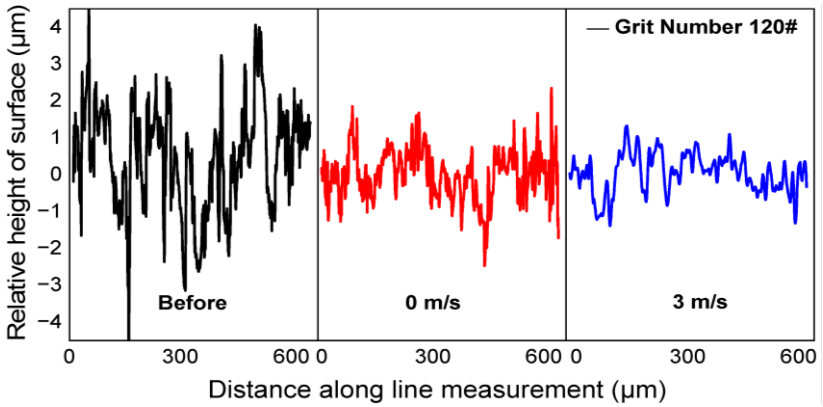


Figure 10. The surface roughness profile of the sample was roughened with 120-grit sandpaper before and after the corrosion tests. [22]

The following figure summarises the results of the tests conducted at the previously outlined temperature and pressure values.

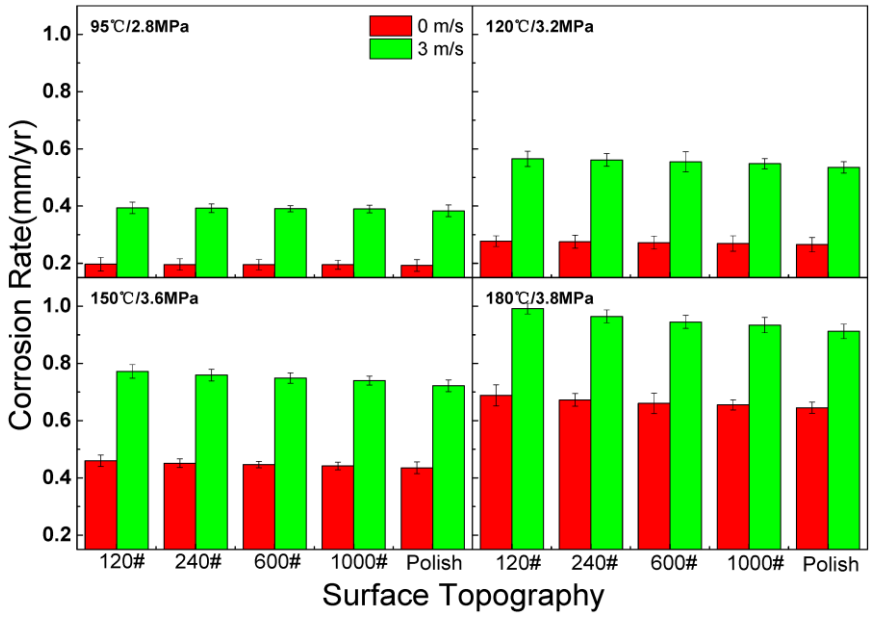


Figure 11. Effect of surface roughness, flow rate, temperature, and pressure on the extent of corrosion [22]

From their measurements, Wang et al. concluded that the interface between the metal and the corrosive solution can be divided into a static and a moving flow layer. The thickness of the surface boundary layer was not affected by the flowing medium, but the thickness of the static layer was reduced. The diffusion of corrosion-causing cations accelerated due to the smaller stagnant layer.

Multi-step vortices formed in the surface boundary layer, hindering the diffusion of Fe^{2+} ions, leading to local acidification along the wall, promoting greater pitting and deeper surface roughness grooves.

Increasing the temperature and pressure reduced the corrosive medium's viscosity, which decreased the thickness of the stagnant layer. This thinning static layer increased the corrosion process.

SUMMARY

In the first part of our two-part review, we presented the multifaceted nature of corrosion, with particular attention to the effects of steel formability and surface roughness. Corrosion resistance is typically determined solely on the basis of chemical composition, often ignoring steel formability, surface roughness, and other manufacturing-related factors.

Our literature review included a number of environmental factors that contribute to corrosion processes, such as material composition, electrochemical potential, surface roughness, stress and strain, and temperature.

This article presents a case study. Corrosion is influenced by the combined effects of many factors, four of which were examined in this case study (temperature, pressure, contact medium flow rate, and surface roughness).

In the second part of our article, we present additional case studies that focus on the corrosion of the corrosion-resistant steels.

REFERENCES

[1] P. A. Schweitzer, Fundamentals of Metallic Corrosion - Atmospheric and Media Corrosion of Metal, Boca Raton: CRC Press, 2007.

[2] Hilti, Corrosion Handbook, 2015.

[3] P. Trampus, Lifetime management (Élettartam gazdálkodás, Lecture notes), Dunaújváros: Dunaújvárosi Főiskola, 2013.

[4] J. Janik, Machine maintenance I. (Gépüzemfenntartás I.), Dunaújváros: Főiskolai Kiadó, 2006.

[5] J. A. Platt, A. Guzman, A. Zuccari, D. W. Thornburg, B. F. Rhodes, Y. Oshida és B. K. Moore, „Corrosion behavior of 2205 duplex stainless steel," American Journal of Orthodontics and Dentofacial Orthopedics, %1. kötet112, %1. szám1, pp. 69-79, 1997.

[6] M. B. Leban, C. Mikyška, T. Kosec, B. Markoli és J. Kovac, „The Effect of Surface Roughness on the Corrosion Properties of Type AISI 304 Stainless Steel in Diluted NaCl and Urban Rain Solution," Journal of Materials Engineering and Performance , %1. kötet23, pp. 1695-1702, 2014.

[7] I. Árpád, Corrosion in technical diagnostics (Korrózió a műszaki diagnosztikában), Debrecen: Debreceni Egyetem Műszaki Kar, 2021.

[8] C. Bolla, Corrosion and corrosion protection (Korrózió és korrózióvédelem), Kolozsfár: Egyetemi Műhely Kiadó, 2009.

[9] T. Liptakova, V. Zatkalikova, A. Alaskari és M. Malcho, „Dominant factors affecting erosion-corrosion resistance of aluminum-brass pipelines," , The Journal of Engineering Research, %1. kötet7, %1. szám4, pp. 358-369, 2020.

[10] A. S. H. Makhlouf és M. A. Botello, „Failure of the metallic structures due to microbiologically induced corrosion and the techniques for protection," in Handbook of Materials Failure Analysis, Oxford, Butterworth-Heinemann, 2018, pp. 1-18.

[11] AUSTRAL WRIGHT METALS, „Copper Alloys Stress Corrosion Cracking – Austral Wright Metals," AUSTRAL WRIGHT METALS, [Online]. Available: https://www.australwright.com.au/technical-data/advice/copper-brass/copper-alloys-stress-corrosion-cracking/. [Hozzáférés dátuma: 5 10 2024].

[12] Khoshnaw, F.; Gubner, R.; , „Corrosion Topics," in Corrosion Atlas Series, Corrosion Atlas Case Studies, Cham, Elsevierí, 2020, pp. 43-68.

[13] H. Xu, T. Tian, B. Hua, W. Zhan, L. Niu, B. Han és Q. Zhang, „Effect of in-situ rolling and heat treatment on microstructure, mechanical and corrosion properties of wire-arc additively manufactured 316L stainless steel," Journal of Materials Research and Technology, %1. kötet27, %1. szám6, pp. 3349-3361, 2026.

[14] J. Bedmar, N. Abu-warda, S. García-Rodríguez, B. Torres és J. Rams, „Influence of the surface state on the corrosion behavior of the 316 L stainless steel manufactured by laser powder bed fusion," Corrosion Science, %1. kötet207, p. 110550, 2022.

[15] Y. Li, T. Xu, S. Wang, B. Fekete, J. Yang, J. Qiu, A. Xu, J. Wang, Y. Xu és D. D. Macdonald, „Modelling and Analysis of the Corrosion Characteristics of Ferritic-Martensitic Steels in Supercritical Water," Materials, %1. kötet12, %1. szám3, p. 409, 2019.

[16] D. S. Janikowski és W. Henricks, „Superferritic Stainless Steels –The Cost Effective Answer for Heat Transfer Tubing," in CORROSION 2008, New Orleans, 2008.

[17] R. Matsuhashi, S. Tsuge, Y. Tadokoro és T. Suzuki, „Estimation of Crevice Corrosion Life Time for Stainless Steels in Seawater Environments," NIPPON STEEL TECHNICAL REPORT, %1. kötet, összesen: %299-72, pp. 62-, 2010.
[18] P. Trampus, V. Krstelj és G. Nardoni, „NDT integrity engineering – A new discipline," Procedia Structural Integrity, %1. kötet17, pp. 262-267, 209.
[19] J. Janik, Machine maintenance II. (Gépüzemfenntartás II.), Dunaújváros: Főiskolai Kiadó, 2006.
[20] H. Khatak és B. Raj, Corrosion of Austenitic Stainless Steels - Mechanism, Mitigation and Monitoring, Sawston: Woodhead Publishing, 2002.
[21] L. Abosrra, A. F. Ashour, S. C. Mitchell és M. Youseffi, „Corrosion of mild steel and 316L austenitic stainless steel with different surface roughness in sodium chloride saline solutions," WIT Transactions on Engineering Sciences, %1. kötet65, pp. 161-172, 2009.
[22] J. Wang, H. Xue, Y. Zhao, T. Zhang és F. Wang, „Effect of Surface Roughness on the Corrosion of HP-13Cr Stainless Steel in the Dynamic Aggressive Oilfield Environment," Metals, %1. kötet14, %1. szám3, p. 280, 2024.
[23] A. Toloei, V. Stoilov és D. Northwood, „The Relationship Between Surface Roughness and Corrosion," in Proceedings of the ASME 2013 International Mechanical Engineering Congress & Exposition IMECE2013, San Diego, 2013.
[24] L. Garbai, A. Jasper és R. Sánta, „Optimization of the operation of existing district heating systems," International Review of Applied Sciences and Engineering, %1. kötet15, 1. szám2, pp. 189-198, 2024.
[25] C. Hetyei és R. Nagy, „Review of Wind Turbine Failures, Highlighting Fire Accidents," Műszaki Katonai Közlöny, %1. kötet30, %1. szám2, pp. 43-56, 2021.
[26] M. D. Giuseppe, Localized corrosion of stainless steels: effect of surface finishing, Milano: Politecnico Milano, 2018.
[27] M. Abdolhosseini és I. G. Ogunsanya, „Determining Factors Affecting Pitting Corrosion of Stainless Steel Reinforcing Bars," in Smart & Sustainable Infrastructure: Building a Greener Tomorrow, Cham, Springer, 2023.
[28] M. Dománkova, E. Kocsisová, I. Slatkovský és P. Pinke, „The microstructure evolution and its effect on corrosion properties of 18Cr-12Ni-2,5Mo steel annealed at 500–900°C," Acta Polytechnica Hungarica, %1. kötet11, %1. szám3, pp. 125-137, 2014.
[29] I. Barányi, „Characterization of Tribological Behaviour of Surface Topographies by Roughness Measurement at the Beginning of the Wear Process," Acta Technica Jaurinensis, %1. kötet13, %1. szám2, pp. 151-160, 2020.
[30] H. Alzyod és P. Ficzere, „Prediction of the Influence of Printing Parameters on the Residual Stress Using Numerical Simulation," System Safety Human - Technical Facility - Environment, %1. kötet4, %1. szám1, pp. 150-156, 2022.
[31] M. Schramkó, Z. Nyikes, L. Tóth és T. A. Kovács, „Investigation of the ultrasonic welded stainless steel corrosion resistance," Journal of Physics Conference Series, %1. kötet2315, %1. szám1, p. 012028, 2022.
[32] C. Hetyei és F. Szlivka, „Review of the Aerodynamical Load on a Dual-Rotor Wind Turbine's Blade," Biztonságtudományi Szemle, %1. kötet3, %1. szám1, pp. 91-108, 2021.

[33] C. Kollár és B. Nagy, „The uses of artificial intelligence in object recognition (part two) (A mesterséges intelligencia felhasználási lehetőségei az objektumfelismerésben (második rész)),” Biztonságtudományi szemle, %1. kötet3, %1. szám2, pp. 115-129, 2021.

[34] P. F. R. Trampus, Z. Kerner, M. Lakatos-Varsányi, P. László, M. Réger, P. J. Szabó, J. Telegdi és B. Verő, „Investigation of Local Corrosion Degradation Developed on a Pipeline System in Service Period,” Material Science Forum, %1. kötet885, pp. 92-97, 2017.

[35] L. R. Hilbert, D. Bagge-Ravn, J. Kold és L. Gram, „Infuence of surface roughness of stainless steel on microbial adhesion and corrosion resistance,” International Biodeterioration & Biodegradation, %1. kötet52, %1. szám3, pp. 175-185, 2003.

[36] L. Tóth, F. Haraszti és T. Kovács, „Surface Roughness Effect in the Case of Welded Stainless Steel Corrosion Resistance,” Acta Materialia Transylvanica , %1. kötet1, %1. szám1, pp. 53-56, 2018.

[37] „Arrhenius-egyenlet,” Wikipédia, [Online]. Available: https://hu.wikipedia.org/wiki/Arrhenius-egyenlet. [Hozzáférés dátuma: 6 11 2024].

DOI: https://doi.org/10.12700/btsz.2025.7.1.145

GLOBAL CHALLENGES IN CYBERSPACE: HUMAN RISK MANAGEMENT IN THE PROTECTION OF CRITICAL INFRASTRUCTURES

GLOBÁLIS KIHÍVÁSOK A KIBERTÉRBEN: HUMÁN KOCKÁZATOK KEZELÉSE A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉBEN

KÁRÁSZ Balázs[1]

Abstract

This paper examines the indirect impacts of global climate change on the functioning of society, and its effects in cyberspace, which are dominantly impacting on warfare and security policy in the 21st century. The focus of the research is on the protection of critical infrastructures, which are increasingly exposed to threats in cyberspace. When threats are complemented by internal vulnerabilities, both components of identifiable risk, impact and likelihood, can increase. Therefore, among the many pillars of protection, it is of paramount importance to prepare critical infrastructure workers by improving their information security awareness and preparedness. The paper explores the context for developing possible ways to manage these risks in a way that is appropriate to the organisational functioning of the critical infrastructure.

Keywords

climate change, critical infrastructure protection, cyberspace, risk management, information security awareness

Absztrakt

Jelen tanulmány a globális klímaváltozásnak a társadalom működésére közvetetten gyakorolt hatásai közül a 21. század hadviselését és biztonságpolitikáját nagymértékben befolyásoló kibertérben megvalósuló hatásait vizsgálja. A kutatás fókuszában a kritikus infrastruktúrák védelme áll, amelyek egyre növekvő számban kitettek a kibertérben megvalósuló fenyegetéseknek. Amennyiben a fenyegetéseket belső gyenge pontok egészítik ki, az azonosítható kockázatok mindkét komponense, a hatás és valószínűség egyaránt növekedhet. Ezért a védelem számos pillére közül kiemelkedő fontosságú a kritikus infrastruktúrák dolgozóinak felkészítése, információbiztonság-tudatosságuk és felkészültségük fejlesztése útján. A tanulmány feltárja azokat az összefüggéseket, amelyek alapján kidolgozhatók e kockázatok kezelésének lehetséges, az adott kritikus infrastruktúra szervezeti működéséhez illeszkedő módszerei.

Kulcsszavak

klímaváltozás, kritikus infrastruktúra védelem, kibertér, kockázatkezelés, információbiztonság-tudatosság

[1] karaszb@gmail.com | ORCID: 0000-0003-2065-4928 | Former PhD Student, National University of Public Service, Doctoral School of Military Engineering | Volt PhD hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

BEVEZETÉS ÉS A KUTATÁS RÉSZLETEI

Korunk társadalma globális kihívásokkal küzd, amelyek egyrészt a mindennapi élet bármely területén képesek jelentős hatást gyakorolni, másrészt kölcsönösen befolyásolják egymást, így a felmerülő külső fenyegetettségek és belső gyengeségek folyamatos változásban vannak. Az információbiztonsági törekvéseknek olyan társadalmi, jogi és digitális technológiai környezetben kell hatékonyan megvalósulniuk, mely egyre gyorsabb alkalmazkodást kíván az egyre komplexebbé váló helyzetekhez, folyamatokhoz.

Az információs társadalom tendenciái arra késztetik a szervezeteket, hogy könnyen elérhető és alkalmazható, naprakész eszközöket vegyenek igénybe az IT-biztonság, a fizikai biztonság, valamint a humán kockázatok kezelése terén (különösen a szervezetfejlesztés és a tudatosságra nevelés tekintetében). Az e célokat szolgáló eszköztár napjainkig folyamatosan bővül és minőségében is fejlődik, hiszen a fentiekből következően alkalmazkodni kénytelen az olyan, globális kihívások által jelentősen befolyásolt információs környezethez is, mint amilyet a 2020-as év járványügyi intézkedései közvetlenül és közvetetten teremtettek.

A kritikus infrastruktúrák, mint – többek közt – az energiaellátás, vízgazdálkodás, közlekedési hálózatok és egészségügyi rendszerek, valamint az egyre növekvő jelentőségű információs infrastruktúrák alapvető szerepet töltenek be a társadalmak működésében, illetve ahhoz egyenesen nélkülözhetetlenek, így védelmük nemcsak gazdasági, hanem biztonságpolitikai szempontból is kulcsfontosságú. Egy-egy létfontosságú rendszerelem kiesése súlyos társadalmi és gazdasági következményekkel járhat, ezért azok folyamatos védelme, fenntarthatóságuk biztosítása és az ellenállóképességük növelése kiemelt feladat az infrastruktúrákat üzemeltetők számára.

Tudományos probléma

Az előzőek fényében felmerül a kérdés, miként befolyásolják napjaink globális kihívásai a kritikus információs infrastruktúrák belső gyengeségeit és hogyan alakítják külső fenyegetettségeit abban a tekintetben is, hogy milyen kockázatkezelési módszerek állnak rendelkezésre a védelem minél magasabb szintű hatékony megvalósításában.

Kutatási cél

A kutatás célja, hogy rövid áttekintést nyújtson a kritikus információs infrastruktúrák mibenlétéről, valamint a 21. század globális kihívásairól, a kibertér aktuális trendjeiről. Ezt követően azonosításra kerülnek a kritikus információs infrastruktúrák főbb fenyegetései és gyengeségei a kiberkörnyezet aktualitásai tükrében. Végezetül a fókusz a humán kockázatok azonosítására, és az ezeket leghatékonyabban kezelő módszerekre, best practice-ekre tevődik.

Kutatási módszerek

A szerző elméleti és empirikus kutatási módszereket alkalmaz, részben a grounded theory eszközével. Kapcsolódó magyar és nemzetközi szakirodalom kerül feldolgozásra, a gyakorlati aspektus hozzáillesztéséhez szervezeti példákból születik inspiráció, összehasonlítást nyújtva egyúttal kritikus infrastruktúrát üzemeltető, és más jellegű szervezetek tulajdonságai között.

A 21. SZÁZAD GLOBÁLIS KIHÍVÁSAI

Jelen fejezetben bemutatásra kerülnek a kritikus (információs) infrastruktúrák, valamint korunk legjelentősebb globális kihívásai és ezek kölcsönhatásai közül azok, amelyek a kritikus infrastruktúrák működése tekintetében a legnagyobb kockázatot, és így megoldási utak kidolgozására váró problémákat jelentenek.

Kritikus infrastruktúrák

Jelen tanulmány a kritikus infrastruktúra és a létfontosságú rendszerelem kifejezést szinonimaként használja, előbbi a nemzetközi gyakorlatban használt terminológiának szó szerinti fordítása, míg utóbbi a magyar jogszabályokban alkalmazott terminus.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény létfontosságú rendszerelemként gazdasági ágazatok széles körének valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszerelemét, továbbá azok által nyújtott szolgáltatásokat határozza meg, „amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.” [1] Az érintett gazdasági ágazatok – melyek alágazatait a törvény tételesen is felsorolja – a következők: energia, közlekedés, agrárgazdaság, egészségügy, társadalombiztosítás, pénzügy, infokommunikációs technológiák, víz, honvédelem, közbiztonság-védelem.

Már 2005-ben megfogalmazásra került [2] a kritikus információs infrastruktúra fogalma, mely kifejezés alatt azokat az infokommunikációs rendszereket értjük, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.).

Klímaváltozás

A korábban számos fórumon megtalálható globális felmelegedés kifejezés helyett jelen tanulmány a globális klímaváltozást használja, mely átfogóbb, a valósághoz közelebbi és tudományos szempontból is elfogadott, semleges összefoglalását adja mindazon folyamatoknak, amelyek meghatározzák mindennapjainkat, kihatással vannak a politikai és társadalmi viszonyokra, a regionális éghajlat és lokális időjárás alakulására világszerte, a természeti katasztrófák előfordulásának gyakoriságára, és magára a klímaváltozásra adott eltérő reakciókra is.

A klímaváltozás a 21. század egyik legösszetettebb globális kihívása, amely nem csak a természeti környezetet érinti, hanem a társadalom működésére is hatást gyakorol. A szélsőséges időjárási jelenségek, az óceánok szintjének emelkedése és az akár emberéleteket követelő természeti katasztrófák olyan rendszerszintű változásokat idéznek elő, amelyek közvetlenül és közvetetten is hatnak az infrastruktúrákra, a gazdasági folyamatokra és a biztonságpolitikára. [3] Hozzá kell tenni, hogy a természeti katasztrófák által okozott károk növekvő költségei egyre nagyobb terhet rónak a nemzetgazdaságokra és a védelmi rendszerekre.

Trendek a kibertérben és a digitális világban

A digitális világ folyamatos fejlődése az elmúlt évtizedekben exponenciálisan növelte az adatok és hálózatok jelentőségét a társadalom és a gazdaság működésében. A telekommunikáció aktuális sarokköveként a 5G-hálózatok, a szintén hálózatos kommunikációra épülő IoT-eszközök és a mesterséges intelligencia elterjedése új lehetőségeket teremt, ugyanakkor ezekkel párhuzamosan a kibertérben megjelenő fenyegetések is egyre összetettebbé válnak. Az állami és nem állami szereplők által elkövetett kibertámadások száma is folyamatosan növekszik, de még fontosabb, hogy egyre inkább célba veszik az alapvető szolgáltatásokat biztosító rendszereket.

A kritikus infrastruktúrák elleni kibertámadások azért lehetnek különösen veszélyesek, mivel az üzemzavar vagy részleges, esetleg teljes leállás súlyos következményekkel járhat egy teljes ország vagy régió gazdaságára és biztonságára nézve, tekintve, hogy egyik infrastruktúra sem értelmezhető pusztán önmagában. Az ellátási láncok digitális sérülékenysége miatt a kibertérben történő incidensek nemcsak egy célba vett vállalatot, hanem teljes iparágakat is megbéníthatnak. A zsarolóvírusok, a social engineering technikák és az ún. fejlett folyamatos fenyegetések (APT-k) már a 2000-es évek elején olyan eszközökké váltak, amelyeket állami és bűnözői csoportok egyaránt alkalmaznak geopolitikai célok elérésére. [4]

Meghatározó szükséglet a kiberbiztonság szempontjából az ellenállóképesség növelése és a megelőző védelmi stratégiák fejlesztése. A mesterséges intelligencia és a gépi tanulás új lehetőségeket kínál a védelmi oldalon is, mégpedig a fenyegetések felismerésére és semlegesítésére, ugyanakkor a kapcsolódó etikai és jogi kérdések is egyre nagyobb figyelmet kapnak. A kiberbiztonsági tudatosság növelése a szervezetek minden szintjén alapvető fontosságú, hiszen a támadások jelentős része továbbra is emberi hibák kihasználásán alapul.

Új típusú koronavírus-járvány

A 2019 végén kirobbant és Magyarországon 2020 márciusa óta jelen lévő új típusú koronavírus-járvány számos társadalmi, gazdasági, ökológiai és politikai folyamat áttervezésére nyújtott lehetőséget, valamint némelyeket ezek közül kényszerpályára segített. Nem véletlen a pozitív hangvétel, ugyanis a nemzetközi szinten jelentős hatású járvány és a kapcsolódó válsághelyzet nem csupán negatív kontextusban értelmezhető. A következő három jelentősebb területen a jelen tanulmány témája vonatkozásában előre mutató folyamatok tapasztalhatók.

A szervezetek, köztük kritikus infrastruktúrát üzemeltető vállalatok szervezetei is munkaerő-szervezési problémákkal szembesültek. A társadalmi felelősségvállalás jegyében igyekeztek az elsődleges hangsúlyt a munkavállalóik és a kiszolgált ügyfelek egészségének megőrzésére helyezni. Kreativitás és megoldás-központú gondolkodás vált azonnal szükségessé ahhoz, hogy a gazdasági élet folytatódhasson, ugyanis a szervezetek működésének alapja a munkavállalók rendelkezésre állása. Különösen igaz ez a kritikus infrastruktúrákra, ahol más szervezetekhez képest összességében a leginkább jellemző a személyes jelenlétet igénylő munkakörök túlsúlya. Bevezetésre került a biztonságos távolságtartás ipari környezetben is, a más kontextusban hosszú távon is hasznosnak bizonyuló higiéniai előírások, egyes irodai munkakörökben pedig az otthoni munkavégzés.

Áthidalandó a kényszerűségből átgondolt munkaerő-szervezési problémákat, felgyorsult a digitalizáció számos szektorban. Az eddig kevésbé hatékonynak bizonyuló törekvések az ügyfélkiszolgálás digitalizálására, valamint a papíralapú adminisztráció volumenének drasztikus csökkentésére hirtelen lehetőségből kényszerűséggé váltak. A vezető testületei átstrukturálták a tervezett költségeket, mely jelenség negatív hozadékai ellenére is a digitalizációra, ehhez kapcsolódóan pedig az információbiztonságra szánt keret növekedésében mutatkozott régóta elvárt, kismértékben javuló tendencia. [5]

Nem utolsó sorban pedig kedvező folyamatok indultak el a klímaváltozás elleni harcban, mely részben köszönhető az ipari létesítmények mérséklődő termelési volumenének, részben az otthoni munkavégzés, kijárási korlátozások és lezárások, valamint az emberek fogyasztási és főként közlekedési hajlandóságának csökkenése által vezérelt alacsonyabb károsanyag-kibocsátásnak.

A KRITIKUS INFRASTRUKTÚRÁK KOCKÁZATAI

Jelen fejezet egy SWOT-analízishez hasonló megközelítésben elemzi a kritikus infrastruktúrák külső tényezők – folyamatok, eszközök, helyzetek – által jelentett fenyegetéseit, és a belső adottságok közül a gyengeségeket, amelyeknél fogva a működésüket veszélyeztető és a védelmi rendszereket próbára tevő hatások felmerülnek. Kiemelten fókuszba kerül továbbá néhány fontos, az adatfeldolgozással és a mesterséges intelligenciával kapcsolatban felmerülő kockázat.

Kritikus infrastruktúrák fenyegetései

A kritikus információs infrastruktúrák külső fenyegetettségei érkezhetnek a fizikai, és az információs vagy virtuális dimenzióból, ezek veszélyei hatást gyakorolhatnak az infrastruktúrák működésére közvetlen és közvetett módon egyaránt. A fizikai fenyegetések közül legjelentősebb hatással a természeti katasztrófák, ipari (technikai jellegű) katasztrófák, terrorizmus és fegyveres konfliktusok. [6]

Az információs dimenzióból érkező fenyegetések mögött ugyan különböző mértékben, de minden esetben megjelenik az emberi tényező, valamint valamilyen személyes, politikai, üzleti érdek. A kibertér már a legalapvetőbb, fizikai komponense jellegénél fogva is elősegíti az ilyen érdekek érvényesítését, ti. a hálózatba kapcsolt eszközök és rendszerek közötti kommunikáció segítségével szélesebb körben biztosított az átjárás, az információhoz való hozzáférés. [7]

A klímaváltozás következtében egyes térségekben romlik az élelmiszer- és vízellátás biztonsága, ami társadalmi feszültségekhez, migrációs hullámokhoz és geopolitikai instabilitáshoz vezethet. Ezek az instabilitási tényezők fokozzák az államok és a nemzetközi szervezetek biztonsági kockázatait, különösen az energia- és vízellátás sérülékenységének növekedése miatt. Az aszályok és árvizek gyakoribbá válása komoly kihívásokat jelent a mezőgazdaság számára, ami az ellátási láncokban is fennakadásokat eredményezhet. [8]

A klímaváltozás okozta társadalmi-gazdasági változások közvetve befolyásolják a kibertér biztonságát is. A klímakatasztrófák során az infrastruktúrák sérülékenyebbé válnak, és a kibertámadások egyre gyakrabban kihasználják az ilyen válsághelyzeteket. Az energiahálózatok és közműszolgáltatások védelme kritikus jelentőségű, mivel ezek célpontjai lehetnek állami és nem állami szereplők általi kibertámadásoknak. A természeti katasztrófák és az azok nyomán fellépő kiberfenyegetések együttesen új típusú biztonsági kihívásokat

eredményeznek. Ide értendő a Covid-19 járvány leküzdése jelentette eltolódott fókusz a védelmi intézkedések kárára, amely exponenciálisan növekvő számú kibertámadás kivitelezésének adott teret. [9]

A klímaváltozás hatására a kritikus infrastruktúrák egyre nagyobb terhelésnek vannak kitéve, hiszen az extrém időjárási körülmények, például hőhullámok vagy áradások, jelentősen befolyásolják működésüket. Egyre fontosabbá válik az infrastruktúrák alkalmazkodóképességének növelése és a rugalmas, ellenálló rendszerek kialakítása. [10] Ezzel párhuzamosan azonban a digitalizáció előretörése miatt a kibertérben megjelenő fenyegetések is növekednek, amelyek célkeresztjében gyakran éppen a kritikus infrastruktúrák állnak.

Kritikus infrastruktúrák gyengeségei

A kritikus infrastruktúrák védelmében kiemelt szerepe van a humán tényezőnek, hiszen az emberi mulasztások és a nem megfelelő információbiztonsági tudatosság jelentős kockázatokat hordoz. A védelem egyik kulcseleme az infrastruktúrát üzemeltető szakemberek folyamatos képzése, az információbiztonsági protokollok betartása és az új fenyegetések felismerésének képessége. Az automatizáció és a mesterséges intelligencia szerepe is egyre növekszik, azonban ezek sem helyettesíthetik az emberi felügyeletet és a megfelelő kockázatkezelési stratégiákat. [3]

A kritikus infrastruktúrák védelmének egyik jelentős belső gyengesége az elavult technológiai rendszerek jelenléte, amelyek nem felelnek meg a modern biztonsági követelményeknek. Számos ilyen infrastruktúra még mindig régi, gyakran évtizedes hardver- és szoftvermegoldásokra épül, amelyeket eredetileg nem a jelenlegi kiberfenyegetések kivédésére terveztek. Ezek a rendszerek gyakran nem kapnak rendszeres biztonsági frissítéseket, és sok esetben olyan sérülékenységeket tartalmaznak, amelyeket a támadók könnyen kihasználhatnak. Az elavult technológia nemcsak a támadásoknak teszi ki az infrastruktúrát, hanem megnehezíti a hatékony incidenskezelést és helyreállítást is. [11]

Egy másik kritikus belső gyengeség a nem megfelelő hálózati felosztás, együtt az elkülönítés hiányával. Sok kritikus infrastruktúrában az informatikai és ipari irányítási és automatizálási rendszerek közvetlenül vagy közvetett módon kapcsolódnak a nyilvános hálózatokhoz, ami növeli a támadások kockázatát. Ha egy rosszindulatú szereplő hozzáférést szerez egy kevésbé védett rendszerelemhez, az egész hálózat kompromittálódhat, mivel a támadó könnyedén továbbterjedhet a rendszeren belül. Az elégtelen hálózati elkülönítés lehetővé teszi, hogy a támadók gyorsan kihasználják az infrastruktúra gyenge pontjait, és akár teljes szolgáltatásokat bénítsanak meg.

A kritikus infrastruktúrák további gyenge pontja a nem megfelelő incidensészlelési és válaszadási képesség. Bár egyre több szervezet alkalmaz kiberbiztonsági monitoring rendszereket, ezek sok esetben nem képesek időben azonosítani a komplex, célzott támadásokat. Az automatizált biztonsági megoldások hiánya és a fenyegetések elemzésére szolgáló eszközök korlátozott kapacitása megnehezíti az anomáliák észlelését és a gyors beavatkozást. Ennek következményeként egy támadás hosszabb ideig észrevétlen maradhat, növelve a potenciális károkat és a helyreállítás költségeit. [12]

Adatelemzés, feldolgozás és a mesterséges intelligencia közreműködése

A környezetmonitorozó szenzorok és az általuk gyűjtött adatok feldolgozásáért felelős rendszerek kibertámadásokkal szembeni sebezhetősége komoly kockázatokat hordoz,

különösen akkor, ha az adatok manipulálása nem szándékolt, akár irányelvekkel szembemenő döntésekhez vezetnek. Ha egy támadó megváltoztatja vagy hamisítja az érzékelők által mért értékeket – például a levegőminőség, vízszennyezettség, hőmérséklet vagy radioaktivitás szintjét illetően –, a döntéshozók vagy a mesterséges intelligenciával kiegészített beavatkozó rendszerek téves következtetésekre juthatnak. Ennek következtében szükségtelen vagy elégtelen válaszlépések történhetnek, például egy ipari létesítmény indokolatlan leállítása vagy egy veszélyes helyzet figyelmen kívül hagyása. Ugyancsak megemlítendő e helyen, hogy az egyes infrastruktúrák nem értelmezhetők önmagukban, önálló rendszerként, szükséges az átfogó megközelítés a hasonló problémák megoldásában.

A kibertámadások által generált hibás adatok különösen veszélyesek lehetnek olyan rendszerek esetében, amelyekben automatikus vészhelyzeti intézkedések kerültek betáplálásra. Ha például egy fejlett árvízvédelmi rendszer szenzorjai meghamisított adatok alapján tévesen érzékelnek áradást, a gátak nem tervezett módon nyílhatnak ki, ami más területeken súlyos következményekkel járhat. Hasonlóképpen, ha egy erdőtüzeket monitorozó rendszer nem érzékeli időben a tüzet egy kibertámadás miatt, a tűzoltás késedelmet szenvedhet, ami súlyosabb károkat és nagyobb emberi áldozatokat eredményezhet. Az ilyen manipulációk kritikusak az ipari és katonai rendszerek vonatkozásában, ahol a hibás döntések stratégiai következményekkel is járhatnak.

A mesterséges intelligencia (AI) alapú döntéshozatali rendszerek különösen sebezhetők közvetett módon, az adatok szándékos torzításával, mivel ezek a modellek részben előre betáplált paraméterekre, részben pedig valós időben érkező adatokra támaszkodva működnek. [13] Ha egy támadó képes meghamisítani az AI tanítására vagy működésére szolgáló adatokat, az hosszú távon is negatívan befolyásolhatja a rendszer teljesítményét, ami nem csupán egyetlen döntést, hanem az egész döntéshozatali folyamatot, valamint a társadalom biztonságérzetét és a védelmi rendszerekkel szembeni bizalmát hosszú távon veszélyezteti. [14]

HUMÁN KOCKÁZATKEZELÉSI LÉPÉSEK

Jelen fejezetben a bemutatott összefüggésekre alapozva azonosításra kerülnek a kritikus infrastruktúrák gyengeségeiből adódó, a humán tényezővel összefüggésbe hozható kockázatainak hatékony menedzselésére szolgáló eszközök, az információbiztonság eszköztárának egy e célból meghatározott módon történő csoportosítása segítségével.

Humán kockázati tényezők kezelése

A kritikus információs infrastruktúrák védelme szempontjából kiemelten fontos a humán tényezőből eredő kockázatok csökkentése. A tanulmány a már korábban is használt „humán tényező” kifejezést annak a kérdéskörnek a leírására alkalmazza, hogy az emberi mulasztás, a figyelmetlenség, valamint a szándékos károkozás jelentős kockázatot jelenthet a rendszerek biztonságára nézve. Ennek megfelelően több olyan eszköz is létezik, amely segíthet minimalizálni az emberi tényezőből adódó sérülékenységeket. Öt kulcsfontosságú intézkedést mutatok be, amelyek hatékonyan járulhatnak hozzá a kockázatok kezeléséhez.

Az első legfontosabb eszköz a folyamatos képzés és a biztonságtudatosság növelése. A munkavállalók rendszeres kiberbiztonsági oktatásban való részesítése elengedhetetlen ahhoz, hogy felismerjék és megfelelően kezeljék a különböző fenyegetéseket. A szimulációs gyakorlatok, például az adathalász támadások elleni tréningek, hozzájárulnak ahhoz,

hogy a dolgozók megtanulják az ilyen próbálkozások kiszűrését. Ezen túlmenően, a szervezeteknek olyan belső kommunikációs stratégiákat kell kialakítaniuk, amelyek folyamatosan informálják az alkalmazottakat az aktuális fenyegetésekről és a legjobb védekezési gyakorlatokról. Az információs biztonság nem egyszeri feladat, hanem folyamatos fejlődést és alkalmazkodást igénylő folyamat, ezért az oktatásnak és az érzékenyítésnek hosszú távon is prioritást kell élveznie.

A második kulcsfontosságú lépés a szigorú hozzáférés-kezelési és jogosultságkezelési rendszer bevezetése. A legkisebb jogosultság elve alapján minden alkalmazottnak kizárólag azokhoz az adatokhoz és rendszerekhez kell hozzáférést biztosítani, amelyek munkájához elengedhetetlenek. A többlépcsős hitelesítés (MFA) kötelezővé tétele jelentősen növeli a védelmet az illetéktelen hozzáférések ellen, hiszen egyetlen ellopott jelszó nem elegendő a rendszerekbe való bejutáshoz. Emellett fontos a jogosultságok rendszeres felülvizsgálata, hogy időben észlelhetők és megszüntethetők legyenek a szükségtelen vagy elavult hozzáférések. Egy jól felépített hozzáférés-kezelési rendszer segít csökkenteni annak esélyét, hogy egy kompromittált fiók vagy egy rosszindulatú belső szereplő kárt okozzon az infrastruktúrában.

A harmadik lényeges elem a belső ellenőrzési és incidensfigyelési rendszerek kiépítése, a hálózaton gyanús tevékenységeket azonosítani képes eszközökkel, amelyek folyamatosan elemzik a felhasználók viselkedését, és riasztást generálnak, ha szokatlan vagy potenciálisan veszélyes műveleteket észlelnek. A rendszeres auditok és naplóelemzések lehetővé teszik a szervezetek számára, hogy időben felfedezzék az esetleges belső fenyegetéseket vagy szabályszegéseket. Egy hatékony incidensfigyelési rendszer nemcsak a megelőzést szolgálja, hanem lehetőséget ad a gyors reagálásra is, így minimalizálva a potenciális károkat.

Negyedikként elengedhetetlen egy erős biztonsági kultúra és felelősségi rendszer kialakítása. A szervezeteknek ösztönözniük kell a dolgozókat arra, hogy aktívan vegyenek részt a biztonsági intézkedések betartásában, például azáltal, hogy jelentik a gyanús eseményeket vagy betartják az előírásokat. A szabályszegések következményeit egyértelművé kell tenni, ugyanakkor a dolgozókat pozitív ösztönzőkkel is motiválni lehet a biztonságtudatos viselkedésre. A belépési és kilépési folyamatok szigorú szabályozása biztosítja, hogy a szervezet érzékeny adatai ne kerüljenek illetéktelen kezekbe. Egy erős biztonsági kultúra hosszú távon hozzájárul a szervezet ellenállóképességének növeléséhez és a humán tényezőből fakadó kockázatok csökkentéséhez.

Egy végső kulcsfontosságú eszköz lehet a válságkezelési és ún. incidensreakciós terv kidolgozása és rendszeres tesztelése, amely részletezi azokat a lépéseket, amelyeket egy kibertámadás vagy egy súlyos biztonsági esemény bekövetkeztekor kell megtenni. Ez magában foglalja az érintett rendszerek izolálását, a károk minimalizálását, az illetékes csapatok riasztását és a helyreállítási folyamatok beindítását. Egy jól kidolgozott válságkezelési terv lehetővé teszi a károk minimalizálását és az üzletmenet gyors helyreállítását egy esetleges támadás után.

Az terv azonban önmagában nem elegendő, hanem kiegészítendő rendszeres gyakorlatokkal és szimulációkkal ahhoz, hogy minden érintett tisztában legyen a teendőivel egy valós helyzetben. A tesztelések segítenek feltárni az esetleges hiányosságokat és finomhangolni a folyamatokat, mielőtt egy éles helyzetben kellene rájuk támaszkodni. Egy jól kidolgozott és kipróbált incidenskezelési stratégia nemcsak az emberi hibákból eredő problémák

enyhítésére alkalmas, hanem az olyan külső fenyegetésekre is gyorsabb és hatékonyabb választ ad, mint a kibertámadások vagy a belső adatlopások.

Eszközök klasszifikációja

A kritikus információs infrastruktúrák védelmében a humán tényező kockázatának csökkentésére alkalmazott eszközök három fő kategóriába sorolhatók: fizikai eszközök, logikai eszközök és adminisztratív eszközök. A humán tényezőből eredő kockázatok csökkentése érdekében a fizikai, logikai és adminisztratív eszközök kombinált alkalmazása jelentősen növeli a kritikus információs infrastruktúrák védelmét, és hozzájárul a szervezet biztonsági szintjének folyamatos fejlődéséhez. [15] Az alábbiakban az előzőekben jellemzett öt kulcsfontosságú eszközt ezeknek megfelelően csoportosítva mutatjuk be.

Az információbiztonsági képzés és tudatosságnövelés az adminisztratív eszközök közé tartozik, hiszen ezek elsősorban az emberi tényezőre fókuszálnak. Az alkalmazottak rendszeres képzése segít megelőzni az olyan gyakori támadásokat, mint az adathalászat vagy a social engineering. Egy szervezet biztonsága nagyban múlik azon, hogyan tudja biztosítani, hogy az alkalmazottak képesek legyenek naprakész módon felismerni és elkerülni a potenciális fenyegetéseket.

A szigorú hozzáférés-kezelési és jogosultságkezelési rendszer részben fizikai, részben logikai eszközöket igényel. Az adatközpontokhoz, szervertermekhez és egyéb érzékeny helyiségekhez való hozzáférést fizikai biztonsági eszközökkel, például beléptető rendszerekkel, biometrikus azonosítókkal vagy intelligens belépőkártyákkal lehet szabályozni. A hozzáférési jogosultságokat nemcsak digitálisan kell felülvizsgálni, hanem a fizikai belépési jogosultságokat is rendszeresen ellenőrizni kell, különösen a távozó alkalmazottak vagy partnerek esetében.

A belső ellenőrzési és incidensfigyelési rendszerek a logikai eszközök kategóriájába tartoznak, hiszen ezek olyan szoftveres megoldásokat jelentenek, amelyek a felhasználói viselkedést és a rendszereseményeket figyelik: például elemzik a hálózat forgalmát, keresve a gyanús tevékenységeket, például a szokatlan bejelentkezéseket vagy az érzékeny adatok tömeges letöltését.

Az erős biztonsági kultúra és felelősségi rendszer kialakítása szintén adminisztratív eszköznek tekinthető. Ez nemcsak azt jelenti, hogy a szervezetnek szigorú szabályokat kell lefektetnie, hanem azt is, hogy ezek betartását folyamatosan ellenőrizni és ösztönözni kell. A biztonsági szabályszegéseknek következményei kell, hogy legyenek, ugyanakkor fontos a pozitív ösztönzés is, például a biztonságtudatos magatartás jutalmazása. Egy jól kialakított biztonsági kultúra hosszú távon hozzájárul a szervezet ellenállóképességének növeléséhez és csökkenti az emberi tényezőből fakadó kockázatokat.

Végül, a válságkezelési és incidensreakciós terv kidolgozása és tesztelése egy másik kulcsfontosságú adminisztratív eszköz, megfelelő dokumentáció és rendszeres frissítés kapcsolódik hozzá. Elengedhetetlen az érintettek folyamatos felkészítése a szimulációs gyakorlatokkal, ennek megszervezése erősíti az adminisztratív jelleget.

ÖSSZEGZÉS

A tanulmány rövid áttekintést nyújt a kritikus információs infrastruktúrákról, azonosítva főbb fenyegetéseiket és gyengeségeiket a 21. század globális kihívásainak, különösen a kibertér aktuális trendjeinek tükrében. A fókusz a humán kockázatok bemutatására,

valamint az ezeket leghatékonyabb módon kezelő módszerekre, szervezeti legjobb gyakorlatokra tevődik. Az e körbe tartozó eszközök, folyamatok és módszerek végezetül az információbiztonság eszköztárának egy meghatározott szempontjából csoportosításra kerülnek. Ez az áttekintés és elemzés feltárja a lehetőséget, hogy a kritikus információs infrastruktúrákat egymással kölcsönhatásban, a tágabb társadalombiztonsági összefüggések fényében értelmezhessék a humán kockázatokat górcső alá vevő további biztonságtudományi kutatások.

FELHASZNÁLT IRODALOM

[1] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://njt.hu/jogszabaly/2012-166-00-00.12 (Elérés: 2025.02.14.)

[2] Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról. (Előterjesztette a Bizottság). Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17.

[3] Bleszity J., et al., "Műszaki kutatások és hatékony kormányzás." *Hadmérnök* vol. 11. no. 3, 2016, pp. 221-242.

[4] Németh Z., Völgyi Z. "A kritikus információs infrastruktúra védelem pszichológiai szempontú megközelítése: Humán biztonsági kockázatelemzés", *Hadtudományi Szemle* vol. 11, no. 3, 2018, pp. 324-337.

[5] Jenei Sz., Módosné Szalai Sz. "A digitális átalakulás és a koronavírus járvány hatásai a munkaerőpiacon." *Új Munkaügyi Szemle* vol. 3, no. 2, 2022, pp. 2-12.

[6] Muha L., *A kritikus információs infrastruktúrák védelme*, Budapest: RelNet, 2015

[7] Haig Zs., *Információs műveletek a kibertérben*, Budapest: Dialóg Campus, 2018

[8] Földi L., "A klímaváltozás által jelentkező új kihívások a kritikus infrastruktúra védelmében." in: *Báthy Sándor [et al.], Ed., Fejezetek a kritikus infrastruktúra védelemből: Kiemelten a közlekedési alrendszer.,* Budapest: Magyar Hadtudományi Társaság, 2013, pp. 268-280.

[9] J. Chigada, R. Madzinga, „Cyberattacks and threats during COVID-19: A systematic literature review.” *South African Journal of Information Management*, vol. 23, no. 1, 2021, pp. 1-11. doi: 10.4102/sajim.v23i1.1277

[10] Horváth A., „A kritikus infrastruktúra védelem komplex értelmezésének szükségessége.” in: *Horváth A., Ed.: Fejezetek a kritikus infrastruktúra védelemből–Kiemelten a közlekedési alrendszer,* Magyar Hadtudományi Társaság, Budapest, 2013, pp. 18-37.

[11] Kralovánszky K., „A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész).” *Nemzetbiztonsági Szemle (Online),* vol. 7, no. 3, 2019, pp. 40-57, doi: 10.32561/nsz.2019.3.4 (Elérés: 2025.02.14.)

[12] Nagy R., "A klímaváltozás hatása a kritikus infrastruktúrák védelmére." *Nemzet és Biztonság, Biztonságpolitikai Szemle,* vol. 3, no. 2, 2010

[13] Kollár Cs., „A mesterséges intelligencia kapcsolata a humán biztonsággal” *Nemzetbiztonsági Szemle (Online)* vol. 6, no. 1, 2018, pp. 5-23, https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1508 (Elérés: 2025.02.14.)

[14] Kollár Cs., „A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában” In: Rajnai Z., Ed., *Kiberbiztonság – Cybersecurity 2.*,

Budapest, Magyarország: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2019, pp. 47-61.

[15] Kárász B., „Analysis Possibilities of the Toolset of Information Security.” *Biztonságtudományi Szemle,* vol. 7, no. 1, 2025

DOI: https://doi.org/10.12700/btsz.2025.7.1.157

SOME THOUGHTS ON HOW TO MEASURE THE PERFORMANCE OF FACILITY MANAGEMENT SERVICES

A LÉTESÍTMÉNYGAZDÁLKODÁSI SZOLGÁLTATÁSOK TELJESÍTMÉNYE MÉRÉSÉNEK EGYES PROBLÉMÁI

CZERNY József[1]

Abstract

This document discusses the challenges and methods of measuring the performance of facility management services, emphasizing the need for clear and standardized approaches. It highlights the importance of measuring services in a post-industrial society where services dominate production. The main focus is on internal organizational services like cleaning and security. There is a vast literature on service measurement, but few methods are widely adopted in practice. The subjective nature of service quality assessment poses a significant challenge. Internal organizational services often lack clear rules, leading to individual negotiations and exaggerated demands. This highlights the need for standardized processes. The study outlines various methods for measuring service quality, emphasizing the need to assess both the delivered service quality and customer satisfaction. Service performance should be assessed using factors like compliance, cost, quality, quantity, and timeliness. Large sample sizes are often needed for accurate measurement.

Keywords

facility management, service management, service quality, measurement of service quality

Absztrakt

Posztindusztriális társadalomban élünk, az előállított javak meghatározó része szolgáltatás. A tanulmányban a szolgáltatások egy bizonyos részével, a létesítménygazdálkodási szolgáltatásokkal és azok mérésének kérdéskörével foglalkozunk. A szolgáltatások mérésének, minősítésének igen kiterjedt irodalma létezik, azon-ban az irodalom által feltárt módszerek közül viszonylag kevés került át az általános gyakorlatba. Az az igen elterjedt vélekedés, hogy szolgáltatásminőség értékelése mindig szubjektív, komoly kihívást jelent. A szolgáltatás minőségét két egymással nem közvetlenül összefüggő nézőpontból kell vizsgálni: a leszállított, fogadott szolgáltatás minőségét, valamint a szolgáltatással való elégedettséget egyaránt mérni kell. A szolgáltatások teljesítményének mérésénél kiterjedt szabványháttérre támaszkodhatunk. A szolgáltatások mérésére fel kell készülni, erre világos útmutatás ad a tanulmány. Számolni kell azzal is, hogy a megbízható méréshez gyakran nagy mintanagyságra van szükség.

Kulcsszavak

szolgáltatás, létesítménygazdálkodás, minőség, mérés, minőségbiztosítás

[1] czerny@mti.bme.hu | ORCID: 0009-0002-7113-4332 | course leader, instructor, BME Institute of Continuing Engineering Education | oktató, tanfolyamvezető, BME Mérnöktovábbképző Intézet | tanfolyamvezető, BME Mérnöktovábbképző Intézet

BEVEZETÉS

Posztindusztriális társadalomban élünk, az előállított javak meghatározó része szolgáltatás. Ebben a tanulmányban a szolgáltatások egy bizonyos körével, a létesítménygazdálkodási szolgáltatásokkal és azok mérésével foglalkozunk.

A szolgáltatások mérésének, minősítésének igen kiterjedt irodalma létezik, azonban az irodalom által feltárt módszerek közül viszonylag kevés került át az általános gyakorlatba. A közvélekedésben elterjedt, és ide tartozik a szakmai közvélekedés is, hogy a szolgáltatások megítélése szubjektív, azaz minőségük mérése szorosan az azt végző egyénhez kapcsolódik. E sorok írója élénken emlékszik arra, hogy a 2000-es évek elején egy győri nagyvállalatnál mekkora derültséget váltott ki, amikor arról beszélt, hogy a takarítási szolgáltatások minőségét mérni kell, a mérési eredményeket visszakereshetően dokumentálni kell és a mért eredményhez kell kapcsolni a szolgáltatás díjazását. Azóta ez a helyzet némiképp javult, de messze nem annyira, mint az kívánatos volna. Ez azért is elgondolkodtató, mert a példánál maradva, a takarítási szolgáltatások minőségmérési rendszereire 2001 óta létezik európai szabvány. [6]

A Science-ben 1968-ban jelent meg Garett Hardin cikke a "The Tragedy of the Commons"[2], a cikk címe magyarul leginkább "A közös legelők tragédiája" –ként fordítható le. A Hardin által, többek között, felhozott példa így szól:

Egy falunak van egy közös legelője (ez valamikor nálunk is szokásos volt), amelyen a falu teheneit legeltetik. Tehenet tartani drága dolog, a tehén értékes jószág, így egyszer az egyik gazda azt gondolja, hogy ha kihajt még egy tehenet, szép haszonra tehet szert, és nem okoz kárt senkinek. Látva ezt a többi gazda, azt gondolják, ha ő megtehette, megtesszük mi is, és kihajtanak még teheneket. A dolog vége az, hogy a legelőn az egyéni döntések alapján több száz tehén kezd legelészni, a legelő tönkremegy, és valamennyi tehén éhen vész.

A cikket „Az emberi természet: Humánetológia" című könyvében [1] idéző Csányi Vilmos konklúziója az, hogy az egyéni mérlegelés, döntés teljesen összhangban van a környezeti, ökológiai feltételekkel akkor, ha nem közös tulajdonról van szó. Csányi Vilmos azt írja, hogy az emberek

„*bizonyos problémái csak külső kényszerekkel, olyan ideákkal oldhatók meg, amelyeket speciálisan az adott probléma megoldására hoztak létre. Ez azért tűnik fontos követelménynek, mert az emberiség többsége biztos abban, hogy amiben eddigi élete során hitt, azok az ideák, amelyek addig szabályozták az életét azok a jók, az igazak, és senkinek sincs joga azokon változtatni. Egyébként ez a hiedelem maga is egy ilyen idea.*"

A fenti gondolatment vezet el a szervezetek belső szolgáltatásainak problémaköréhez, ilyen a szervezeti működés során az említett takarítás is, de természetesen a biztonsági szolgáltatások is ide tartoznak. Igen sokszor a területek és így az épületek, amelyekhez kivétel nélkül minden belső szolgáltatás kapcsolódik, egyfajta közös, osztatlan javakat jelentenek, amelyeket mindenki használ és amelyekből mindenki a lehető legnagyobb részt

[2] Garrett Hardin, Science, 162(1968):1243-1248. Ez az egyik talán legtöbbet idézett tanulmány. Az utóbbi időkben Hardin munkásságát komoly kritikák érték, magát az idézett tanulmányt is. A köznapi tapasztalat azonban sokszor igazolja az emberi természet idézett tulajdonságait.

akarja kikanyarítani magának, képletes és valóságos értelemben véve egyaránt. Igen sokszor hiányoznak azok a szabályok, amelyek előírják, ki és hogyan részesedhet ezekből a „közös" javakból.

Világos, mindenki által elfogadott szabályok hiányában az igényeket egyéni alkuk során bírálják el és aki elsőnek „hajtja ki a tehenét" előnybe kerülhet. Mindenki igyekszik tehát eltúlozni az igényeit, számítva arra, hogy nem sikerül mindent jóváhagyatnia.

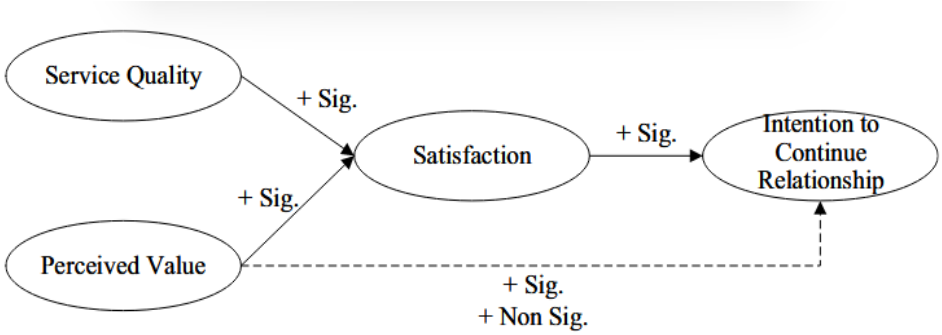
Az idézett gondolatmenetet követve belátható, hogy szervezeti környezetben a szolgáltatások mérésére való hajlandóság szorosan összefügg a szervezeti működéssel, azaz az általánosan elfogadott szervezeti folyamatokkal. Ebben a tanulmányban arra teszünk kísérletet, hogy egyrészt rávilágítsunk a szolgáltatások mérése problémáira, másrészt megmutassuk a lehetséges megoldások útját, korlátozva vizsgálatainkat a szervezeti, vállalati, nagyvállalati belső szolgáltatásokra [12] [13].

Az elmélet és a napi gyakorlat összekapcsolásában döntő ismeretforrást jelentettek a BME Mérnöktovábbképző Intézetben huszonöt éve folyó létesítménygazdálkodási továbbképző tanfolyamon végzett elemzési gyakorlatok [10].

A SZOLGÁLTATÁSOK MÉRÉSÉNEK PROBLÉMÁI

A szolgáltatások mérésére számtalan módszer létezik, amelyekről a szakirodalom bőséges eligazítást nyújt. [7], [8], [9].

Az alapproblémát legjobban az alábbi ábra szemlélteti:



1. A Systematic literature review using PRISMA [7] 2. ábrája alapján

Az idézett ábra bal oldala jól mutatja a szolgáltatások minősítésének kettősségét, azaz a szolgáltatás minőségét mindig két egymással nem közvetlenül összefüggő nézőpontból kell vizsgálni:

- a leszállított, fogadott szolgáltatás minőségét, valamint
- a szolgáltatással való elégedettséget egyaránt mérni kell.

Sem a leszállított minőség, sem a szolgáltatással való elégedettség sem eléggé kifejező önmagában. A szakmai közvélekedés szinte kizárólag ez utóbbi tekinti szükségesnek [10], holott egy nagyon egyszerű példa alapján belátható, hogy ez nem így van.

Tegyük fel, hogy a vállalati ebédlőben kelkáposztafőzeléket szolgálnak fel. Azt is tegyük fel, hogy a kelkáposztafőzelék minőségét objektív eszközökkel mérik és a méréseket dokumentálják (általában nem így van). Nyilvánvaló, hogy aki nem szereti a kelkáposztafőzeléket, az azzal mindig elégedetlen lesz, függetlenül annak mért minőségétől. Ez az 1.

ábrán feltüntetett „Perceived Value” jelentősége, amit legjobban talán minőségérzetnek nevezhetnénk. A minőségérzet (a vevői elégedettség) jelentősége alapvető, de a közvélekedéssel ellentétben [10] önmagában nem kifejező, csak a szolgáltatás mért és dokumentált minőségével együtt kiértékelve, azaz e kettőt összevetve tudhatjuk meg, hogy mivel is volt a szolgáltatást fogadó elégedett vagy elégedetlen és mennyire.

A LÉTESÍTMÉNYGAZDÁLKODÁS FOGALMA

Mint írtuk, a szolgáltatások igen széles köréből egy belső szervezeti szolgáltatási körre szűkítettük le a vizsgálódásainkat, a létesítménygazdálkodási szolgáltatások körére. A létesítménygazdálkodást tekintve számtalan eltérő értelmezéssel találkozunk. Az eredeti kifejezés a „facility management” vagy „facilities management” eredete is homályos, sok különböző magyarázat létezik.

Valószínűsíthető, hogy a kifejezés a 80-as évek során jött létre az Egyesült Államokban. A 2000-es évek elején elindult először nemzeti, majd európai szabványosítás hozott létre először egységes definíciót. Ezt követte az ISO szabványok kidolgozása, amelyek egy része magyarul is megjelent. A szabványháttérre a következő pontban térünk ki részletesen.

A létesítménygazdálkodás fogalma [2] alapján:

Szervezeti funkció, amely integrálja az embereket, a helyet és a folyamatot az épített környezeten belül, az emberek életminőségének és a fő tevékenység termelékenységének javítása céljából. A létesítménygazdálkodás feladata **a szervezeten belül a munkahely és a munkavégzés szükségleteihez kapcsolódó belső szolgáltatások** iránti kereslet és kínálat irányítása a szervezet stratégiájának figyelembe vételével.

Egy szervezet létesítménygazdálkodási funkciója nyújtja a főtevékenységnek mindazon olyan szolgáltatásokat, amelyek szükségesek ahhoz, hogy maga a szervezet működőképes maradjon. Ez köznapi nyelve lefordítva azt jelenti, hogy minden szervezetnek van létesítménygazdálkodása, akár tudják, akár nem. Sok esetben másképp hívják, van, hogy az egyes ide tartozó szervezeti funkciók szétszórtak, nincs egységes irányításuk. Az oktatási tapasztalatok alapján [10] ritka az olyan szervezet, amelynél pontosan tisztában vannak ennek a szervezeti funkciónak a jelentőségével és még ritkább, amelynél minden érintett számára világos szabályzatok tartalmaznák a követelményeket és az eljárási módokat. Igen gyakori, hogy a szervezeti funkció összemosódik az általa nyújtott szolgáltatásokkal.

A SZABVÁNYHÁTTÉR

Mint már említettük, a létesítménygazdálkodás szabványosítása jó 25 évre nyúlik vissza. A szabványosítás a CEN, az európai szabványosítással vette kezdetét, amelyet két nemzeti szabványosítási kezdeményezés is megelőzött. A CEN létesítménygazdálkodási szabványosítás két alapvető nemzeti szabványból indult ki a 2000-es évek elején:

- NEN 2748: Ez a holland szabvány a létesítménygazdálkodás terminológiáját és definícióit tartalmazta.
- BS 8536: Ez a brit szabvány a létesítménygazdálkodás szerződéseinek és szolgáltatásainak irányelveit határozta meg.

Ezek a szabványok szolgáltak alapul a CEN létesítménygazdálkodási szabványosítás további fejlesztéséhez és bővítéséhez.

A 2010-es évek elején, számos kidolgozott és bevezetett CEN szabvány után került sor az elkészült szabványok ISO szintre emelésére és az elkészülő ISO szabványok után a megfelelő CEN szabványok visszavonására ill. az ISO szabványok átvételére CEN szabványként. A [2], [3], [4], példa élő ISO CEN szabványokra, [5] egy ma is hatályos CEN szintű szabványra, míg [6] egy önálló szolgáltatási CEN szabványra.

A SZOLGÁLTATÁSOK MINŐSÉGE

Minden szolgáltatás, így bármely létesítménygazdálkodási szolgáltatás is mindig egy termelési folyamat eredménye. Ez azt is jelenti, hogy a termelő folyamatokban megszokott és bevett módszereket lehet a szolgáltatások minőségbiztosításánál használni, természetesen megfelelően alkalmazva, azaz a szolgáltatások eredményességét, minőségét és a követelményeknek való megfelelését is mérni és dokumentálni kell.

A szolgáltatás teljesítményének megítélése során öt fő tényezőt érdemes vizsgálni, amikor erre lehetőség van:

- A hatósági, törvényi, szabvány és a szervezet belső előírásainak való megfelelést (Compliance)
- A szolgáltatás költségét (Cost)
- A szolgáltatás minőségét (Quality)
- A leszállított szolgáltatások mennyiségi megfelelését (Quantity)
- Az időbeli teljesítés megfelelőségét (Timeliness)

A szolgáltatásokat általában nagyminta-vételezéssel kell ellenőrizni, kivételt képezhetnek egyes szervezetileg kritikus szolgáltatások, amelyeket tételesen, azaz 100%-os mintán kell és sokszor hatóságilag kötelező is ellenőrizni. Ilyenek például a tisztaterek takarítása, műtők, élelmiszer feldolgozó terek fertőtlenítése többek között.

Az ellenőrzéshez az egyes szolgáltatásokra szolgáltatási szint megállapodásokat kell kidolgozni. [4]

A szolgáltatások két nagy csoportba lehet besorolni a szolgáltatás típusa és a szolgáltatás tervezhetősége szerint:

- A tervezhetőség szerint tervezetten nyújtott szolgáltatások és igény esetén nyújtott szolgáltatások
- A szolgáltatás típusa szerinti megelőző szolgáltatások és eredményorientált szolgáltatások.

A tervezetten nyújtott szolgáltatások azok a szolgáltatások, amelyek iránti igényt minden esetben előre lehet látni és a szolgáltatás nyújtását (a szolgáltatások termelését) ütemezni lehet. Ilyen tervezetten nyújtott szolgáltatások pl. a megelőző karbantartási szolgáltatások, takarítási szolgáltatások többsége, a biztonsági szolgáltatások döntő része.

Az igény esetén nyújtott szolgáltatások azok, amelyek nyújtásának időpontja iránti igényt többnyire nem lehet előre látni. Az igény esetén nyújtott szolgáltatásoknál a reagálási idő (azaz a szolgáltatás megkezdéséig és befejezéséig eltelt idő) fontos, sokszor döntő szerepet játszik.

A megelőző szolgáltatások esetén valamilyen jövőbeli esemény megtörténtét akarjuk megakadályozni, például, hogy valamely berendezés meghibásodjon vagy valamilyen esemény megtörténjen. Természetesen minden törekvésünk ellenére előbb utóbb minden meghibásodik vagy megtörténik valami, amit nem szeretnénk. Az ilyen szolgáltatások célja, hogy ezen események bekövetkezésének valószínűségét csökkentsék és ennek érdekében végrehajtandó műveletek sorát írjuk elő, lásd karbantartási utasítások, őrutasítás, hatósági előírások stb.

Az eredményorientált szolgáltatások mindig valamilyen állapot helyreállítását szolgálják és azokat az állapot vizsgálatával mérjük. Erre a legjobb példa a takarítás, amikor egy végeredményt várunk el, tiszta legyen valami, és ekkor ennek a végeredménynek az elérését mérjük,

A négy szolgáltatási típus összefüggéseit és néhány példát a szolgáltatásokra a 2. táblázatban tüntettünk fel.

	Megelőző szolgáltatások	Eredményorientált szolgáltatások
Tervezetten nyújtott szolgáltatások	biztonsági szolgáltatások, megelőző karbantartás	takarítás
Igény esetén nyújtott szolgáltatások	*nem jellemző*	hibaelhárítás

2. Példák szolgáltatási típusokra

A megelőző szolgáltatások és az eredményorientált szolgáltatások a gyakorlatban sokszor összemosódnak [10]. Igen gyakran az eredményorientált szolgáltatásoknál is műveletsorokat írnak elő, nagyon jellemző ez a takarításnál, amikor ellenőrizni és minősíteni azokat csak a végeredménnyel lehet.

Fontos fogalom a szolgáltatási esemény, amelyet a szakirodalom és a gyakorlat egyaránt sokféleképpen nevez meg. A legtöbb szolgáltatás szolgáltatáscsoport. Ilyenek például a biztonságtechnikai szolgáltatások, amelyeket nem véletlenül használunk többes számban, mivel számtalan külön-külön szolgáltatásból állnak össze, de ugyanígy ilyen a takarítás is, ami szintén egy szolgáltatáscsoport, és ezért fontos a szolgáltatási esemény fogalma.

A szolgáltatási esemény az az elemi szolgáltatás, amit jól körül határolhatóan nyújtottak, amit már nem bontunk fel részekre és amelyeket minőségét közvetlenül mérni akarjuk. Legjobban példákon keresztül lehet megvilágítanunk. Takarításnál többnyire egy jól körül határolt terület tisztaságára vagyunk kíváncsiak, ilyen például egy helyiség, azaz helyiségek tisztaságát minősítjük. Megelőző karbantartási szolgáltatásoknál egy-egy berendezés vagy berendezéscsoport karbantartását minősítjük. Ezek a szolgáltatási események képezik majd annak a halmaznak az elemeit, amelyen a mintavételezéses ellenőrzést elvégezzük. Ez a módszer ipari környezetben bevett, sőt kötelezően előírják szerződések és többnyire jól működik, gondoljunk itt a repülőgépek karbantartására vagy a felvonóberendezés karbantartásának hatósági szabályozására.

A leszállított szolgáltatásokat, minőségileg és mennyiségileg egyaránt ellenőrizni kell. Sokszor az igen nagyszámú szolgáltatási esemény miatt a teljes körű, azaz minden egyes szolgáltatási eseményre kiterjedő ellenőrzés igen nagy munkával járna, költsége a

legtöbb esetben összemérhető lenne magának a szolgáltatásnak a költségével. Vannak olyan szolgáltatások, amelyeknél ez indokolt, ezek a szervezetileg kritikus szolgáltatások, amelyeknél a szolgáltatás kimaradásával vagy rossz minőségével okozott kár akkora, hogy sokszor eltörpül a szolgáltatások tételes ellenőrzése még oly nagy költsége mellett. A létesítménygazdálkodási szolgáltatásoknál azok jellege miatt ilyen ellenőrzésre legtöbb esetben sem lehetőség, sem szükség nincs, ezért a szolgáltatások minőségi és mennyiségi teljesítését nagymintán kell elvégezni.

Az alábbi táblázat tartalmazza a tételek számától függő megkívánt minimális mintanagyságokat.

A tétel nagysága	1. fokozat	2.fokozat	3.fokozat
2 -8	2	2	3
9 - 15	2	3	5
16 - 25	3	5	8
26 - 50	5	8	13
51 - 90	5	13	20
91 - 150	8	20	32
151 - 280	13	32	50
281 - 500	20	50	80
501 - 1200	32	80	125
1201 - 3200	50	125	200
3201 - 10000	80	200	315
10001 - 35000	125	315	500
35001 - 150000	200	500	800
150001 - 500000	315	800	1250
500001 - végtelen	500	1250	2000

3. Az MSZ EN 13549 szabvány C1 táblázata.

A táblázat értelmezése:

- A tétel jelentése a vizsgált szolgáltatási események száma, például egy adott időszak alatt (ez általában egy hónap) az azonos típusú biztonsági berendezéseken elvégezett azonos karbantartási munka, felbontva azokat egyes munkafázisokra.
- A mintanagyság jelentése az összes szolgáltatási esemény közül hányat kell legalább ellenőrizni, hogy a kapott eredmény jellemző legyen a teljes halmazra, azaz az összes szolgáltatási eseményre.

Az összes szolgáltatási eseményből, a tételből, a mintákat véletlenszerűen kell meghatározni. Ennek előfeltétele, hogy valamennyi szolgáltatási esemény egyedileg kell, hogy

azonosítható legyen. Ez megelőző karbantartásnál lehet maga a berendezés. Az egy csoportba tartozó berendezéseket egyedi azonosítóval kell ellátni. Ez utóbbi egyre inkább teljesül is a gyakorlatban.

A SZOLGÁLTATÁSOK MINŐSÉGE ÉS AZ ADATOK

A szolgáltatások mérése, minőségbiztosítása során óriási mennyiségű adat keletkezik és többnyire vész el nyomtalanul. Kövessük ezt nyomon egy egyszerű példán.

A 4. táblázatban példaképpen az őrszemélyzettel kapcsolatos alaki, megjelenési követelmények foglaltuk össze és ezekre mutatunk lehetséges ellenőrzési módszert. Az alaki követelmények teljesítése is szolgáltatás, és igen fontos a teljes szolgáltatás megítélése szempontjából (1. ábra – *Perceived Value*)

A jobb oldali oszlop megadja az adható minőségi kategóriákat. Ha kategóriában (0,2) szerepel, akkor a szolgáltatás ezen eleme kritikus és ha a kritikus elemek közül akárcsak egy is nem teljesül, a teljes szolgáltatás hibás, azaz az őrt ki kell vonni a szolgálatból. A (0,1,2) azt jelzi, hogy lehet egy közbenső minősítés is, azaz „1”, ami elégségest jelent.

Jellemző példa, hogy egyszerre jóval több mit húsz őr teljesít szolgálatot, legyen az őrök száma = 24. Az őröket naponta ellenőrizzük mintavételezéssel és havonta szeretnénk minősíteni a szolgáltatást. Az őrszolgálat minden nap két műszakban működik, azaz 24 x 30 x 2 = 1440 szolgáltatási esemény van havonta, ez a tétel nagysága. A 3. sz. táblázat szerint 1. fokozatú ellenőrzéssel 50 ellenőrzést kell végeznünk. Összesen 60 műszak van, azaz, ha műszakonként egy-egy véletlenszerű ellenőrzést végzünk el és ezeket megfelelően dokumentáljuk [3], eleget teszünk a legalapvetőbb minőségbiztosítási követelményeknek.

Követelmény	**Megítélés, adható pont (0,1,2)**
Az ellenőrzés idejére kirendelt helyettesítő őr a megadott időn belül megérkezett	0, 2
Az őr a szolgálati helyén van, vagy szolgálati okokból indokoltan távozott	0, 2
Az őr nem fogyasztott szeszesitalt, ill. nincs más okból sem bódult állapotban	0, 2
Az őr ruházata megfelel az előírásoknak	0,1,2
Jól láthatóan viseli a személyi azonosítóját	0, 2
Valamennyi kötelezően előírt okmány az őrnél: sz.ig, vagyonőri ig, kamarai ig.	0, 2
Az őr személyi higiéniája megfelelő, borotvált vagy szakálla ápolt, tetoválása nem látható és más módon sem kelt ápolatlan benyomást	0,1,2

4. Az őrszolgálat alaki követelményei

Magyarázat az első ellenőrzési ponthoz *„Az ellenőrzés idejére kirendelt helyettesítő őr a megadott időn belül megérkezett”*: Mivel az őr ellenőrzése feltűnés nélkül kell történjen, az ellenőrzés idejére az őrt ki kell vonni a szolgálatból, azaz helyére egy helyettesítő őrt kell kirendelni. Célszerű az őr mellől felhívni a szolgálatvezetést és kirendeltetni a helyettesítő őrt. Ez a pont egyben az irányítás reagálási idejét is méri, azaz a megadott idő alatt odaér-e a helyettesítő őr.

A gyakorlat messze nem mindig ez és sok esetben ilyen szigorúnak tűnő ellenőrzés számos okból nem is kivitelezhető. A példa mégis rámutat a keletkező adatmennyiség nagyságára. Csak ebből az egyetlen egy szolgáltatásból, amely egy sokkal nagyobb szolgáltatáscsoport része, évi 17 280 szolgáltatási eseményt kell ellenőriznünk és ehhez 720 mintát kell kiválasztanunk, azaz legalább 720 rekordot kell rögzíteni, és ez az összes biztonsági szolgáltatás közül csak az egyik, és annak is csak egy része.

Az ellenőrzési folyamatot igen jól lehet gépesíteni, megfelelő begyakorlással az ellenőrzés naponta legfeljebb 5 -10 percet vesz igénybe, cserébe viszont pontos áttekintés nyerhetünk a szolgáltatás nyújtott teljesítményéről, amely az 1. ábra megfogalmazásával a szolgáltatás leszállított minősége.

FELKÉSZÜLÉS A SZOLGÁLTATÁSOK MINŐSÉGÉNEK MÉRÉSÉRE

Mint már kiviláglott, az általunk vizsgált szolgáltatási kör mérésére fel is kell készülni. Ez lehet az alapja annak szervezeti szabályrendszernek, amit a bevezetőben is említettünk [12] [13]. Az alábbiakban sorra vesszük azokat a lépéseket, amelyeket érdemes mérlegelni a felkészülés során.

1. Melyik szolgáltatást akarjuk méri?
   Itt mérlegelni kell, hogy a köznapi szóhasználat sokszor nem pontos és szolgáltatási csoportokat nevez meg, így biztonsági szolgáltatás, takarítás, karbantartás, holott ezek szolgáltatáscsoportok. A felbontásban el kell jutni az egyedi szolgáltatásokhoz a csoportokon belül.
2. Az azonosított szolgáltatás melyik típusba tartozik a 2. táblázat alapján?
3. Azonosítani kell a kiválasztott szolgáltatásnál azt a szolgáltatási eseményt, eseményeket, amelyeket mérni akarunk.
4. Az öt fő tényező közül az adott szolgáltatásnál melyeket tudjuk mérni és hogyan? Itt mindenképpen mérlegelni a mintavételezéssel való mérésének módját, azaz a szolgáltatás szervezetileg, üzletileg kritikus-e vagy sem.
5. Ki kell dolgozni a szolgáltatásra vonatkozó szolgáltatási szint megállapodást az MSZ EN ISO 41012:2018 Létesítménygazdálkodás. Útmutató a stratégiai erőforrás-kezelésre és megállapodások kidolgozására szabvány alapján [4]
6. A szolgáltatások minősítési adatait rögzíteni kell [3]

FELHASZNÁLT IRODALOM

[1] V. Csányi, Az emberi természet. Akadémiai Kiadó, 2016. doi:10.1556/9789630598057.
[2] MSZ EN ISO 41011:2018 Létesítménygazdálkodás. Szótár (ISO 41011:2017)
[3] MSZ EN ISO 41001:2018 Létesítménygazdálkodás. Irányítási rendszerek. Követelmények alkalmazási útmutatóval (ISO 41001:2018)

[4] MSZ EN ISO 41012:2018 Létesítménygazdálkodás. Útmutató a stratégiai erőforrás-kezelésre és megállapodások kidolgozására (ISO 41012:2017)
[5] MSZ EN 15221-7:2013 Létesítménygazdálkodás. 7. rész: Irányelvek szolgáltatások összehasonlító teljesítménymérésére
[6] MSZ EN 13549:2001 Takarítási szolgáltatások. Alapvető követelmények és ajánlások minőségmérési rendszerekhez
[7] B. Tedja, M. Al Musadieq, A. Kusumawati, és E. Yulianto, „Systematic literature review using PRISMA: exploring the influence of service quality and perceived value on satisfaction and intention to continue relationship", Futur Bus J, köt. 10, sz. 1, Art. sz. 1, dec. 2024, doi: 10.1186/s43093-024-00326-4.
[8] Kövesi János, Topár József, és Erdei János, A minőségmenedzsment alapjai. Budapest: BMGE GTK: Typotex, 2006.
[9] Gábor R., Richárd K., és László M., „A szolgáltatásminőség értelmezésének különbségei – percepcióvezérelt szolgáltatások minőségmodellje kialakításának első lépései".
[10] A szerzőnek BME Mérnöktovábbképző Intézetben folyó létesítménygazdálkodási képzésen szerzett személyes tapasztalatai (https://www.mti.bme.hu/tanfolyam/letesitmenygazdalkodas-i-facility-management-menedzseri-szint-2/)
[11] MSZ ISO 2859 szabványsorozat: Minősítéses ellenőrzések mintavételi eljárásai
[12] MSZ EN ISO 41014:2021 Létesítménygazdálkodás. A létesítménygazdálkodási stratégia kidolgozása (ISO 41014:2020)
[13] MSZ EN ISO 41018:2023 Létesítménygazdálkodás. A létesítménygazdálkodási irányelvek kidolgozása (ISO 41018:2022)

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